Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации

Московский ордена Почета университет
Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

О. Ю. Новикова

ТЕХНОЛОГИИ ПОЛУЧЕНИЯ ОПЕРАТИВНО ЗНАЧИМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Учебное пособие

Москва

Московский университет
МВД России имени В.Я. Кикотя

2025

УДК 004.056
ББК 32.973.202
Н73

Рецензенты:
начальник кафедры информационного обеспечения органов внутренних дел Уральского юридического института МВД России кандидат юридических наук **А. П. Леонов**;
ведущий научный сотрудник НИЦ № 2 (по исследованию проблем оперативно-розыскного противодействия общеуголовным преступлениям, экстремизму и терроризму) ВНИИ МВД России кандидат юридических наук **Н. Н. Грибовская**;
начальник БСТМ ГУ МВД России по Пермскому краю **Д. С. Сафронов**;
доцент Учебно-научного центра «Информационная безопасность» Института радиоэлектроники и информационных технологий – РТФ Уральского федерального университета имени первого Президента России Б. Н. Ельцина **М. Г. Гизатуллин**

Новикова, О. Ю.

Н73 **Технологии получения оперативно значимой информации в информационно-телекоммуникационных сетях** : учебное пособие / О. Ю. Новикова. – М. : Московский университет МВД России имени В.Я. Кикотя, 2025. – 440 с.
ISBN 978-5-9694-1612-3

Учебное пособие содержит систематическое изложение материала по курсу «**Технологии получения оперативно значимой информации в информационно-телекоммуникационных сетях**».

Предназначено для курсантов факультета подготовки специалистов в области информационной безопасности, обучающихся по специальностям 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» и 10.05.03 «Информационная безопасность автоматизированных систем».

УДК 004.056
ББК 32.973.202

ISBN 978-5-9694-1612-3

© Московский университет МВД России имени В.Я. Кикотя, 2025
© Новикова О. Ю., 2025

Оглавление

Список сокращений.....12
ВВЕДЕНИЕ.....16
Глава 1. ОБЩАЯ ХАРАКТЕРИСТИКА ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ РАСПРОСТРАНЕНИЯ, ХРАНЕНИЯ, ОБРАБОТКИ И ПЕРЕДАЧИ ИНФОРМАЦИИ
§ 1. Общие положения нормативно-правового регулирования информационных процессов.....20
§ 2. Стандарты информационной безопасности, нормативные документы, определяющие организационные и технические требования в области защиты информации.....34
§ 3. Основные нормативные правовые документы, регламентирующие распространение, хранение, обработку и передачу информации в информационно-телекоммуникационных сетях.....38
§ 4. Приоритетные направления государственной политики Российской Федерации в области информационной безопасности.....43
§ 5. Ответственность за нарушения в сфере защиты информации.....46
Учебно-методический раздел к главе 1.....49
Библиографический список к главе 1.....53
Глава 2. КОМПЬЮТЕРНАЯ РАЗВЕДКА В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В ИНФОРМАЦИОННОЙ СФЕРЕ
ВВЕДЕНИЕ.....60
§ 1. Основные понятия и определения компьютерной разведки.....61
§ 2. Особенности, формы и виды компьютерной разведки.....65

§ 3. Технологии применения компьютерной разведки
в борьбе с преступлениями в информационной сфере.....69
§ 4. Проблемы, возникающие при проведении компьютерной
разведки, и возможные пути их решения.....72
Учебно-методический раздел к главе 2.....75
Библиографический список к главе 2.....78
Глава 3. СРЕДСТВА И ТАКТИКА СКРЫТОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ ИЗ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ
ВВЕДЕНИЕ.....81
§ 1. Информация: основные свойства, угрозы
и уязвимости.....82
§ 2. Методы и средства несанкционированного получения
информации из автоматизированных систем.....94
§ 3. Виды и формы тактики при скрытом получении
информации из защищенных компьютерных систем.....97
§ 4. Методики кибератак MITRE ATT&CK и технология
Cyber Kill Chain.....101
§ 5.Автоматизация информационной деятельности
при получении информации из защищенных компьютерных
систем.....104
Учебно-методический раздел к главе 3.....109
Библиографический список к главе 3.....115
Глава 4. ИНФОРМАЦИОННЫЕ РЕСУРСЫ: ПОНЯТИЕ, КЛАССИФИКАЦИЯ И ИСПОЛЬЗОВАНИЕ ПРИ СБОРЕ ИНФОРМАЦИИ
ВВЕДЕНИЕ.....117
§ 1. Понятие «информационные ресурсы».....118
§ 2. Задачи информационных ресурсов по реализации
функций основной и информационной деятельности.....122
§ 3. Типология информационных ресурсов.....127

§ 4. Иерархическая природа информационных ресурсов.....130
§ 5. Классификация и использование информационных ресурсов при сборе информации.....135
§ 6. Информационные услуги – особый вид товара на информационном рынке.....139
Учебно-методический раздел к главе 4.....143
Библиографический список к главе 4.....146
Глава 5. СОЦИАЛЬНЫЕ СЕТИ: ВИДЫ, ХАРАКТЕРИСТИКА, СОДЕРЖАЩАЯСЯ ИНФОРМАЦИЯ
ВВЕДЕНИЕ.....149
§ 1. Возникновение. Понятие. Формы.....150
§ 2. Технологии применения социальных сетей.....161
§ 3. Негативные влияния социальных сетей в процессе общения.....167
Учебно-методический раздел к главе 5.....169
Библиографический список к главе 5.....173
Глава 6. ОФИЦИАЛЬНЫЕ ЗАПРОСЫ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ С ЦЕЛЬЮ ПОЛУЧЕНИЯ ОПЕРАТИВНО ЗНАЧИМОЙ ИНФОРМАЦИИ
ВВЕДЕНИЕ.....177
§ 1. Проблемы раскрываемости преступлений и роль официальных запросов в получении оперативно значимой информации.....178
§ 2. Нормативные правовые документы, регламентирующие понятие «запросы».....180
§ 3. Формы и виды официальных запросов.....184
§ 4. Характеристики и особенности официальных запросов.....187
Учебно-методический раздел к главе 6.....194
Библиографический список к главе 6.....197

Глава 7. МЕТОДИКА ВЫЯВЛЕНИЯ И ПРЕСЕЧЕНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБОРОТОМ КУЛЬТУРНЫХ ЦЕННОСТЕЙ В СЕТИ ИНТЕРНЕТ

ВВЕДЕНИЕ.....201

§ 1. Нормативно-правовое регулирование охраны культурных ценностей.....202

§ 2. Оборот культурных ценностей в сети Интернет.....212

§ 3. Методика выявления и пресечения преступлений, связанных с незаконным оборотом культурных ценностей в сети Интернет.....216

Учебно-методический раздел к главе 7.....220

Библиографический список к главе 7.....223

Глава 8. МЕТОДИКА ВЫЯВЛЕНИЯ МЕДИЙНЫХ ИСТОЧНИКОВ, РАСПРОСТРАНЯЮЩИХ ЛОЖНУЮ ИНФОРМАЦИЮ В СЕТИ ИНТЕРНЕТ

ВВЕДЕНИЕ.....226

§ 1. Источники информации и медийные источники: классификация, свойства и роль в распространении ложной информации.....228

§ 2. Нормативные правовые документы, регламентирующие понятие «медийные источники».....236

§ 3. Общие принципы российского законодательства, определяющие порядок формирования и распространения информации.....241

§ 4. Полномочные государственные органы Российской Федерации в области средств массовой информации: их права и обязанности.....245

§ 5. Порядок и требования к регистрации средств массовой информации.....248

§ 6. Правовой статус блогеров и их ответственность.....251

§ 7. Методика выявления медийных источников,
распространяющих ложную информацию
в сети Интернет 256
Учебно-методический раздел к главе 8.....261
Библиографический список к главе 8.....264
Глава 9. МЕТОДИКА ВЫЯВЛЕНИЯ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С РАСПРОСТРАНЕНИЕМ ПРОТИВОПРАВНОГО КОНТЕНТА В СЕТИ ИНТЕРНЕТ
ВВЕДЕНИЕ.....266
§ 1. Формы и виды контента в сети Интернет.....267
§ 2. Методики выявления и раскрытия преступлений,
связанных с распространением противоправного контента
в сети Интернет.....284
§ 3. Методики выявления и раскрытия преступлений,
связанных с распространением противоправного контента
в сети Интернет.....288
§ 4. Методы выявления деструктивных информационных
операций на их ранних стадиях в социальных сетях.....295
Учебно-методический раздел к главе 9.....302
Библиографический список к главе 9.....305
Глава 10. МЕТОДИКА ВЫЯВЛЕНИЯ И РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБОРОТОМ ОРУЖИЯ С ИСПОЛЬЗОВАНИЕМ ОТКРЫТЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ
ВВЕДЕНИЕ.....308
§ 1. Нормативные правовые документы, регламентирующие
понятие «оборот оружия» и «незаконный оборот оружия».....309
§ 2. Нормативные правовые документы, регламентирующие
понятия «оборот оружия» и «незаконный оборот оружия»
в сети Интернет.....314

§ 3. Незаконный оборот оружия с использованием открытых источников информации.....318
§ 4. Торговля оружием в даркнете: методы выявления и противодействия.....321
§ 5. Методика выявления и раскрытия преступлений, связанных с незаконным оборотом оружия с использованием сети Интернет.....324
Библиографический список к главе 10.....335
Глава 11. МЕТОДЫ И СРЕДСТВА ОПРЕДЕЛЕНИЯ КОНФИГУРАЦИИ СЕТИ. ПЕРЕХВАТ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО СЕТИ. МОНИТОРИНГ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ
ВВЕДЕНИЕ.....338
§ 1. Общие и основные особенности мониторинга в информационно-телекоммуникационных сетях.....339
§ 2. Характеристики, виды и формы мониторинга в информационно-телекоммуникационных сетях.....346
§ 3. Технологии мониторинга в информационно-телекоммуникационных сетях.....349
§ 4. Методики мониторинга (пошагово, как делать).....353
Учебно-методический раздел к главе 11.....363
Библиографический список к главе 11.....369
Глава 12. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ
ВВЕДЕНИЕ.....372
§ 1. Нормативные правовые документы, определяющие понятие «социальная инженерия».....374
§ 2. Характеристики и особенности социальной инженерии, ее формы и методы.....377

Учебно-методический раздел к главе 12.....387
Библиографический список к главе 12.....390
Глава 13. ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ ПОЛУЧЕНИЯ ОПЕРАТИВНО ЗНАЧИМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ
ВВЕДЕНИЕ.....393
§ 1. Оперативно-разыскная информация: сущность и проекции.....394
§ 2. Оформление оперативно значимой информации.....396
§ 3. Общие и основные требования к оформлению результатов оперативно значимой информации в информационно-телекоммуникационных сетях.....404
§ 4. Порядок оформления результатов получения оперативно значимой информации в информационно-телекоммуникационных сетях.....408
§ 5. Основные НПА, регулирующие проведение ОРМ в сети Интернет.....424
Учебно-методический раздел к главе 13.....430
Библиографический список к главе 13.....435
ЗАКЛЮЧЕНИЕ.....437

Список сокращений

Российские организации, законы и термины

АС – автоматизированная система.

АСУ ТП – автоматизированные системы управления технологическими процессами.

БДУ ФСТЭК – база данных уязвимостей Федеральной службы по техническому и экспортному контролю Российской Федерации.

ГИС – государственная информационная система.

ГК РФ – Гражданский кодекс Российской Федерации.

ГОСТ – государственный стандарт Российской Федерации.

ИАС КР – информационно-аналитическая система компьютерной разведки.

ИБ – информационная безопасность.

ИКТ – информационно-коммуникационные технологии.

ИС – информационная система.

ИСПД – информационная система персональных данных.

ИТС – информационно-телекоммуникационные сети.

КИИ – критическая информационная инфраструктура.

КСС – компьютерные системы и сети.

КоАП РФ – Кодекс Российской Федерации об административных правонарушениях.

ЛПР – лица, принимающие решения.

МИБ – международная информационная безопасность.

МЭ – межсетевой экран (файрвол, брандмауэр).

НСД – несанкционированный доступ.

ООН – Организация Объединенных Наций.

ОРД – оперативно-разыскная деятельность.

ОРМ – оперативно-разыскное мероприятие.

ОС – операционная система.

ПДн – персональные данные.

ПО – программное обеспечение.

СЗИ – средства защиты информации.

СУБД – система управления базами данных.

УК РФ – Уголовный кодекс Российской Федерации.

ФСБ России – Федеральная служба безопасности Российской Федерации.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации.

ШОС – Шанхайская организация сотрудничества.

ЭВТ – электронно-вычислительная техника.

Международные и технические сокращения

API (Application Programming Interface) – программный интерфейс приложения.

APT (Advanced Persistent Threat) – продвинутая устойчивая угроза.

Buffer Overflow – переполнение буфера, уязвимость ПО.

CERT/CC (Computer Emergency Response Team / Coordination Center) – координационный центр реагирования на компьютерные инциденты.

CIA-триада – Confidentiality (конфиденциальность), Integrity (целостность), Availability (доступность).

CVE (Common Vulnerabilities and Exposures) – каталог уязвимостей и эксплойтов.

CVSS (Common Vulnerability Scoring System) – система оценки уязвимостей.

Data Mining – интеллектуальный анализ данных.

Deep Web – глубокая сеть, недоступная для индексации поисковыми системами.

DDoS (Distributed Denial of Service) – распределенная атака «отказ в обслуживании».

DoS (Denial of Service) – отказ в обслуживании.

IDS (Intrusion Detection System) – система обнаружения вторжений.

IoT (Internet of Things) – интернет вещей.

IPS (Intrusion Prevention System) – система предотвращения вторжений.

ISO/IEC – Международная организация по стандартизации / Международная электротехническая комиссия.

Knowledge Discovery – процесс выявления знаний в данных.

MITM (Man-in-the-Middle) – атака «человек посередине».

NVD (National Vulnerability Database) – национальная база данных уязвимостей США.

OSINT (Open Source Intelligence) – разведка по открытым источникам.

RAT (Remote Access Trojan) – троян удаленного доступа.

SAM (Security Accounts Manager) – база данных Windows для хранения хэшей паролей.

SCADA (Supervisory Control And Data Acquisition) – система диспетчерского управления и сбора данных.

SDLC (Secure Development Lifecycle) – жизненный цикл безопасной разработки ПО.

SID (Security Identifier) – уникальный идентификатор безопасности в Windows.

SIP (Session Initiation Protocol) – протокол установления сеанса.

SNMP (Simple Network Management Protocol) – протокол управления сетью.

SQL (Structured Query Language) – язык структурированных запросов.

SQLi (SQL-инъекция) – внедрение вредоносного кода в SQL-запросы.

TCP (Transmission Control Protocol) – протокол управления передачей.

Text Mining – интеллектуальный анализ текстовой информации.

UDP (User Datagram Protocol) – протокол пользовательских датаграмм.

VLAN (Virtual Local Area Network) – виртуальная локальная сеть.

VPN (Virtual Private Network) – виртуальная частная сеть.

XSS (Cross-Site Scripting) – межсайтовый скриптинг.

Введение

Современный мир переживает этап масштабной трансформации, который в научной литературе принято обозначать как переход от индустриального общества к обществу информационному. Данный процесс является не только технологическим, но и социально-экономическим, культурным и политическим. Он затрагивает все уровни организации общества – от глобальной системы международных отношений до бытовых практик отдельного человека. Если для индустриальной эпохи определяющим ресурсом выступали материальные активы, производственные мощности и энергетические ресурсы, то в информационную эпоху именно информация становится ведущим стратегическим ресурсом, способным определять направление развития целых государств и регионов.

В условиях информационного общества информация перестает быть сопутствующим элементом человеческой деятельности. Она превращается в самостоятельный фактор, от которого зависят эффективность управления, качество принимаемых решений, развитие инновационных технологий и конкурентоспособность национальной экономики. Более того, в ряде случаев информация по своей значимости превосходит традиционные экономические и энергетические активы. Сегодня именно она формирует основу для создания новых товаров и услуг, для совершенствования образовательных и культурных практик, а также для повышения эффективности государственного управления.

При этом информационная эпоха несет не только уникальные возможности, но и новые угрозы. Будучи ценнейшим ресурсом, информация одновременно является уязвимым объектом. Она может быть неправомерно использована, похищена,

искажена, уничтожена или обращена во вред интересам личности, общества и государства. Масштабы этих рисков возрастают в условиях стремительного развития информационно-телекоммуни-кационных технологий (ИКТ), которые, с одной стороны, расширяют горизонты взаимодействия, а с другой – создают новые каналы для несанкционированного доступа, утечки конфиденциальных данных и совершения киберпреступлений.

В контексте правоохранительной деятельности подобные вызовы приобретают особую остроту. Преступность активно осваивает цифровое пространство, используя его для совершения противоправных деяний: от финансовых махинаций и хищений до распространения деструктивного контента, организации экстремистских сообществ и террористических актов. Это требует от правоохранительных органов не только понимания технических особенностей функционирования ИКТ, но и владения специализированными методиками по выявлению, сбору, анализу и использованию оперативно значимой информации. Такая информация, полученная законными способами и должным образом оформленная, становится основой доказательственной базы при расследовании преступлений в киберпространстве.

Учебное пособие «Технологии получения оперативно значимой информации в информационно-телекоммуникационных сетях» разработано специально для студентов специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере». Его ключевая цель заключается в том, чтобы обеспечить будущих специалистов всесторонними знаниями и навыками, необходимыми для работы в сфере противодействия современным вызовам информационной безопасности. Авторы ставят перед собой задачу подготовить кадры, способные не только реагировать на существующие угрозы,

но и предвидеть новые, вырабатывать эффективные стратегии защиты и внедрять инновационные подходы в обеспечение кибербезопасности.

Структура пособия охватывает широкий спектр тем. В первых разделах рассматриваются фундаментальные правовые и организационные основы, регулирующие информационные отношения и защиту данных. Далее внимание сосредоточено на концепции компьютерной разведки, методах и тактике скрытого получения информации, а также на принципах работы с различными информационными ресурсами и социальными сетями, которые в современных условиях активно используются преступными сообществами. В последующих разделах подробно описываются методики выявления и пресечения преступлений, связанных с незаконным оборотом культурных ценностей, распространением ложной информации, противоправного контента и незаконного оборота оружия через сеть Интернет.

Кроме того, пособие включает материалы о мониторинге сетевой активности, особенностях эксплуатации сетевого оборудования, а также раскрывает угрозы социальной инженерии, которые являются одними из наиболее распространенных и опасных форм неправомерного воздействия на пользователей информационных систем. Существенное внимание уделено вопросам правильного документирования результатов оперативно-разыскной деятельности, поскольку именно это обеспечивает их юридическую силу и возможность использования в качестве доказательств в судебном процессе.

Каждый раздел пособия построен таким образом, чтобы студент не только овладевал теоретическими знаниями, но и развивал аналитическое мышление, умение критически оценивать информацию и применять полученные знания в реальных условиях. В качестве дополнительных элементов в книгу включены

контрольные вопросы, методические рекомендации и глоссарий ключевых терминов, что делает данное пособие удобным и для самостоятельного изучения, и для аудиторной работы.

Мы убеждены, что данное учебное пособие станет надежным фундаментом для формирования профессиональных компетенций специалистов в области информационной безопасности. Полученные знания и навыки позволят будущим выпускникам не только успешно справляться с профессиональными задачами, но и вносить значимый вклад в обеспечение национальной безопасности, защиту конституционных прав граждан и поддержание правопорядка в условиях цифровой трансформации общества.

Глава 1. ОБЩАЯ ХАРАКТЕРИСТИКА ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ РАСПРОСТРАНЕНИЯ, ХРАНЕНИЯ, ОБРАБОТКИ И ПЕРЕДАЧИ ИНФОРМАЦИИ

§ 1. Общие положения нормативно-правового регулирования информационных процессов

Переход от общих закономерностей информационной эпохи к правовым механизмам ее обеспечения обусловлен тем, что устойчивость цифровых процессов определяется не только технологиями, но и качеством нормативной базы. Поэтому далее обратимся к структуре действующего законодательства, задающей рамки правоприменения в ИКТ-сфере.

Формирование правовой основы регулирования информационных отношений в Российской Федерации является процессом длительным и многоуровневым. Оно отражает стремление государства не только к адаптации международных правовых норм, но и к созданию собственной системы защиты национальных интересов в цифровой среде. На современном этапе нормативное регулирование в сфере информационно-коммуникационных технологий (ИКТ) выстроено как комплексная иерархическая система, включающая международные соглашения, Конституцию Российской Федерации, федеральные законы, указы Президента, постановления Правительства, акты федеральных органов исполнительной власти, а также законы субъектов Российской Федерации и локальные регламенты организаций.

Такой многоуровневый характер позволяет учесть как глобальные вызовы, так и особенности российской правовой системы. Международные соглашения обеспечивают совместимость с мировыми стандартами и участие России в формировании

глобальной архитектуры информационной безопасности. Федеральное законодательство и подзаконные акты конкретизируют эти нормы, адаптируя их к национальным реалиям. Локальные акты организаций регулируют прикладные вопросы эксплуатации информационных систем, включая порядок доступа к данным, требования к защите персональной информации и правила сертификации технических решений.

Для систематизации анализа принято выделять две группы нормативных документов:

1. Нормативные правовые акты, формирующие правовую основу информационной сферы. К ним относятся международные договоры, Конституция Российской Федерации, федеральные законы, указы Президента Российской Федерации и постановления Правительства Российской Федерации. Именно эти акты закрепляют фундаментальные права и свободы граждан, определяют обязанности государственных органов и организаций, а также устанавливают базовые принципы функционирования информационного общества.

2. Нормативно-техническая база, регламентирующая практическую сторону использования ИКТ. Сюда входят государственные стандарты (ГОСТ), методические документы, инструкции и критерии оценки качества, которые определяют порядок проектирования, внедрения и эксплуатации информационных систем. Особое место занимают документы, касающиеся лицензирования деятельности в сфере ИКТ, сертификации программных и технических средств защиты информации.

Важно подчеркнуть, что нормативно-технические документы, хотя и обладают меньшей юридической силой по сравнению с законами, но именно они обеспечивают возможность практической реализации требований информационной безопасности. Таким образом, именно совокупность нормативной правовой

и нормативно-технической базы позволяет комплексно регулировать вопросы распространения, хранения, обработки и передачи информации, что особенно значимо в условиях цифровизации общества и экономики.

На федеральном уровне действуют несколько десятков нормативных актов, регулирующих информационную сферу. Основополагающие принципы закреплены в Конституции Российской Федерации, а также в ряде стратегических документов. Среди них можно выделить Доктрину информационной безопасности Российской Федерации, где определены национальные интересы в цифровом пространстве, и Стратегию развития информационного общества в Российской Федерации на 2017–2030 годы, в которой поставлены задачи по интеграции цифровых технологий во все сферы общественной жизни.

Таким образом, современная система законодательства в области ИКТ характеризуется комплексностью и системностью. Она сочетает в себе общие правовые нормы и конкретные технические требования, обеспечивая баланс между защитой интересов личности, общества и государства, с одной стороны, и развитием цифровых технологий – с другой.

Современное правовое поле, регулирующее процессы обработки, хранения и распространения информации, представляет собой многоуровневую систему, включающую нормы международного и национального законодательства. В России регулирование данной сферы осуществляется комплексом нормативных актов различной юридической силы – от конституционных норм до ведомственных регламентов.

Рассмотрев уровни и группы актов, начнем с основания правовой пирамиды – конституционных норм. Именно они формируют базовые гарантии и пределы вмешательства в информационную сферу, определяя баланс свободы и защиты.

1.1. Конституционное регулирование информационных отношений в России

Конституция Российской Федерации занимает центральное место в системе источников права, регулирующих информационные отношения. Она не только закрепляет фундаментальные права и свободы граждан, но и формирует правовую основу для развития всей совокупности отраслевого законодательства в сфере информационной безопасности. Основной закон государства отражает баланс между принципом свободы информации и необходимостью защиты личности, общества и государства от неправомерного использования данных.

Ключевые положения Конституции Российской Федерации [5] прямо касаются информационной сферы:

– **статья 23** закрепляет право каждого гражданина на неприкосновенность частной жизни, личную и семейную тайну, а также на защиту своей чести и доброго имени. Данная норма является базовой для защиты персональных данных и частной коммуникации;

– **статья 24** устанавливает запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Это правило исключает возможность произвольного вмешательства в личную сферу и обязывает государственные органы действовать строго в рамках закона;

– **статья 29** провозглашает свободу мысли и слова, а также право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Эта норма составляет основу свободы массовой информации и гарантирует открытость общественного диалога;

– **статья 33** закрепляет право граждан обращаться лично, а также направлять индивидуальные и коллективные обращения

в государственные органы и органы местного самоуправления. Это положение обеспечивает возможность обратной связи между обществом и властью;

– **статья 42** гарантирует право каждого гражданина на достоверную информацию о состоянии окружающей среды, что напрямую связано с правом на благоприятные условия жизни и защиту здоровья.

Особое значение имеет также **ч. 2 ст. 23**, которая гарантирует тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права возможно исключительно на основании судебного решения. Таким образом, Конституция устанавливает строгий правовой режим охраны личной и семейной тайны, препятствующий произвольному вмешательству со стороны государства или частных лиц.

Таблица 1

Принципы конституционного регулирования

Принцип	***Содержание***	***Конституционная основа***
Информационной открытости	Право на свободный доступ к информации	ст. 29
Конфиденциальности	Защита персональных данных и тайны коммуникаций	ст.ст. 23, 24
Баланса интересов	Сочетание прав граждан и интересов государства	ст. 55

Указанные конституционные нормы создают правовую основу для развития отраслевого законодательства, обеспечивая защиту прав граждан в условиях цифровизации всех сфер общественной жизни.

Важно подчеркнуть, что конституционные нормы не только формулируют права и свободы, но и закрепляют механизмы их реализации. Так, обязанность государственных органов

обеспечивать доступ граждан к информации, затрагивающей их права и свободы, способствует развитию открытого общества и повышает уровень доверия к власти.

На практике данные конституционные положения находят развитие в федеральном законодательстве, регулирующем вопросы персональных данных, тайны связи, государственной тайны, а также в подзаконных актах, определяющих порядок функционирования государственных и муниципальных информационных систем. Таким образом, Конституция выступает не только в качестве источника прав и свобод, но и как фундамент, на котором строится вся система законодательства в сфере информационной безопасности.

Конституционные гарантии корреспондируют общепризнанным принципам и нормам международного права. Для полноты картины обозначим международные стандарты, влияющие на российскую модель информационной безопасности.

1.2. Основные нормы международного права в сфере информационной безопасности

Регулирование информационных отношений в национальном законодательстве неразрывно связано с международными правовыми стандартами. В условиях глобализации информационные процессы выходят за рамки национальных границ, что делает необходимым опору на универсальные нормы международного права. Именно они закладывают фундамент, на основе которого строится национальная система обеспечения информационной безопасности, и задают единые ориентиры для государств – участников мирового сообщества.

Международное право в сфере информации имеет несколько ключевых направлений: обеспечение свободы доступа к инфор-

мации, защита персональных данных, охрана интеллектуальной собственности, а также противодействие распространению вредного и противоправного контента. Важнейшие документы закрепляют как права личности, так и допустимые ограничения, направленные на охрану общественных интересов и национальной безопасности.

Всеобщая декларация прав человека

Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10 декабря 1948 г.) [1] стала первым универсальным международным документом, провозгласившим право каждого человека на свободу поиска, получения и распространения информации. В ст. 19 Декларации закреплено, что данное право включает свободу придерживаться собственных убеждений и свободно выражать их без вмешательства. Тем самым был заложен принцип открытости информации, который и сегодня остается краеугольным камнем демократического общества.

Европейская конвенция о защите прав человека / основных свобод

Европейская конвенция о защите прав человека и основных свобод (подписана в Риме 4 ноября 1950 г.) [2] развивает идеи Декларации. В ст. 10 закреплено право каждого человека свободно выражать свое мнение, а также получать и распространять информацию. В то же время Конвенция допускает установление ограничений – в интересах национальной безопасности, территориальной целостности, защиты здоровья, морали, прав и свобод других лиц. Таким образом, формируется важный баланс между правами личности и необходимостью защиты общественных интересов.

Международный пакт о гражданских и политических правах

Международный пакт о гражданских и политических правах (принят Генеральной Ассамблеей ООН 16 декабря 1966 г.) [3] закрепил обязательность выполнения положений о праве на свободу слова и информации для государств-участников. В ст. 19 Пакта дополнительно акцентируется ответственность за злоупотребление свободой слова и предусматриваются допустимые ограничения, что позволяет учитывать не только права отдельного индивида, но и интересы всего общества.

Защита персональных данных

Особое значение для формирования российского законодательства имеет Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г., вступила в силу для России в 2005 г.) [4]. Данный документ впервые установил международные стандарты в области защиты персональных данных. Конвенция обязывает государства-участники обеспечивать законность и справедливость обработки персональной информации, ее сохранность и использование исключительно в легитимных целях.

Формирование концепции информационного общества

В XXI в. международное право сосредоточено также на вопросах глобального развития информационного общества. Важнейшее значение имеет Декларация принципов Всемирной встречи на высшем уровне по вопросам информационного общества (Женева, 2003 г.). Декларация называется «Построение информационного общества – глобальная задача в новом тысячелетии» [6], в ней подчеркивается необходимость равного доступа государств и граждан к информационным ресурсам, а также

важность международного сотрудничества для противодействия киберугрозам.

Итоговое значение международных норм

Таким образом, международные документы формируют основу для построения национальных правовых систем в сфере информационной безопасности. Их нормы закрепляют универсальные принципы: свободу получения и распространения информации, уважение частной жизни, охрану персональных данных, а также ответственность за злоупотребление информацией. Российская Федерация, ратифицируя ключевые международные акты, тем самым подтверждает свою приверженность общепризнанным принципам международного права и адаптирует их к национальным условиям.

Универсальные международные подходы получают конкретизацию в российском правопорядке. Ниже проследим эволюцию национального законодательства: от разрозненных норм к отраслевой системе правовых режимов защиты информации.

1.3. Правовые основы обеспечения информационной безопасности в Российской Федерации

Следует подчеркнуть, что регулирование информационных отношений в Российской Федерации опирается не только на конституционные положения, но и на разветвленную систему федеральных законов и подзаконных актов, в рамках которой субъектами информационных правоотношений выступают как государственные органы, так и граждане и организации. Такая архитектура позволяет одновременно обеспечивать публичные интересы и гарантировать реализацию частных прав в цифровой среде.

Важным элементом этой системы является обязанность органов государственной власти обеспечивать доступ граждан к документам и материалам, непосредственно затрагивающим их права и свободы, за исключением случаев, прямо предусмотренных законом. Подобная открытость способствует прозрачности деятельности государственных структур и укрепляет доверие общества к институтам власти, что особенно значимо в условиях стремительного развития информационно-коммуникационных технологий (ИКТ).

Историческая эволюция: от фрагментарности к системности

В постсоветский период правовое регулирование информационной сферы формировалось первоначально фрагментарно: нормы, касающиеся защиты информации, ответственности за ее неправомерное использование и преступления в сфере компьютерной информации, были распределены по различным кодексам – Гражданскому (ч. 1), Уголовному и КоАП РФ. На этом этапе информационная безопасность еще не выступала самостоятельным предметом правового регулирования: соответствующие положения служили обеспечивающими нормами в иных отраслях права.

Сдвиг к системности начался с принятия первых профильных актов, положивших основу развития отрасли. К ним относятся:

– Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» – закрепил недопустимость цензуры и ответственность за злоупотребление свободой СМИ;

– Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» – определил исчерпывающий пере-

чень сведений, составляющих государственную тайну, и режим их охраны;

– Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» – для своего времени дал системное регулирование защиты информации и прав субъектов информационных отношений (впоследствии утратил силу);

– Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене» – легализовал термин «информационная безопасность», установил ограничения на трансграничный оборот информации и запрет недостоверной иностранной документированной информации в Российской Федерации (утратил силу).

Консолидация и специализация норм

Дальнейшее развитие законодательства было направлено на устранение пробелов, противоречий и дублирования, а также на конкретизацию правовых режимов применительно к различным видам информации и практикам ее использования. Именно на этом этапе появляются акты, обеспечившие охрану информации ограниченного доступа и данных специального режима обработки:

– Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» – уточнил состав сведений, составляющих коммерческую тайну, и механизмы ее защиты;

– Федеральный закон от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях» – регламентировал формирование и использование кредитных историй;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» – установил правовой режим обработки персональных данных, обязанности операторов и полномочия уполномоченного органа;

– Федеральный закон от 27 июля 2010 г. № 224-ФЗ о противодействии неправомерному использованию инсайдерской информации и манипулированию рынком – впервые системно урегулировал предупреждение злоупотреблений на финансовых рынках.

Названные акты задали стандарты ответственности за разглашение охраняемых сведений, определили контролирующие органы и процессуальные механизмы надзора. В совокупности это позволило говорить о формировании баланса интересов граждан, общества и государства при защите как публичных, так и частных информационных ресурсов.

Отдельного внимания заслуживают два важнейших направления:

– защита детей от вредной информации: Федеральный закон от 29 декабря 2010 г. № 436-ФЗ установил систему классификации, ограничения и ответственности за распространение информации, способной причинить вред здоровью и развитию несовершеннолетних;

– противодействие экстремистской деятельности: Федеральный закон от 25 июля 2002 г. № 114-ФЗ определил критерии признания материалов экстремистскими, порядок их запрета и механизмы пресечения оборота.

Интеллектуальная собственность и цифровая экономика

Значительный массив норм, критически важных для информационной безопасности, был сконцентрирован в ч. 4 ГК РФ, объединившей ранее разрозненные акты в сфере авторского и патентного права, а также правовой охраны программ для ЭВМ и баз данных. Тем самым законодатель признал охраняемые результаты интеллектуальной деятельности важнейшим ресурсом цифровой экономики.

Параллельно выстраивалась правовая база для электронного документооборота. Принятый в 2002 г. закон № 1-ФЗ «Об электронной цифровой подписи» отработал базовые подходы (утратил силу), а действующий Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» закрепил юридическую значимость электронных подписей, их типологию и требования к инфраструктуре доверия.

Основы и принципы государственной политики

Стратегические ориентиры государственной политики закреплены в Доктрине информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации 05.12.2016 № Пр-1895). В документе сформулированы цели, задачи и приоритеты, среди которых:

– защита критической информационной инфраструктуры, охрана персональных данных, развитие отечественных ИКТ-решений и кадрового потенциала;

– соблюдение Конституции Российской Федерации, законодательства и общепризнанных принципов и норм международного права при обеспечении информационной безопасности;

– открытость деятельности органов государственной власти и общественных объединений при информировании общества в пределах законодательно установленных ограничений;

– правовое равенство участников информационного взаимодействия вне зависимости от их статуса, основанное на конституционном праве свободного поиска, получения, передачи, производства и распространения информации законными способами;

– приоритетное развитие отечественных ИКТ, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей

и их интеграцию в глобальные инфраструктуры при соблюдении жизненно важных интересов Российской Федерации.

Логично соотносится с Доктриной и Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности», который среди базовых начал безопасности ставит на первый план соблюдение и защиту прав и свобод человека, и гражданина, законность, а также системность и комплексность применения правовых, организационных и информационно-технических мер.

Каркасный закон об информации и режимы ИС

Системообразующее значение для практики имеет Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Этот закон выступает своего рода каркасом, задающим определения, принципы и базовые режимы обращения с информацией.

Ключевые положения 149-ФЗ, важные для практики правоохранительной и административной деятельности:

1. Классификация информационных систем (ст. 13):

– государственные (федеральные и региональные), создаваемые на основании законов и актов госорганов;

– муниципальные, учреждаемые решениями органов местного самоуправления;

– иные информационные системы, создаваемые и эксплуатируемые другими субъектами права.

2. Оператор информационной системы. Если иное не установлено федеральным законом, оператором признается владелец технических средств обработки данных либо лицо, с которым заключен договор на эксплуатацию системы. На оператора возлагается обязанность обеспечивать законность обработки, безопасность и, когда это прямо предусмотрено, публикацию сведений в формате открытых данных для свободного использования.

3. Права владельца информации. Права на информацию, содержащуюся в базах данных, охраняются независимо от авторских или иных прав на сами базы данных, что обеспечивает защиту интересов владельцев как содержательной составляющей, так и структуры информационных ресурсов.

4. Единые требования к публичным ИС. Требования, предъявляемые законом к государственным информационным системам (ГИС), в равной мере распространяются на муниципальные ИС, если иное прямо не предусмотрено законодательством о местном самоуправлении.

5. Техническое регулирование и эксплуатация. Особенности создания и эксплуатации государственных и муниципальных ИС могут дополнительно определяться техническими регламентами и иными нормативными актами уполномоченных органов, что увязывает юридические требования с практикой стандартизации и сертификации средств защиты.

§ 2. Стандарты информационной безопасности, нормативные документы, определяющие организационные и технические требования в области защиты информации

Вопросы защиты информации невозможно свести только к законам и общим доктринальным установкам. Законодательство задает рамки, но жизнь информационной безопасности обеспечивается через нормативные и методические документы, которые регулируют организационные и технические аспекты работы с данными. Именно они позволяют перейти от абстрактных формулировок к конкретным мерам защиты, применимым в организациях, на предприятиях и в государственных структурах. Без них правовая база оставалась бы скелетом без мускулов.

2.1. Роль ФСТЭК России

Следует подчеркнуть, что центральную роль в этой системе играет **Федеральная служба по техническому и экспортному контролю** (ФСТЭК). В соответствии с Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 именно ФСТЭК выступает ключевым органом, отвечающим за реализацию государственной политики в области технической защиты информации.

Функции ФСТЭК весьма широки и охватывают:

– защиту критической информационной инфраструктуры России;

– противодействие иностранным техническим разведкам;

– обеспечение защиты информации, содержащей государственную тайну и иную охраняемую законом информацию, от утечки по техническим каналам и несанкционированного доступа;

– контроль за безопасностью при разработке, эксплуатации и утилизации излучающих систем и устройств;

– участие в системе экспортного контроля.

При этом ФСТЭК не ограничивается лишь функциями регулятора. Она также является **органом защиты государственной тайны**, ее приказы и методические документы обязательны к исполнению не только в федеральных органах власти, но и в органах субъектов Российской Федерации, на предприятиях, в организациях и учреждениях независимо от формы собственности.

Таким образом, ФСТЭК России – это своего рода технический гарант национальной безопасности, обеспечивающий целостность и защищенность информационного пространства страны.

2.2. Многоуровневая система нормативных документов

Помимо ФСТЭК в создании нормативной базы участвуют и другие структуры: **ФСБ России**, выпускающая приказы в области криптографической защиты информации, а также профильные министерства и органы исполнительной власти. В результате формируется **многоуровневая система**, включающая:

– **Доктрину информационной безопасности Российской Федерации** [24] как стратегический ориентир;

– приказы ФСТЭК и ФСБ, определяющие обязательные требования;

– государственные стандарты (ГОСТы) и рекомендации по стандартизации;

– международные стандарты (например, ISO/IEC 27000);

– методические указания, обеспечивающие практическое внедрение правил защиты информации.

В совокупности они создают единый регулятивный массив, позволяющий органично сочетать стратегию, организационные меры и технические решения.

2.3. Примеры ключевых документов

Характерным примером является **постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119**, определяющее уровни защищенности информационных систем, в которых обрабатываются персональные данные. Фактически этот документ стал основой для построения систем защиты персональной информации в государственных и коммерческих организациях.

Не менее значимы и руководящие документы ФСТЭК. Среди них можно выделить:

– «**Защита от несанкционированного доступа к информации. Термины и определения**» – документ, формирующий единый профессиональный язык специалистов;

– «**Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД**» – регламент, задающий порядок проектирования и испытаний средств защиты;

– «**Автоматизированные системы. Защита от НСД. Классификация и требования**» – документ, определяющий классы защищенности автоматизированных систем и требования к их защите.

Отдельного упоминания заслуживает **приказ ФСТЭК России от 14 марта 2014 г. № 31**, устанавливающий требования к защите информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах. Этот приказ направлен на предотвращение ситуаций, когда нарушение работы таких систем может повлечь угрозу жизни людей, окружающей среде или безопасности государства.

Как видим, нормативная база охватывает как общие понятия и классификации, так и узкоспециализированные технические вопросы, что обеспечивает комплексный подход к построению систем защиты.

2.4. Роль и значение стандартов

Стандарты и методические документы выполняют сразу несколько функций. Они не только закрепляют **правовые обязанности**, но и:

– задают организационные правила работы с информацией;

– устанавливают технические параметры защиты;

– формируют единый понятийный аппарат и культуру информационной безопасности.

Таким образом, речь идет не просто о формальных требованиях. Нормативные акты в сфере защиты информации воспитывают профессиональное сообщество, приучают специалистов мыслить категориями рисков, угроз и уровней защищенности.

2.5. Актуальность и доступность документов

Наконец, важно отметить, что нормативная база в этой области динамична. Постановления, приказы и руководящие документы регулярно редактируются, а национальные стандарты гармонизируются с международными. Сегодня специалисты могут в любое время получить доступ к актуальным редакциям стандартов, приказов и методических указаний через официальные интернет-ресурсы ФСТЭК, ФСБ и национальных центров стандартизации.

Это означает, что специалист в области информационной безопасности должен не только знать общие принципы и правовые основы, но и уметь работать с массивом актуальных документов, ориентируясь в изменениях нормативной среды.

§ 3. Основные нормативные правовые документы, регламентирующие распространение, хранение, обработку и передачу информации в информационно-телекоммуникационных сетях

Как уже отмечалось ранее, фундаментальные права граждан в отношении информации закреплены в **Конституции Российской Федерации**. Часть 4 ст. 29 гарантирует свободу поиска, получения, передачи, производства и распространения информации любым законным способом. Эта формулировка звучит

убедительно, но вместе с тем порождает и трудности: как определить, где пролегает граница между законными и незаконными способами обработки информации?

Юристы традиционно выделяют два подхода:

– **«запрещено все, что не разрешено»** – жесткая модель, ограничивающая доступ и действия;

– **«разрешено все, что не запрещено»** – более мягкий подход, фактически закрепленный в российской практике.

Второй вариант обеспечивает гибкость и свободу, но одновременно создает почву для правовых лазеек, которые могут использовать злоумышленники. Именно поэтому безопасность информации требует не только нормативных запретов, но и комплексной системы условий – правовых, организационных, технических, – делающих невыгодным и затруднительным любое злоупотребление.

3.1. Персональные данные и частная жизнь

Уже в Конституции заложено понимание ключевых категорий защищаемой информации. В ст.ст. 23 и 24 закреплено право граждан на неприкосновенность частной жизни, личную и семейную тайну, а также запрет на сбор, хранение и распространение сведений о частной жизни без согласия лица. Эти положения стали основой для последующего правового регулирования в сфере **персональных данных** (ПДн), формируя целый пласт законодательства.

Ключевым актом в этой сфере является **Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»**. Именно он определяет понятия, принципы и условия обработки ПДн, устанавливает права субъектов данных и обязанности операторов. В развитие этого закона действует **постановление Правитель-**

ства Российской Федерации от 1 ноября 2012 г. № 1119, устанавливающее требования к защите ПДн при их обработке в **информационных системах персональных данных (ИСПДн)**.

Дополняют систему специальные акты – **приказы ФСТЭК России** [24], методические документы ФСБ России, а также национальные стандарты: например **ГОСТ Р 57580-2017** и **ГОСТ Р ИСО/МЭК 27001-2012**, регламентирующие организационные и технические меры безопасности.

Таким образом, именно 152-ФЗ стал каркасом всей правовой системы защиты ПДн, а подзаконные акты конкретизируют и детализируют его положения.

3.2. Информационная безопасность как категория

Системное понимание информационной безопасности России закреплено в **Доктрине информационной безопасности Российской Федерации**. Она определяет информационную безопасность как состояние защищенности национальных интересов в информационной сфере. Это состояние достигается благодаря балансу интересов личности, общества и государства и требует комплексного подхода: от защиты прав граждан до обороны критической инфраструктуры.

Доктрина подчеркивает, что обеспечение информационной безопасности возможно только при одновременном развитии правовых норм, организационных механизмов, технических средств защиты информации (СЗИ) и кадрового потенциала.

3.3. Федеральный закон № 149-ФЗ

Более конкретно вопросы применения информационных технологий и защиты информации регулируются Федеральным

законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Этот закон стал базовым для всей сферы информатизации и закрепил фундаментальные принципы:

– свободу поиска, получения и распространения информации;

– условия ограничения доступа;

– требования к достоверности и своевременности информации;

– правовой режим информационных систем и сетей;

– нормы об ограничении доступа (например, к персональным данным, государственной тайне, служебной информации).

Принципы 149-ФЗ отражают современное понимание баланса интересов: свобода информации допускается до тех пор, пока она не вступает в противоречие с требованиями безопасности личности, общества и государства.

3.4. Открытая и ограниченная информация

Российское законодательство различает общедоступную информацию и информацию с ограниченным доступом.

Общедоступная информация – это сведения, к которым любой гражданин имеет свободный доступ (например, нормативные акты, общеизвестные факты).

Информация ограниченного доступа – это данные, использование которых регулируется специальными правилами.

К этой категории относятся: государственная тайна, коммерческая тайна, профессиональные тайны (адвокатская, врачебная, банковская, тайна следствия, тайна связи), а также служебная информация.

Особо выделяются сведения, доступ к которым не может быть ограничен: нормативные правовые акты, данные об использовании бюджетных средств, информация об окружающей среде, сведения о деятельности органов государственной власти.

3.5. Государственная тайна и профессиональные тайны

Классическим примером информации ограниченного доступа является государственная тайна. Ее режим регулируется Законом Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне», а перечень сведений утвержден Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203 (ред. от 25.03.2021).

Кроме государственной тайны существует целая система профессиональных тайн: адвокатская, врачебная, банковская, тайна следствия, тайна связи и др. Их регулирование закреплено в профильных законах и подзаконных актах, что подчеркивает комплексность правовой системы.

3.6. Конфиденциальная информация

Важное место в системе правового регулирования занимает Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» (ред. от 13.07.2015).

Документ дополняет систему ограниченного доступа, выделяя сведения, отнесенные к конфиденциальной информации: персональные данные, служебная тайна, информация о сущности изобретений до их публикации и др.

На практике защита такой информации обеспечивается мерами организационного и технического характера, а контроль

возложен на уполномоченные органы – прежде всего ФСТЭК и ФСБ России.

§ 4. Приоритетные направления государственной политики Российской Федерации в области информационной безопасности

Современная политика России в сфере информационной безопасности неразрывно связана с более широким контекстом развития информационного общества и цифровой экономики. Государство стремится одновременно решать две ключевые задачи:

– создать благоприятную среду для инноваций и свободного обмена информацией;

– минимизировать риски и угрозы, связанные с использованием информационно-телекоммуникационных технологий.

4.1. Стратегия развития информационного общества

Основополагающим документом здесь выступает **Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы.** Она утверждена **Указом Президента Российской Федерации от 9 мая 2017 г. № 203** и определяет цели и задачи государственной политики в цифровой сфере.

Согласно Стратегии, ключевыми приоритетами являются:

– построение национальной цифровой экономики;

– развитие отечественных технологий и снижение зависимости от зарубежных решений;

– формирование современного правового режима использования данных;

– обеспечение доверия граждан к государственным цифровым сервисам;

– защита конституционных прав и свобод личности в информационной сфере.

Особо отмечается необходимость гарантировать суверенитет России в киберпространстве и устойчивость национальной критической информационной инфраструктуры (КИИ).

4.2. Основы государственной политики в области международной информационной безопасности

Глобализация информационного пространства неизбежно приводит к появлению трансграничных угроз. Поэтому Россия выстраивает стратегию не только внутри страны, но и на международной арене.

Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» стал ключевым документом в этой области.

В нем зафиксированы:

– российская позиция по вопросам киберугроз и их нейтрализации;

– цели по созданию справедливой системы международных правил в сфере информационной безопасности;

– задачи по предотвращению межгосударственных конфликтов в информационном пространстве;

– меры по продвижению российских инициатив на международных площадках (в том числе в рамках ООН и ШОС).

Таким образом, Россия рассматривает кибербезопасность как элемент глобальной безопасности и активно формирует международно-правовые механизмы для ее обеспечения.

4.3. Взаимосвязь с Доктриной информационной безопасности

Нельзя рассматривать данные документы изолированно. **Доктрина информационной безопасности Российской Федерации** остается фундаментом, тогда как Стратегия 2017–2030 и Основы 2021 года задают практическое развитие ее положений.

Если Доктрина определяет концептуальные основы и принципы (баланс интересов личности, общества и государства), то Стратегия и Основы конкретизируют приоритеты:

– в национальной плоскости – цифровая экономика, КИИ, правовой режим данных;

– в международной плоскости – противодействие кибератакам, укрепление сотрудничества и формирование глобальной архитектуры доверия.

4.4. Тенденции и вызовы

Современные вызовы в сфере информационной безопасности выходят за рамки технических проблем. Они включают в себя:

– распространение деструктивного и экстремистского контента в сети Интернет;

– угрозы вмешательства во внутренние дела государств через информационные каналы;

– рост киберпреступности и транснациональных кибератак;

– зависимость цифровой экономики от зарубежного софта и оборудования;

– использование технологий искусственного интеллекта в целях манипулирования общественным мнением.

Ответом государства на эти вызовы является системный подход: правовое регулирование, техническое импортозамещение,

развитие национальных платформ и усиление международного сотрудничества.

§ 5. Ответственность за нарушения в сфере защиты информации

Как отмечалось ранее, правовое регулирование информационных отношений в России строится на балансе интересов личности, общества и государства. Однако сама по себе система запретов и ограничений не гарантирует защищенность информации. Важным элементом является механизм юридической ответственности, который обеспечивает неотвратимость наказания за нарушения в сфере информационной безопасности.

Российское законодательство предусматривает несколько уровней ответственности: административную, гражданско-правовую и уголовную. Их разграничение зависит от характера и тяжести нарушения, а также от последствий, которые наступили для личности, общества или государства.

5.1. Административная ответственность

В соответствии с Кодексом Российской Федерации об административных правонарушениях (КоАП РФ) к административным нарушениям в сфере защиты информации относятся:

– нарушение порядка сбора, хранения, использования или распространения персональных данных (ст. 13.11 КоАП РФ). Санкции включают штрафы: от 1 000 до 3 000 руб. для граждан, от 5 000 до 10 000 руб. для должностных лиц и от 30 000 до 50 000 руб. для юридических лиц;

– нарушение правил защиты информации, в том числе использование несертифицированных средств защиты (ст. 13.12

КоАП РФ). Наказания варьируются от предупреждений до штрафов (до 50 000 руб. для организаций);

– разглашение информации с ограниченным доступом (служебной или коммерческой тайны) (ст. 13.14 КоАП РФ). Санкции: до 1 000 руб. для граждан и до 5 000 руб. для должностных лиц.

Таким образом, административная ответственность применяется в случаях менее тяжких нарушений, когда ущерб либо незначителен, либо не выходит за рамки локальных последствий.

5.2. Гражданско-правовая ответственность

В случаях, когда нарушение влечет имущественный или моральный ущерб, применяются нормы Гражданского кодекса Российской Федерации (ГК РФ).

Наиболее показательные примеры:

– ст. 139 ГК РФ закрепляет право на коммерческую тайну и предусматривает возмещение убытков при ее разглашении;

– ст. 151 ГК РФ обязывает компенсировать моральный вред, причиненный неправомерным распространением персональных данных или иной конфиденциальной информации.

Гражданско-правовая ответственность ориентирована прежде всего на восстановление нарушенных прав владельцев информации и компенсацию причиненного ущерба.

5.3. Уголовная ответственность

Наиболее серьезные посягательства на информационную безопасность квалифицируются как преступления и наказываются в рамках Уголовного кодекса Российской Федерации (УК РФ).

Среди ключевых статей:

– ст. 137 УК РФ – незаконное собирание или распространение сведений о частной жизни (лишение свободы до 2 лет);

– ст. 138 УК РФ – нарушение тайны переписки, телефонных переговоров и иных сообщений (до 1 года лишения свободы);

– ст. 183 УК РФ – незаконное получение или разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (до 7 лет лишения свободы);

– ст. 272 УК РФ – неправомерный доступ к компьютерной информации, повлекший модификацию, уничтожение или копирование данных (до 5 лет лишения свободы);

– ст. 274 УК РФ – нарушение правил эксплуатации средств хранения и передачи компьютерной информации, если это повлекло тяжкие последствия (до 5 лет лишения свободы).

Уголовная ответственность отражает высокий уровень общественной опасности подобных деяний и играет превентивную роль в защите критически важных информационных ресурсов.

5.4. Дополнительные меры воздействия

Помимо штрафов и уголовных наказаний законодательство предусматривает и иные меры воздействия на нарушителей:

– приостановление деятельности организаций, допустивших нарушения;

– аннулирование лицензий на эксплуатацию информационных систем;

– блокировка интернет-ресурсов или отдельных сервисов;

– предписание об устранении нарушений в установленный срок.

Эти меры имеют административно-принудительный характер и направлены на восстановление законного порядка в сфере защиты информации.

5.5. Взаимосвязь ответственности с государственной политикой

Важно отметить, что система ответственности не существует сама по себе. Она встроена в общую структуру государственной политики информационной безопасности. Если Стратегия 2017–2030 годов и Основы международной политики 2021 года определяют стратегические приоритеты, то нормы КоАП РФ, ГК РФ и УК РФ формируют механизм практической реализации этих целей через санкции и правоприменительную практику.

Таким образом, можно утверждать: система юридической ответственности в России является ключевым элементом национальной модели информационной безопасности, увязывающим воедино принципы права и практику их применения.

Учебно-методический раздел к главе 1

Цели учебного занятия

– Освоить систему нормативных правовых документов, регулирующих защиту информации в Российской Федерации.

– Сформировать представление о механизмах обеспечения информационной безопасности на уровне государства, организаций и личности.

– Развить умение анализировать правовые акты и применять их к конкретным практическим ситуациям.

– Выработать навыки командного взаимодействия и критического мышления при решении кейсов и дискуссионных вопросов.

Вопросы для семинарского занятия

Как соотносятся конституционные гарантии свободы информации и ограничения, связанные с защитой частной жизни и государственной тайны?

Какие международные правовые документы оказали наибольшее влияние на российскую систему информационной безопасности?

Как эволюционировало законодательство России в сфере информации: от фрагментарных норм в кодексах к системе специальных законов?

Какова роль Федерального закона № 152-ФЗ «О персональных данных» и Постановления Правительства № 1119 в формировании режима защиты информации?

Какое место занимают нормативно-технические документы (ГОСТы, руководящие документы ФСТЭК, приказы ФСБ) в системе правового регулирования?

Какие современные вызовы в сфере информационной безопасности обозначены в Доктрине 2016 г. и Стратегии развития информационного общества (2017–2030)?

Практические задания

1. Анализ нормативных документов. Изучить Федеральный закон № 152-ФЗ «О персональных данных». Подготовить краткий обзор его положений. Выделить меры защиты информации и ответственность за их нарушение.

2. Разработка политики информационной безопасности. Составить проект локального акта для небольшой компании: меры защиты данных, алгоритм реагирования на инциденты, ответственность сотрудников.

3. Практическое задание

3. 1. Баланс прав и ограничений

Задание: разберите конкретные статьи Конституции Российской Федерации (ст.ст. 23, 24, 29) и сопоставьте их с нормами закона «О государственной тайне». Подготовьте аргументы «за» и «против» усиления ограничений в сфере информационной безопасности.

Цель: развить навык анализа коллизий правовых норм и умение аргументировать позицию.

3.2. Международные документы

Задание: составьте таблицу, где сопоставьте положения Всеобщей декларации прав человека (ст. 19), Европейской конвенции (ст. 10) и Конвенции Совета Европы 1981 г. с российским законодательством (149-ФЗ и 152-ФЗ).

Цель: научить студентов видеть преемственность и различия международных и национальных норм.

3.3. Эволюция законодательства

Задание: составьте хронологическую ленту развития законодательства Российской Федерации в сфере информации (от Закона 1991 г. «О СМИ» до Стратегии 2017–2030). Выделите ключевые этапы и их значение.

Цель: закрепить понимание исторической динамики и причин изменений в законодательстве.

3.4. 152-ФЗ и 1119-ПП

Задание: проанализируйте Федеральный закон № 152-ФЗ и постановление Правительства № 1119. Определите, какие конкретные требования предъявляются к операторам информационных систем персональных данных.

Цель: развить практические навыки работы с нормативными документами.

3.5. Роль ФСТЭК и ФСБ

Задание: подготовьте мини-доклад о роли ФСТЭК России и ФСБ России в обеспечении информационной безопасности. Включите примеры приказов или руководящих документов, которые применяются на практике.

Цель: научить работать с подзаконной базой и видеть ее связь с законами.

3.6. Современные вызовы и стратегии

Задание: на основе Доктрины информационной безопасности (2016) и Стратегии 2017–2030 выделите не менее трех вызовов и предложите меры по их преодолению.

Цель: развить аналитическое мышление и способность предлагать решения.

Иные формы обучения

– **Деловая игра**: роли «компания», «хакеры», «регуляторы». Моделирование атаки и защиты данных.

– **Мозговой штурм** «Как улучшить защиту персональных данных в социальных сетях?».

– **Ролевая игра** «Утечка данных в компании» – разработка антикризисного плана.

– **Дискуссия** «Баланс между свободой информации и защитой персональных данных».

– **Круглый стол** «Современные угрозы информационной безопасности и пути их нейтрализации».

Библиографический список к главе 1

Международные документы

1. Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) // Организация Объединенных Наций [сайт]. – URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 18.07.2025).

2. Европейская конвенция о защите прав человека и основных свобод (заключена в г. Риме 04.11.1950) // URL: https://www.echr.coe.int/documents/d/echr/Convention_RUS (дата обращения: 18.07.2025).

3. Международный пакт о гражданских и политических правах (принят Генеральной Ассамблеей ООН 16.12.1966) // Организация Объединенных Наций [сайт]. – URL: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (дата обращения: 04.08.2025).

4. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981, вступила в силу для Российской Федерации в 2005 г.) // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/ document/cons_doc_LAW_121499/ (дата обращения: 04.08.2025).

Конституция и кодифицированные акты

5. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993, с изм., одобренными 01.07.2020) // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 11.12.2025).

6. Гражданский кодекс Российской Федерации : ГК : принят Государственной Думой 24 ноября 2006 г. : одобрен Советом Федерации 8 декабря 2006 г. // СПС «КонсультантПлюс». – URL:

https://www.consultant.ru/document/cons_doc_LAW_64629/ (дата обращения: 04.08.2025).

7. Трудовой кодекс Российской Федерации : ТК : принят Государственной Думой 21 декабря 2001 г. : одобрен Советом Федерации 26 декабря 2001 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 04.08.2025).

8. Уголовный кодекс Российской Федерации : УК : принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 04.08.2025).

9. Кодекс Российской Федерации об административных правонарушениях : КоАП : принят Государственной Думой 20 декабря 2001 г. : одобрен Советом Федерации 26 декабря 2001 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 04.08.2025).

Федеральные законы

10. Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» Российской Федерации // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_1511/ (дата обращения: 04.08.2025).

11. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_2481/ (дата обращения: 04.08.2025).

12. Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» (документ утратил силу) // СПС «КонсультантПлюс». – URL: https://www.

consultant.ru/document/cons_doc_LAW_5887/ (дата обращения: 04.08.2025).

13. Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене» (документ утратил силу) // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_10929/ (дата обращения: 04.08.2025).

14. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_37867/ (дата обращения: 04.08.2025).

15. Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (документ утратил силу) // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_34838/ (дата обращения: 04.08.2025).

16. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 04.08.2025).

17. Федеральный закон от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_51043/ (дата обращения: 04.08.2025).

18. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 04.08.2025).

19. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 04.08.2025).

20. Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_103037/ (дата обращения: 04.08.2025).

21. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_108546/ (дата обращения: 04.08.2025).

22. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 04.08.2025).

23. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 04.08.2025).

Доктрины и стратегии

24. Доктрина информационной безопасности Российской Федерации (утв. Президентом Российской Федерации 05.12.2016 № Пр-1895) // НПП «Гарант-сервис». – URL: https://base.garant.ru/71556224/(дата обращения: 04.08.2025).

25. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (утв. Указом Президента Российской Федерации от 09.05.2017 № 203) // НПП «Гарант-сервис». – URL: https://base.garant.ru/71670570/ (дата обращения: 04.08.2025).

Указы Президента Российской Федерации

26. Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне» // Президент России [сайт]. – URL: http://www.kremlin.ru/acts/bank/8549 (дата обращения: 04.04.2025).

27. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» // НПП «Гарант-сервис». – URL: https://base.garant.ru/10200083/ (дата обращения: 11.12.2025).

28. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы ФСТЭК России» // URL: https://hub.zlonov.ru/ (дата обращения: 11.12.2025).

29. Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_381999/ (дата обращения: 04.04.2025).

Постановления Правительства Российской Федерации

30. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «О требованиях к материальным носителям биометрических персональных данных и технологиям хранения вне информационных систем персональных данных» // НПП «Гарант-сервис». – URL: https://base.garant.ru/193541/ (дата обращения: 13.10.2024).

31. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс». –

URL: https://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/ (дата обращения: 13.10.2024).

Приказы и ведомственные документы

32. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» // НПП «Гарант-сервис». – URL: https://base.garant.ru/70690918/ (дата обращения: 13.10.2024).

33. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» // НПП «Гарант-сервис». – URL: https://www.garant.ru/products/ipo/prime/doc/70351476/ (дата обращения: 13.10.2024).

34. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 мая 2017 г. № 94 «Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных…» // НПП «Гарант-сервис». – URL: https://www.garant.ru/products/ipo/prime/doc/71652212/ (дата обращения: 13.10.2024).

Стандарты и руководящие документы

35. Национальный стандарт Российской Федерации. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» // База ГОСТ,

ГОСТ Р – национальные стандарты РФ. – URL: https://rosgosts.ru/file/gost/03/060/gost_r_57580.1-2017.pdf (дата обращения: 13.05.2024).

36. Национальный стандарт Российской Федерации. ГОСТ Р ИСО/МЭК 27001-2012. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» // «Русский Регистр». – URL: https://rusregister.ru/standards/iso-РД «Защита от НСД к информации. Термины и определения» (утв. решением Гостехкомиссии при Президенте Российской Федерации от 30.03.1992). – М. : Гостехкомиссия России, 1992.

37. РД «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД» (утв. Гостехкомиссией при Президенте Российской Федерации 30.03.1992). – URL: https://uchebana5.ru/cont/1557275.html (дата обращения: 23.09.2024).

38. РД «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» (утв. Гостехкомиссией при Президенте Российской Федерации 30.03.1992). – URL: https://uchenie.top/articles/fstek-avtomatizirovannaya-sistema-opredelenie.html (дата обращения: 21.12.2024).

Глава 2. КОМПЬЮТЕРНАЯ РАЗВЕДКА В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В ИНФОРМАЦИОННОЙ СФЕРЕ

ВВЕДЕНИЕ

Современное общество переживает глубокую трансформацию, обусловленную двумя взаимосвязанными процессами, – **цифровизацией** и **виртуализацией** социальной реальности. Эти процессы изменяют не только характер коммуникаций, но и формы организации общественной жизни, создавая одновременно новые возможности и новые угрозы.

Под цифровизацией понимается глобальный процесс внедрения цифровых технологий во все сферы деятельности человека: от промышленного производства и экономики до образования, здравоохранения и государственного управления. Наибольшую значимость в этом процессе приобретают такие технологии, как **искусственный интеллект (ИИ)**, анализ больших данных, квантовые вычисления, нейротехнологии, интернет вещей (IoT), облачные сервисы, робототехника, а также виртуальная и дополненная реальность. Особую роль среди них играет именно искусственный интеллект, позволяющий решать задачи обработки естественного языка, распознавания образов, прогнозирования и принятия решений в условиях неопределенности.

Виртуализация же связана с проникновением цифровых сред в сферу индивидуальной и коллективной жизни. Люди все чаще взаимодействуют друг с другом не напрямую, а через виртуальные коммуникационные каналы, будь то социальные сети, мессенджеры или форумы. Тем самым формируется своеобразное виртуализированное общество, где значительная часть социально значимой информации циркулирует в цифровой форме.

Для органов, осуществляющих **оперативно-разыскную деятельность** (ОРД), подобные изменения означают необходимость пересмотра традиционных методов работы. Если раньше основными каналами получения сведений были личные контакты, наблюдение и работа с документами, то сегодня все чаще приходится иметь дело с так называемыми **цифровыми следами**. Эти следы остаются при использовании мобильных устройств, посещении интернет-ресурсов, взаимодействии в социальных сетях. Именно они становятся важным источником информации о событиях, фактах и личностях, представляющих интерес для правоохранительных органов.

Таким образом, цифровизация и виртуализация формируют новые вызовы для ОРД, делая необходимым развитие таких направлений, как **компьютерная разведка**.

§ 1. Основные понятия и определения компьютерной разведки

В последние десятилетия все большее распространение получает деятельность, связанная с поиском и получением информации из открытых и закрытых информационных систем, и с контролем за сообщениями, передаваемыми через компьютерные сети. Для ее обозначения используются различные термины: «компьютерная разведка», «киберразведка», «компьютерный поиск», «аналитическая разведка», «компьютерный мониторинг» и др. Однако до настоящего времени в нормативных правовых актах и научной литературе отсутствует единое понимание сущности, задач и методов компьютерной разведки.

Исторически термин «аналитическая разведка» впервые был введен в нормативные документы МВД России в 1992 г. для обозначения особой формы деятельности оперативно-разыскных

подразделений милиции. Под ней понимался комплексный анализ материалов скрытого наблюдения и оперативной установки, разведывательного поиска, технической разведки, а также изучение информации СМИ, статистики и автоматизированных банков данных. Компьютерная разведка рассматривалась как один из видов аналитической разведки, применяемый для мониторинга компьютерных систем.

Сегодня в научной литературе встречаются разные трактовки этого понятия. Так, С. С. Овчинский определяет компьютерную разведку как оперативно-разыскное мероприятие, заключающееся в поиске и получении информации из компьютерных систем и сетей. А. И. Доронин и С. К. Мисюк связывают ее с аналитической обработкой больших объемов данных из открытых источников (прежде всего интернета). Д. Б. Халяпин трактует ее как вид технической разведки, основанный на использовании специальных средств, а В. К. Ржавский – как разновидность радиоэлектронной разведки, включающей перехват и анализ побочных электромагнитных излучений.

С точки зрения военной науки компьютерная разведка – новейший вид технической разведки, возникший в рамках концепции информационной войны. Но в условиях ОРД у нее есть свои особенности. Здесь компьютерная разведка используется, прежде всего, как инструмент профилактики, выявления, предотвращения и раскрытия преступлений.

В таком контексте ***компьютерная разведка – это оперативно-разыскное мероприятие, заключающееся в целенаправленном поиске и получении информации из компьютерных систем и сетей, осуществляемое работниками оперативных или оперативно-технических подразделений с целью получения оперативно значимой информации криминогенного и криминального характера.***

Сущность компьютерной разведки заключается в добывании:

– компьютерной информации, обрабатываемой, хранимой и передаваемой в информационно-телекоммуникационных сетях (ИТС);

– данных о характеристиках программных, аппаратных и программно-аппаратных комплексов, используемых в ИТС;

– сведений о методах, способах и механизмах защиты информации в ИТС;

– персональной информации о пользователях ИТС.

Глобальная цель компьютерной разведки – информационное обеспечение должностных лиц органов управления в процессе выработки ими управленческих решений.

Важно подчеркнуть: в отличие от других видов технической разведки компьютерная разведка не привязана к конкретным физическим полям или сигналам. Ее основным методом является несанкционированный доступ (НСД) к информации, циркулирующей в ИТС.

Ключевые направления ее применения в ОРД включают:

– поиск информации, свидетельствующей о противоправных действиях;

– сбор данных о физических и юридических лицах, предметах и событиях, связанных с противоправной деятельностью;

– проведение активных мероприятий в компьютерных сетях (оперативный опрос, эксперимент, закупка и др.).

Необходимость нормативного закрепления понятия «компьютерная разведка» назрела давно. В качестве одного из шагов в этом направлении Министерством внутренних дел Российской Федерации был разработан проект федерального закона «О внесении изменения в статью 6 Федерального закона "Об оперативно-розыскной деятельности"». Документ был опубликован

на портале проектов федеральных нормативных актов 14 августа 2023 г. (ID проекта 01/05/08-23/00140881).

Согласно пояснительной записке, целью законопроекта являлось законодательное закрепление возможности оперативного исследования информации, представленной в форме электрических сигналов, независимо от средств ее хранения, обработки и передачи. Такой подход полностью согласуется с примечанием к ст. 272 УК РФ, где под **компьютерной информацией** понимаются сведения (сообщения, данные), представленные в форме электрических сигналов.

Особое внимание в законопроекте уделялось трудностям документирования преступлений, совершаемых с использованием банковских карт, сети Интернет, мобильной связи и компьютерной техники. Эти преступления осложняются применением злоумышленниками сервисов **виртуальной частной сети VPN (Virtual Private Network** – виртуальная частная сеть, создающая зашифрованный канал поверх другой сети), которые позволяют устанавливать зашифрованные безопасные соединения поверх другой сети, а также возможностями подмены телефонных номеров при помощи **протокола установления сеанса Session Initiation Protocol (SIP)**, когда аналоговый сигнал преобразуется в цифровой и обратно.

Несмотря на очевидную актуальность, инициатива пока остается нереализованной. Однако ее принятие стало бы серьезным шагом в развитии ОРД, открыв правовое пространство для использования новейших технологий в выявлении и пресечении преступлений, совершаемых с применением информационно-коммуникационных технологий (ИКТ).

Для повышения эффективности применения компьютерной разведки на практике особое значение имеет развитие технологий интеллектуального анализа данных. Здесь выделяются такие направления, как:

– **семантический анализ информации** – процесс извлечения смысла и контекста из данных, позволяющий выявлять ключевые темы и отношения между ними;

– **Knowledge Discovery** – процесс обнаружения полезных знаний в сырых данных;

– **Data Mining** – поиск в больших объемах данных неочевидных, объективных и полезных закономерностей, основанный на выявлении скрытых шаблонов;

– **Text Mining** – направление обработки текстовой информации, объединяющее методы контент-анализа, компьютерной лингвистики и искусственного интеллекта.

Важным направлением в работе компьютерной разведки становится доступ к так называемой **Deep Web (глубокая сеть)**, которая представляет собой часть интернета, недоступную для индексации традиционными поисковыми системами (Google, Bing, Яндекс и др.). Именно в этой зоне сосредоточено значительное количество информации, потенциально представляющей оперативный интерес.

Наконец, в условиях роста объемов персональных данных и частой их утечки все более актуальным становится **обезличивание информации**, т. е. процесс удаления или изменения идентифицирующих данных, делающий невозможным определение личности конкретного человека.

§ 2. Особенности, формы и виды компьютерной разведки

Современные условия противодействия преступности требуют учитывать ряд особенностей компьютерной разведки, делающих ее одним из ключевых инструментов ОРД.

Во-первых, на современном этапе развития информационно-телекоммуникационных технологий компьютерная разведка

становится одним из наиболее востребованных методов поиска и получения оперативной информации. В отличие от иных способов добывания сведений ее проведение зачастую не требует преодоления сложных рубежей логической защиты: достаточно фиксировать данные, уже циркулирующие в информационных системах (ИС). Главная цель при этом – выявление сведений криминогенного и криминального характера.

Во-вторых, проведение данного мероприятия, как правило, не связано с ограничением конституционных прав граждан и, следовательно, не требует судебного решения. Это делает метод гибким и оперативным.

В-третьих, компьютерная разведка реализуется сотрудниками оперативных или оперативно-технических подразделений с использованием программных, аппаратных либо комбинированных средств. Такие технологии позволяют не только добывать сведения, но и фиксировать, хранить и анализировать их в электронном виде.

В-четвертых, в отличие от радиоэлектронной или технической разведки компьютерная разведка фокусируется не на побочных излучениях и сигналах, а на информации, создаваемой в результате штатного функционирования ИС.

Наконец, ее особенность заключается в возможности использования как пассивных, так и активных методов.

Пассивные методы – перехват и анализ сетевого трафика, изучение цифровых следов, сканирование накопителей, мониторинг активности без вмешательства в работу системы.

Активные методы – внедрение вредоносного программного обеспечения (вирусов, троянов, логических бомб), активирующихся по заданным условиям или внешнему сигналу.

Отдельно стоит выделить **семантический анализ информации** – процесс извлечения смысла и установления связей между

данными. В сочетании с технологиями **Knowledge Discovery** (обнаружение знаний в сырых данных), **Data Mining** (поиск скрытых закономерностей в больших массивах информации) и **Text Mining** (глубокая обработка текстов средствами компьютерной лингвистики и искусственного интеллекта) он превращает разрозненные сведения в основу для принятия управленческих решений.

2.1. Технические направления

С технической точки зрения методы компьютерной разведки можно условно разделить на три группы:

1. **Разведка в системах телекоммуникаций** включает перехват сообщений, прослушивание телефонных разговоров, выявление IP-адресов и местоположения абонентов, расшифровку закодированных сигналов и отслеживание действий пользователей в сети.

2. **Сетевая разведка** – комплекс мероприятий по изучению ресурсов информационных систем, архитектуры, используемого оборудования, программного обеспечения и средств защиты. Цель – выявление уязвимостей и определение границ возможного проникновения.

3. **Интернет-разведка OSINT (Open Source Intelligence)** – систематический поиск информации в открытых источниках (социальные сети, базы данных, форумы, медиа и др.) с последующей машинной обработкой.

При этом важно подчеркнуть, что к методам компьютерной разведки **не относятся**: выведывание сведений через персонал ИТС, использование аппаратных закладок в средствах электронно-вычислительной техники (ЭВТ), физическое проникновение к элементам ИС или передача разведданных через КСС (компьютерные системы и сети).

2.2. Ограничения и трудности

Несмотря на очевидные достоинства, компьютерная разведка сталкивается и с рядом проблем.

Во-первых, это **избыточность данных в Интернете**. По оценкам специалистов, более 97 % информации, представляющей интерес для разведки, недоступно через традиционные поисковые системы: даже такие гиганты, как Google, индексируют лишь малую часть.

Во-вторых, **динамичность цифровой среды**. Данные непрерывно изменяются и удаляются. Системы мониторинга позволяют частично компенсировать этот фактор, но окончательно проблему не решают.

В-третьих, остается **сложность автоматического анализа разнотипных данных** – как структурированных (таблицы, базы данных), так и неструктурированных (тексты). Здесь перспективны упомянутые выше технологии Data Mining и Text Mining.

В-четвертых, значительную сложность представляет доступ к **Deep Web (глубокой сети)** – сегменту Интернета, не индексируемому поисковиками (Google, Bing, «Яндекс»). Именно там хранится массив данных, зачастую более ценный, чем в открытом доступе.

И, наконец, пятая проблема – **анонимизация данных**. Этот процесс направлен на защиту личности пользователя путем удаления или изменения идентифицирующих элементов, что серьезно осложняет деанонимизацию преступников.

По экспертным оценкам, лишь 10–15 % необходимых данных доступны в готовом виде, тогда как 85–90 % приходится добывать путем анализа и сопоставления разрозненных источников.

Таким образом, компьютерная разведка в условиях цифровой трансформации общества является не только техническим

приемом, но и комплексной системой добывания и анализа сведений. Ее эффективность зависит от сочетания нормативного регулирования, технических решений и уровня подготовки кадров. Новые возможности, открываемые **машинным обучением и искусственным интеллектом**, позволяют говорить о переходе к более высокому уровню разведывательной аналитики, где технологии становятся не заменой, а партнером человеческого анализа.

§ 3. Технологии применения компьютерной разведки в борьбе с преступлениями в информационной сфере

Когда мы говорим о компьютерной разведке, важно понимать, что речь идет не просто о технических приемах, а о целой системе, которая шаг за шагом становится неотъемлемой частью ОРД. Современные технологии дают возможность работать с гигантскими массивами данных, и вопрос здесь не только в том, где найти информацию, но и как ее превратить в реальные знания, полезные для практики.

Наиболее ярким примером таких решений выступают **информационно-аналитические системы компьютерной разведки (ИАС КР)**.

Специализированные информационно-аналитические системы позволяют не просто фиксировать данные, а превращать их в осмысленные знания для практического применения. В состав таких систем входят:

– комплексы контент-мониторинга, обеспечивающие сбор информации из открытых сетей – веб-пространства, социальных сетей, блогов, видеохостингов и мессенджеров;

– средства экстрагирования понятий, извлекающие из массивов текстов данные о событиях, лицах, организациях;

– инструменты визуализации информационных связей, выявляющие аномалии и неочевидные закономерности;

– модули формирования аналитических документов, подготавливающие отчеты и рекомендации для лиц, принимающих решения (ЛПР).

Формирование базы данных ИАС КР осуществляется через прямое подключение к сети Интернет и охватывает веб-сайты, блоги (LiveJournal, «Яндекс.Дзен», VK), социальные сети (OK.ru, TikTok и др.), видеосервисы (RuTube, VK Видео, «Яндекс.Видео»), мессенджеры (Telegram, Viber, WhatsApp). Для эффективности требуется настройка модулей автоматического сканирования и создание служебных аккаунтов для работы с ограниченным контентом.

В профессиональной литературе этот процесс часто описывают как разведывательный цикл, включающий пять этапов:

– целеуказание и планирование (определение задач, стратегии, источников);

– сбор данных (получение информации из разнообразных каналов);

– обработка сведений (учет, классификация, верификация, хранение);

– анализ и синтез (превращение «сырых» данных в новые знания, выводы, прогнозы);

– доведение до ЛПР в понятной форме (справки, отчеты, визуализация).

Характерной особенностью разведывательного цикла является его адаптивность: при необходимости он может быть сокращен до упрощенного анализа, а итоговые документы всегда должны быть четкими, лаконичными и лишенными ссылок на конфиденциальные источники. Важно и то, что подача материала подстраивается под восприятие ЛПР: известен пример,

когда аналитические отчеты ЦРУ президенту США Рональду Рейгану готовились в виде видеороликов, поскольку этот формат был для него наиболее доступным.

Работа с огромными массивами данных в Интернете требует применения специализированных поисковых инструментов, которые можно разделить на подгруппы:

– средства поиска по отдельным сайтам;

– каталоги и подборки ссылок;

– классические поисковые системы (Google, Bing, «Яндекс»);

– мета-поисковые системы, агрегирующие результаты сразу из нескольких источников;

– системы мониторинга и контент-анализа;

– экстракторы объектов и событий;

– технологии Knowledge Discovery, Data Mining, Text Mining;

– специализированные и интегрированные системы компьютерной разведки.

Так, каталоги и поисковые системы сходны по результату, но принципиально различаются механизмами: каталоги пополняются вручную, а поисковые системы используют роботов для постоянного сканирования веб-пространства. Мета-поисковые системы интегрируют результаты, что делает их более информативными. Мониторинговые платформы позволяют отслеживать динамику информационного потока, а экстракторы объектов выделяют из него неизвестные заранее факты (например, фиксация необычного события – выезда автомобиля без номерных знаков за пределы города) [60].

Отдельно стоит отметить использование технологий Data Mining, Text Mining и Knowledge Discovery. Эти методы позволяют находить неочевидные связи, например установить факт знакомства между двумя людьми на основании данных об учебе

в одной школе и в одном классе, даже если они не упоминают друг друга напрямую [61].

Особый интерес представляют интегрированные системы, которые объединяют все доступные поисковые и аналитические ресурсы, создавая логически связанные массивы информации для дальнейшего анализа.

Практическая ценность методов компьютерной разведки особенно заметна на простом примере – регистрации пользователя на сайте. При создании учетной записи пользователь указывает личные данные (ФИО, телефон, e-mail, город), которые автоматически сохраняются вместе с технической информацией: датой регистрации, IP-адресом, данными браузера и операционной системы. Эти сведения фиксируются скрытно и нередко используются владельцем сайта для внутренней статистики или блокировок. Однако та же информация может стать бесценным источником для оперативных подразделений: по IP-адресу можно установить геолокацию, по метаданным – выявить устройство, а по стилю активности – связать аккаунт с другими цифровыми следами [62; 63].

Таким образом, технологии компьютерной разведки – это не только сбор информации ради информации. Это умение превратить хаос цифровых следов в стройную картину, позволяющую не только раскрывать преступления, но и предугадывать угрозы. И именно это делает компьютерную разведку сегодня одним из ключевых инструментов борьбы с киберпреступностью.

§ 4. Проблемы, возникающие при проведении компьютерной разведки, и возможные пути их решения

Несмотря на очевидную значимость компьютерной разведки, ее практическая реализация сопряжена с целым рядом трудностей, которые приходится учитывать при планировании и про-

ведении оперативно-разыскных мероприятий. Эти проблемы затрагивают как техническую, так и правовую сторону, требуя комплексного подхода к их преодолению.

Во-первых, злоумышленники нередко используют при регистрации на сайтах заведомо ложные данные или применяют сервисы анонимизации, такие как VPN или прокси-серверы. В результате реальная личность и местоположение пользователя скрываются, что существенно затрудняет идентификацию. Особенно остро эта проблема стоит тогда, когда оперативные подразделения не имеют доступа к технической статистике ресурса или логам серверов.

Во-вторых, даже в условиях анонимизации у злоумышленников остаются цифровые следы, которые при правильной обработке могут стать ключом к их деанонимизации. Важнейшую роль здесь играет работа с метаданными – скрытой информацией, автоматически прикрепляемой к файлам. Метаданные могут содержать дату и время создания документа, координаты места съемки фотографии, модель устройства и даже название программы, в которой производилось редактирование. Для их анализа применяются специальные инструменты:

– *Photoinvestigator* (photoinvestigator.co) – сервис, позволяющий определить геолокацию и устройство, на котором был сделан снимок;

– *ExifTool* (exiftool.org) – универсальная утилита для чтения и редактирования метаданных в различных форматах файлов.

В-третьих, важное направление работы связано с анализом IP-адресов и сетевой активности. Даже если пользователь пытается скрыться за VPN или прокси, его сетевой трафик может раскрыть реальные точки входа. Здесь применяются такие инструменты, как *Wireshark* (wireshark.org) – анализатор сетевого трафика, фиксирующий IP-адреса, протоколы и подозрительные

пакеты, и *Nmap* (nmap.org) – программа для сканирования сетей, выявляющая активные устройства и открытые порты.

В-четвертых, особое значение имеет деанонимизация через открытые источники OSINT (*Open Source Intelligence*). Многие пользователи сами оставляют цифровые следы в социальных сетях, форумах, блогах и комментариях. При грамотной аналитике эти данные можно объединить в информационный портрет. Для этого используются:

– *Maltego* (maltego.com) – платформа, визуализирующая связи между людьми, организациями, доменами и IP-адресами;

– *SpiderFoot* (github.com/smicallef/spiderfoot) – инструмент, автоматически собирающий данные из десятков открытых источников.

В-пятых, важным направлением становится поведенческий анализ. Даже под маской анонимного аккаунта человека выдает стиль его письма, частоту входов, выбор тем и круг интересов. Анализ таких «цифровых привычек» позволяет сопоставить разные учетные записи и установить реальную личность. В этом помогают:

– *Sentinel Visualizer* (fmsasg.com) – инструмент для визуализации связей и выявления аномалий;

– *IBM i2 Analyst's Notebook* (ibm.com) – профессиональная система для анализа данных и поиска скрытых закономерностей.

Шестая трудность – работа с цифровыми следами в мессенджерах (Telegram, WhatsApp, Viber и др.), которые активно используются в преступной среде. Для их изучения применяются:

– *Cellebrite* (cellebrite.com) – комплекс для извлечения данных с мобильных устройств;

– *Magnet AXIOM* (magnetforensics.com) – универсальная платформа анализа цифровых следов.

Седьмая проблема связана с необходимостью мониторинга активности в социальных сетях и блогах. Для этого применя-

ются системы контент-мониторинга: *Brandwatch* (brandwatch.com) и *Hootsuite* (hootsuite.com), позволяющие анализировать динамику публикаций и управлять аккаунтами.

Наконец, существенные трудности вызывает поиск информации в глубокой сети (Deep Web), недоступной для традиционных поисковых систем. Для этого используются специализированные инструменты: *Website-Finder* (softpedia.com), *dtSearch* (dtsearch.com), *InfoNgen* (infongen.com), *CIRadar* (ciradar.com).

Для анализа скрытых взаимосвязей применяются также комплексные решения: *InfoStream* (infostream.ua), *CyberAggregator*, *PolyAnalyst* (megaputer.ru), *SAP BusinessObjects Text Analysis* (sap.com), *Neticle Text Analysis* (neticle.com), позволяющие составлять цифровые портреты, выявлять скрытые связи и закономерности.

Таким образом, проблемы компьютерной разведки обусловлены не только техническими барьерами, но и особенностями поведения пользователей, стремящихся к анонимности. Решение этих задач требует сочетания современных аналитических систем, инструментов работы с цифровыми следами и профессиональной подготовки специалистов. Только при таком подходе компьютерная разведка сможет превратиться в по-настоящему эффективный инструмент противодействия преступлениям в информационной сфере.

Учебно-методический раздел к главе 2

Цели изучения темы

1. Сформировать у студентов целостное представление о сущности и содержании компьютерной разведки как одного из ключевых инструментов ОРД.

2. Освоить основные понятия, формы и методы компьютерной разведки, ее особенности в условиях цифровизации и виртуализации общества.

3. Научить анализировать технические и организационные направления компьютерной разведки, выявлять ее возможности и ограничения.

4. Сформировать навыки работы с современными инструментами анализа цифровых следов, OSINT и системами контент-мониторинга.

5. Развить умение сопоставлять теоретические знания с практикой противодействия преступлениям в информационной сфере.

Вопросы для семинарского занятия

1. Каковы особенности становления и развития компьютерной разведки в России?

2. Чем отличается компьютерная разведка от иных видов технической разведки?

3. Как цифровизация и виртуализация общества влияют на задачи и методы ОРД?

4. Какие технические направления компьютерной разведки (телекоммуникационная, сетевая, интернет-разведка) наиболее значимы в современной практике?

5. С какими основными проблемами сталкиваются оперативные сотрудники при проведении компьютерной разведки?

6. Каковы перспективы использования искусственного интеллекта и Data Mining в развитии методов компьютерной разведки?

Практические задания

1. **Анализ метаданных.** Используя ExifTool или Photo-investigator, извлеките метаданные из цифрового изображения и определите геолокацию, дату создания и параметры устройства.

2. **Сетевая разведка.** С помощью Nmap выполните сканирование локальной сети, определите активные устройства и открытые порты, составьте отчет об уязвимостях.

3. **OSINT-исследование.** На основе Maltego или SpiderFoot создайте информационный портрет пользователя по его открытому аккаунту в социальной сети.

4. **Контент-мониторинг.** Используя систему (Brandwatch или Hootsuite), отследите динамику информационного потока по выбранной теме и сделайте выводы о тенденциях.

5. **Сравнительный анализ систем.** Сравните возможности Website-Finder, dtSearch и CIRadar, определите их сильные и слабые стороны для задач компьютерной разведки.

Иные формы обучения

– **Деловая игра**: студенты разделяются на оперативников и киберпреступников; задача первых – выявить цифровые следы и деанонимизировать злоумышленников.

– **Мозговой штурм** на тему «Как повысить эффективность компьютерной разведки в условиях Big Data?».

– **Ролевая игра**: моделирование ситуации утечки информации с участием оперативников, IT-специалистов и юристов.

– **Круглый стол** «Этические и правовые границы компьютерной разведки».

Библиографический список к главе 2

Нормативные правовые акты

1. Уголовный кодекс Российской Федерации : УК : принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 04.08.2025).

2. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

3. Проект федерального закона «О внесении изменения в статью 6 Федерального закона «Об оперативно-розыскной деятельности» // НПП «Гарант-сервис». – URL: https://base.garant.ru/56967150/ (дата обращения: 04.08.2025).

Книги, статьи

4. Артемьев, А. А. Компьютерная разведка в системе ОРД / А. А. Артемьев. – М. : Юрлитинформ, 2020.

5. Халяпин, Д. Б. Технические средства оперативного поиска / Д. Б. Халяпин. – СПб. : Питер, 2019.

6. Ржавский, В. К. Радиоэлектронная разведка: теория и практика / В. К. Ржавский. – М. : Академический проект, 2018.

7. Денисов, С. А. Методы компьютерной разведки / С. А. Денисов // Вестник МВД. 2021. № 5.

8. Осипенко, А. Л. Цифровизация общества и виртуализация реальности: усложнение вызовов и расширение перспектив оперативно-розыскной деятельности / А. Л. Осипенко // Оперативно-розыскная деятельность в цифровом мире : сборник научных трудов / под ред. В. С. Овчинского. – М. : Инфра-М, 2021.

9. Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP / [А. А. Барсегян и др.]. – 2-е изд., перераб. и доп. – СПб. : БХВ-Петербург, 2007.

10. Russell, S. Artificial Intelligence: A Modern Approach / S. Russell, P. Norvig. 4th ed. Pearson, 2021.

11. Anderson R. Security Engineering. Wiley, 2020.

12. Han J., Kamber M., Pei J. Data Mining: Concepts and Techniques. – 4th ed. – Elsevier, 2022.

13. Ovchinsky, S. S. Cyber Intelligence in Law Enforcement / S. S. Ovchinsky. – M. : Юрлитинформ, 2021.

Электронные ресурсы

14. Что такое VPN (Virtual Private Network)? // Лаборатория Касперского [сайт]. – URL: https://www.kaspersky.ru/resource-center/definitions/vpn (дата обращения: 25.08.2025).

15. Что такое SIP (Session Initiation Protocol)? // Cisco [сайт]. – URL: https://www.cisco.com/c/ru_ru/solutions/collateral/enterprise-Deep Web (глубокая сеть) // Лаборатория Касперского [сайт]. –URL: https://www.kaspersky.ru/resource-center/threats/deep-web (дата обращения: 25.08.2025).

16. ExifTool – утилита для чтения и редактирования метаданных [сайт]. – URL: https://exiftool.org (дата обращения: 25.08.2025).

17. Wireshark – анализатор сетевого трафика [сайт]. – URL: https://www.wireshark.org (дата обращения: 25.08.2025).

18. Nmap – инструмент для сканирования сетей [сайт]. – URL: https://nmap.org (дата обращения: 25.08.2025).

19. Maltego – инструмент для визуализации связей [сайт]. – URL: https://www.maltego.com (дата обращения: 25.08.2025).

20. SpiderFoot – автоматизированный инструмент OSINT // URL: https://github.com/smicallef/spiderfoot (дата обращения: 25.08.2025).

21. Cellebrite – система для извлечения данных с мобильных устройств [сайт]. – URL: https://cellebrite.com (дата обращения: 25.08.2025).

22. Magnet AXIOM – система анализа цифровых следов // URL: https://www.magnetforensics.com (дата обращения: 25.08.2025).

23. Brandwatch – система мониторинга соцсетей [сайт]. – URL: https://www.brandwatch.com (дата обращения: 25.08.2025).

24. Hootsuite – инструмент для управления аккаунтами в соцсетях [сайт]. – URL: https://www.hootsuite.com (дата обращения: 25.08.2025).

25. Website-Finder – поисковая программа // URL: https://www.softpedia.com (дата обращения: 25.08.2025).

26. dtSearch – поисковая программа [сайт]. – URL: https://www.dtsearch.com (дата обращения: 25.08.2025).

27. InfoNgen – агрегатор онлайн-источников [сайт]. – URL: https://www.infongen.com (дата обращения: 25.08.2025).

28. CIRadar – система поиска информации в даркнете [сайт]. – URL: https://www.ciradar.com (дата обращения: 25.08.2025).

29. InfoStream – система контент-мониторинга [сайт]. – URL: https://infostream.ua (дата обращения: 25.08.2025).

30. CyberAggregator – система мониторинга // URL: (актуальный адрес может отличаться).

Глава 3. СРЕДСТВА И ТАКТИКА СКРЫТОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ ИЗ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

ВВЕДЕНИЕ

В современном цифровом обществе информация превратилась в стратегический ресурс, ценность которого зачастую превосходит материальные активы. Сегодня именно она становится главным объектом конкурентной борьбы, политического давления и криминальных посягательств. Киберпространство превратилось в арену противостояния, где злоумышленники постоянно совершенствуют методы скрытого получения данных, а специалисты по безопасности разрабатывают новые подходы к защите.

Актуальность рассматриваемой темы определяется стремительным ростом числа кибератак и масштабом их разрушительных последствий. По данным исследований, каждая успешная атака на корпоративную сеть может обернуться для организации не только многомиллионными убытками, но и серьезными репутационными потерями, нарушением законодательства о защите персональных данных, а в отдельных случаях – полной остановкой бизнес-процессов.

Особую опасность представляют именно скрытые методы получения информации. В отличие от прямых атак они способны действовать в течение долгого времени незаметно, обеспечивая злоумышленникам постоянный доступ к критически важным ресурсам. Здесь речь идет не только о технических приемах, но и о комплексном использовании социальных, психологических и организационных механизмов. От элементарного фишинга до сложнейших атак класса APT (Advanced Persistent Threats) –

все эти формы воздействия требуют глубокого понимания как самих методов их реализации, так и способов противодействия.

Для специалистов в области информационной безопасности изучение механизмов скрытого получения информации имеет не только академическую, но и практическую ценность. Оно позволяет не просто разрабатывать превентивные меры защиты, но и своевременно реагировать на инциденты, минимизируя их последствия. В этом контексте важно не только знание технических средств атаки и защиты, но и понимание тактических приемов, которыми пользуются как преступники, так и специалисты правоохранительных органов при проведении ОРД.

Таким образом, изучение средств и тактики скрытого получения информации из защищенных компьютерных систем имеет двойственную природу. С одной стороны, оно раскрывает возможности злоумышленников, что необходимо учитывать при построении системы кибербезопасности, с другой – позволяет вооружить сотрудников, ответственных за защиту информации, набором эффективных инструментов и практических навыков, способных обеспечить безопасность цифрового пространства.

§ 1. Информация: основные свойства, угрозы и уязвимости

Прежде чем говорить о скрытых методах получения информации, давайте еще раз вернемся к базовым вещам. Что вообще мы понимаем под термином «защищенная информация» и какими свойствами такая информация должна обладать? Согласно общепринятому в теории информационной безопасности подходу, защита информации основывается на так называемой триаде CIA (Confidentiality – Integrity – Availability), где выделяются три ключевых свойства:

Целостность – гарантия того, что данные сохраняют свою первоначальную форму и не подвергаются несанкционированным изменениям. Например, даже малейшее искажение бухгалтерского отчета может повлечь за собой финансовые и юридические последствия

Конфиденциальность – предотвращение несанкционированного доступа к информации. В классическом виде это означает, что посторонний пользователь не должен получить доступ к закрытым базам данных или переписке.

Доступность – обеспечение своевременного доступа к информационным ресурсам для авторизованных пользователей. Бесполезно хранить данные в полной целостности и конфиденциальности, если в нужный момент система окажется недоступной.

Вместе с тем современная практика дополняет базовые свойства рядом дополнительных характеристик:

Неотказуемость – невозможность отказа от совершенных действий. Участники коммуникации не могут отрицать факта отправки или получения сообщения.

Подлинность – уверенность в том, что информация поступила из достоверного источника и не была подменена.

Подотчетность – возможность отследить действия пользователей и установить их ответственность за совершенные операции.

Таким образом, защищенная информация должна одновременно обладать всеми этими свойствами. Нарушение любого из них приводит к инциденту информационной безопасности.

1.1. Угрозы безопасности информации

Любая угроза формируется из трех взаимосвязанных компонентов:

Источник угрозы – лицо, организация или фактор, создающий риск. Это могут быть внешние злоумышленники, внутренние инсайдеры или силы природы.

Уязвимость актива – слабое место в системе, которое может быть использовано источником угрозы.

Способ реализации угрозы – конкретный метод, с помощью которого злоумышленник использует уязвимость для достижения своих целей.

Классическим примером является ситуация, когда хакер (источник угрозы) использует уязвимость веб-приложения (SQL-инъекцию) для получения доступа к базе данных (способ реализации угрозы). В данном случае объектом воздействия выступает сама информация – персональные данные или финансовые сведения.

Источники угроз можно классифицировать следующим образом:

Внешние – хакеры-одиночки, киберпреступные группировки, конкурентные организации.

Внутренние – сотрудники организации с легитимным доступом, в том числе халатные, недовольные, увольняющиеся или намеренно завербованные.

Третьи лица и силы природы – государственные органы, проводящие проверки; природные катастрофы; техногенные аварии; эпидемии и вооруженные конфликты.

Объектом атаки почти всегда остается информация – персональная, коммерческая, технологическая.

1.2. Уязвимость актива: где тонко и почему рвется

Под **уязвимостью** в информационной безопасности понимается недостаток в системе, программном или аппаратном сред-

стве, который может быть использован злоумышленником для нарушения конфиденциальности, целостности или доступности информации [79]. Это определение закреплено как в российских стандартах (ГОСТ Р 56546-2015), так и в международных документах (ISO/IEC 27000:2018).

Если говорить проще, уязвимость – это слабое место, через которое можно незаметно проникнуть в систему.

Различают несколько уровней уязвимостей:

Уязвимости кода. Ошибки при разработке программного обеспечения.

Например, Buffer Overflow (переполнение буфера) – когда программа записывает данные за пределами выделенной памяти, и этим можно воспользоваться для внедрения вредоносного кода.

SQL-инъекция (SQL Injection) – злоумышленник вводит в строку поиска или форму входа фрагмент SQL-кода, чтобы получить доступ к базе данных. Например, вместо логина «Иванов» вводится OR '1'='1', и система может выдать список всех пользователей.

XSS (Cross-Site Scripting) – внедрение вредоносного скрипта на веб-страницу, который потом выполняется у посетителей сайта, крадя их данные.

Уязвимости конфигурации. Ошибки в настройках: открытые порты, слабые пароли, чрезмерные права пользователей. *Пример, администратор оставил стандартный пароль «admin123», и им воспользовались для входа в систему.*

– **Уязвимости архитектуры.** Недочеты в проектировании системы. *Например, отсутствие разделения прав: когда у всех сотрудников компании одинаковый доступ к базе данных.*

– **Организационные уязвимости.** Пробелы в регламентах, отсутствие политики безопасности, недостаточная подготовка

персонала. *Например, сотрудники пишут пароли на стикерах и крепят их к мониторам.*

– **Комбинированные уязвимости.** На практике часто встречается сочетание нескольких слабых мест. *Например, ошибка в коде + неверная конфигурация = полный контроль над системой.*

Уязвимости могут скрываться практически везде:

– в операционных системах (Windows, Linux, macOS);

– в системах управления базами данных (MySQL, PostgreSQL);

– в прикладном и специализированном ПО (CRM, ERP);

– в прошивках устройств и BIOS/UEFI;

– в мобильных приложениях и чипах IoT-устройств;

– в сетевом оборудовании (маршрутизаторы, коммутаторы);

– даже в средствах защиты – антивирусах или межсетевых экранах.

Для оценки серьезности уязвимостей применяется международный стандарт **CVSS (Common Vulnerability Scoring System).** В актуальной версии (3.1) каждая уязвимость получает балл от 0 до 10: чем выше показатель, тем опаснее проблема.

Ведутся также реестры уязвимостей:

– **MITRE CVE (Common Vulnerabilities and Exposures)** – международный каталог уникальных идентификаторов уязвимостей;

– **NIST NVD (National Vulnerability Database)** – национальная база США, где уязвимости сопровождаются описанием и оценкой по CVSS;

– **CERT/CC** – координационный центр CERT (США), также ведущий собственный реестр;

– **БДУ ФСТЭК России** – отечественная база данных уязвимостей.

Примеры реальных уязвимостей:

– **CVE-2021-34527 (PrintNightmare)** – ошибка в службе печати Windows, позволявшая выполнять произвольный код с правами администратора. Балл CVSS: 8.8 (высокая опасность).

– **CVE-2021-44228 (Log4Shell)** – уязвимость в библиотеке Log4j, которая позволяла выполнять удаленный код через специально созданные логи. CVSS: 10.0 (критическая опасность).

– **Spectre/Meltdown** – ошибки в архитектуре процессоров, позволявшие извлекать данные из памяти других процессов. CVSS до 7.9 (высокая опасность).

Таким образом, уязвимость актива – это не абстрактный термин, а вполне конкретное слабое звено, которое злоумышленник обязательно постарается найти и использовать. Понимание типов уязвимостей и умение их распознавать – ключевой шаг к созданию эффективной системы защиты.

1.3. Способы реализации угроз: чем бьют

Чтобы лучше понять логику злоумышленников, важно не только перечислить угрозы, но и разобрать, **какими методами они реализуются на практике**. По сути, это инструментарий атаки. В методических документах ФСТЭК России выделяются следующие ключевые способы:

– **несанкционированный сбор информации.** Классика разведывательных действий: сканирование сети, перехват трафика (сниффинг), применение социальной инженерии (обман сотрудников для получения паролей). *Пример: с помощью программы Wireshark можно «подсмотреть» незашифрованный HTTP-трафик и вытащить логины и пароли пользователей;*

– **исчерпание ресурсов.** Злоумышленник перегружает систему так, чтобы она перестала обслуживать легальных поль-

зователей. *Например, самый известный метод – **DDoS-атака**: сотни зараженных компьютеров одновременно запрашивают сайт, и он ложится. Другой пример – SYN Flood: сервер переполняется половинчатыми соединениями и не может обработать новые;*

– **инъекции.** Внедрение кода в систему через уязвимые точки ввода. *Например, SQL-инъекция – вставка SQL-команды в форму сайта, чтобы получить доступ к базе данных. OS Command Injection – злоумышленник вставляет в поле ввода команду операционной системы, и сервер ее выполняет;*

– **подмена при взаимодействии.** Задача – выдать себя за доверенный объект. *Например, IP-спуфинг – маскировка под надежный IP-адрес. MITM (Man-in-the-Middle) – злоумышленник встраивается в обмен между клиентом и сервером и перехватывает данные. Фишинг – подделка сайта банка или письма для обмана пользователей;*

– **манипулирование временем и состоянием.** Атаки на временные метки или синхронизацию системы. *Например, злоумышленник подменяет кэш браузера и подсовывает пользователю устаревший, но выгодный ему вариант страницы;*

– **злоупотребление функционалом.** Использование легальных инструментов системы в нелегальных целях. *Например, PowerShell в Windows может применяться для запуска вредоносных скриптов, хотя изначально это инструмент администрирования*;

– **вероятностные методы.** Здесь в ход идет метод подбора. *Например, Brute force – автоматический перебор паролей. Тайминговые атаки – анализ времени отклика системы для извлечения криптографических ключей;*

– **срыв аутентификации и авторизации.** Использование уязвимостей в механизмах проверки личности и прав досту-

па. *Например, кража токенов доступа через вредоносное ПО или повышение привилегий для получения прав администратора;*

– **манипуляции структурами данных.** Изменение форматов и характеристик данных, чтобы обойти защиту. *Например, подмена цифровой подписи документа или искажение формата файла для обхода антивирусной проверки;*

– **анализ целевого объекта.** Сбор сведений о системе с целью подготовки атаки. *Например, используются сканеры (Nmap) для выявления открытых портов и сервисов;*

– **эксплуатация технических ошибок.** Использование багов и уязвимостей, в том числе нулевого дня (zero-day), о которых еще не знают производители. *Например, атака через уязвимость в прошивке роутера, для которой еще нет патча;*

– **физический доступ.** Если злоумышленник получил доступ к серверу или рабочей станции, то установка «ядовитой» USB-флешки или загрузка системы с внешнего носителя могут полностью обойти все цифровые защиты;

– **организационные слабости.** Использование пробелов в управлении и регламентах. *Например, атака на цепочку поставок – заражение обновлений ПО у подрядчика, через которые вирус попадает к конечным пользователям.*

Таким образом, способы реализации угроз охватывают **и технические уязвимости, и человеческий фактор, и пробелы в организации защиты**. Для специалистов важно не только знать названия методов, но и понимать, как они работают на практике. Именно это позволит выстраивать эффективные меры противодействия.

1.4. Объекты воздействия: кто и что страдает в первую очередь

В теории информационной безопасности объект воздействия – это элемент информационной системы, на который направлено вредоносное действие с целью нарушения ее ключевых свойств: конфиденциальности, целостности и доступности. На практике таких объектов несколько, и у каждого – свои уязвимости.

1.4.1. Люди

Человеческий фактор остается самым слабым звеном. Даже самая защищенная система может быть скомпрометирована, если сотрудник откроет фишинговое письмо или установит сомнительное приложение.

Пример: сотруднику приходит письмо «от банка» с просьбой обновить данные. Он вводит пароль на поддельном сайте – и доступ к системе оказывается у злоумышленников.

Меры защиты: обучение персонала, регулярные тесты на устойчивость к фишингу, строгие правила работы с конфиденциальной информацией.

1.4.2. Данные

Основная цель атак – сами информационные ресурсы. Угрозы направлены на кражу, искажение или уничтожение данных.

Пример: вирус-шифровальщик блокирует все файлы на диске и требует выкуп.

Меры защиты: шифрование данных на диске и «в полете» (во время передачи), резервное копирование, ограничение доступа по принципу минимальных прав.

1.4.3. Процессы разработки и поставки

Уязвимости могут закладываться на этапе создания и сопровождения программного обеспечения.

Пример: в 2020 г. в систему обновлений SolarWinds Orion был внедрен вредоносный код, через который хакеры получили доступ к десяткам правительственных структур США.

Меры защиты: безопасный жизненный цикл разработки ПО (Secure Development Lifecycle, SDLC), проверка контрагентов, тестирование продуктов перед вводом в эксплуатацию.

1.4.4. Сети и каналы связи

Любая передача данных сопровождается риском перехвата.

Пример: если корпоративная сеть не использует шифрование, злоумышленник может снять трафик с помощью сниффера и получить пароли.

Меры защиты: сегментация сети, использование VPN, применение современных криптографических протоколов, мониторинг трафика для выявления аномалий.

1.4.5. Программные и аппаратные средства

Уязвимости могут скрываться в коде приложений, прошивках оборудования или даже в микропроцессорах.

Пример: уязвимости Spectre и Meltdown (2018 г.) позволяли считывать данные из памяти процессора, включая пароли.

Меры защиты: регулярное обновление программного обеспечения, использование антивирусов и систем обнаружения вторжений, контроль целостности и физическая защита серверов.

Таким образом, объекты воздействия в информационной безопасности охватывают весь спектр элементов – от людей до инфраструктуры. Понимание уязвимостей каждого объекта позволяет выстраивать многоуровневую систему защиты, где технические меры дополняются организационными и образовательными.

1.5. Вредоносное воздействие: к чему все приводит

Под вредоносным воздействием понимаются действия, направленные на нарушение нормального функционирования информационной системы, ее компонентов и обрабатываемых данных. Такое воздействие бьет по ключевым свойствам информации – конфиденциальности, целостности и доступности (триада CIA: Confidentiality, Integrity, Availability), а также по дополнительным атрибутам: подлинности, неотказуемости и подотчетности.

Рассмотрим основные последствия.

1.5.1. Нарушение конфиденциальности

Информация становится доступна тем, кто не имеет на это права. *Пример: кража базы клиентов интернет-магазина и ее публикация в открытом доступе.*

Последствия: финансовые потери, подрыв репутации, возможная ответственность по Федеральному закону № 152-ФЗ «О персональных данных».

1.5.2. Нарушение целостности

Данные искажаются или подменяются, что делает их ненадежными. *Пример: злоумышленник меняет реквизиты в электронных документах, перенаправляя платежи на свои счета.*

Последствия: ошибки в управлении организацией, прямые убытки, утрата доверия к системе.

1.5.3. Нарушение доступности

Данные или сервисы становятся недоступными для пользователей. Пример: DDoS-атака (Distributed Denial of Service) парализует работу сайта банка, блокируя доступ к онлайн-услугам.

Последствия: остановка бизнес-процессов, потеря клиентов, дополнительные расходы на восстановление работы.

1.5.4. Подрыв подлинности

Возникает возможность подделки информации или источника ее происхождения. *Пример: использование поддельного цифрового сертификата для подписания вредоносного кода.*

1.5.5. Отказ от действий (нарушение неотказуемости)

Пользователь или организация может отрицать совершенные действия. *Пример: сотрудник отправил важное сообщение, но утверждает, что этого не делал.*

Меры противодействия: электронная подпись (Федеральный закон № 63-ФЗ «Об электронной подписи»).

1.5.6. Потеря подотчетности

Невозможно точно определить, кто и какие действия совершал в системе. *Пример: использование общего пароля для нескольких сотрудников, что исключает идентификацию нарушителя.*

Исходя из перечисленного можно сделать вывод, что вредоносное воздействие – это не просто атака на систему, а целый спектр последствий, нарушающих работу организации и безопасность ее данных. Именно поэтому в современной практике применяется подход многоуровневой защиты (defense in depth), сочетающий технические средства, организационные меры и подготовку персонала.

§ 2. Методы и средства несанкционированного получения информации из автоматизированных систем

Методы и средства несанкционированного получения информации из автоматизированных систем (АС) можно классифицировать по различным основаниям. Такая классификация важна для того, чтобы понимать логику действий злоумышленников и разрабатывать адекватные меры защиты.

2.1. По виду доступа

Физический доступ. Злоумышленник получает возможность напрямую взаимодействовать с оборудованием: кража жесткого диска, подключение через USB-носитель, установка аппаратных закладок и пр. В этом случае компрометация системы идет через сам объект техники, минуя логические барьеры.

Логический доступ. Проникновение осуществляется через сеть, чаще всего посредством удаленного соединения. Атака может быть произведена с любого устройства, имеющего доступ к Интернету, что значительно расширяет радиус действия злоумышленников.

2.2. По уровню доступа

Полный доступ. Включает полный контроль над системой – от пользовательских данных до административных привилегий. *Пример: эксплуатация уязвимости Log4Shell (CVE-2021-44228), позволявшей выполнять произвольный код через библиотеку Log4j.*

Ограниченный доступ. Доступ только к отдельным ресурсам или сервисам. Например, гостевой вход в ОС с минимальными правами. Однако даже такой уровень может быть использован как точка опоры для эскалации привилегий.

2.3. По характеру действий злоумышленника

Пассивные атаки. Сбор информации без изменения состояния системы: перехват сетевого трафика (например, через Wireshark), анализ метаданных файлов, мониторинг активности пользователей.

Активные атаки. Внедрение изменений в систему: установка вредоносного кода, подмена данных, нарушение логов. Характерный пример – уязвимость PrintNightmare (CVE-2021-34527), позволявшая выполнять произвольный код с системными правами.

2.4. По многократности доступа

Одноразовый доступ. Разовая атака, направленная на быстрое извлечение информации (например, копирование базы данных клиентов).

Постоянный доступ. Создание устойчивого канала связи с системой: использование бэкдоров, троянских программ, рутки-

тов. Этот вариант особенно опасен, так как позволяет злоумышленникам длительное время незаметно контролировать систему.

2.5. По направленности действий

Целенаправленные атаки. Атакуется конкретная организация или объект. Пример – шпионские кампании APT-групп, ориентированные на получение доступа к данным государственных органов.

Ненаправленные атаки. Массовые сканирования сети, автоматический поиск уязвимых сервисов или дырявых конфигураций (например, открытые RDP-порты). Такие атаки зачастую проводятся ботнетами и имеют облавный характер.

2.6. По тяжести последствий

Легкие атаки. Не наносят серьезного ущерба: ограниченный сбой в работе сайта, кратковременные перебои в доступе к сервису.

Тяжелые атаки. Приводят к серьезным последствиям: масштабная утечка конфиденциальных данных, нарушение работы критической инфраструктуры, повреждение или уничтожение информации. Яркий пример – уязвимости Spectre и Meltdown, позволявшие извлекать данные прямо из памяти процессора.

Представленная классификация демонстрирует широкий спектр методов, используемых злоумышленниками для получения несанкционированного доступа к автоматизированным системам. При этом конечная цель всегда одна – установление контроля над системой или данными. Понимание особенностей каждого метода позволяет создавать многоуровневую защиту, сочетающую технические, организационные и правовые меры.

§ 3. Виды и формы тактики при скрытом получении информации из защищенных компьютерных систем

Когда мы говорим о скрытом получении информации, важно помнить: злоумышленник почти никогда не действует в лоб. Наоборот, вся его тактика построена на том, чтобы оставаться незамеченным и использовать слабые места системы – будь то невнимательность сотрудника, дырка в настройках или забытый порт на сервере.

Локальный уровень.

Здесь все начинается с самого простого: физического доступа.

Хищение. Классика жанра. Унести жесткий диск, флешку или даже весь компьютер – один из самых старых способов. И нередко он маскируется под банальную кражу имущества.

Прямое копирование. Если компьютер оставлен включенным, достаточно вставить загрузочный USB и скопировать нужные данные. Даже шифрование не спасет: файл можно украсть сейчас, а расшифровать позже.

Открытый сеанс. Пользователь отошел от рабочего места и оставил незаблокированный ПК? Для злоумышленника это золотая жила: он работает в рамках реальных полномочий жертвы.

Пароли. Слабые пароли до сих пор остаются причиной большинства взломов. Программы типа John the Ripper подбирают их быстрее, чем мы успеваем осознать ошибку.

Гостевая учетная запись. Даже минимальный доступ позволяет сделать первый шаг к администраторским правам.

Загрузка с внешнего носителя. Вставил флешку с Linux – и уже можно обходить штатные ограничения Windows.

3.2. Удаленный уровень

Удаленные атаки куда более опасны: они позволяют действовать на расстоянии, и жертва может долго не понимать, что ее система уже пробита.

Первое, что делает злоумышленник, – собирает информацию:

– **Whois** – кто зарегистрировал домен, какие контакты оставлены;

– **Traceroute** – карта маршрутов до узла;

– **Nslookup** – DNS-записи;

– **VisualRoute, Sam Spade** – графическая визуализация сетей.

Эти простые шаги дают полную картину: как устроена сеть, где стоят серверы, кто ими управляет.

3.3. Сканирование

Затем идет сканирование сети – поиск уязвимостей.

– **Ping** – проверка доступности.

– **Nmap** – главный инструмент для поиска портов и сервисов.

– **Netcat** – универсальный швейцарский нож TCP/UDP.

Пример: с помощью Nmap злоумышленник обнаруживает сервер с открытым SSH (порт 22), где работает устаревший OpenSSH. Эксплойт уже готов – дальше вопрос техники.

3.4. Идентификация ресурсов

Когда карта сети готова, наступает очередь сбора данных о пользователях и сервисах.

– **Windows**: Net, Nbtstat, DumpSec.

– **Unix**: finger, rusers, rpcinfo.

– **Дополнительно**: user2sid, enum – для сопоставления идентификаторов с реальными людьми.

3.5. Эксплуатация и закрепление

На этом этапе злоумышленник внедряется в систему и старается там закрепиться:

– ставит **трояны** или **бэкдоры**;

– запускает **keylogger** для кражи паролей;

– создает **скрытые учетные записи**;

– меняет автозагрузку, чтобы код запускался при каждом старте системы.

3.6. MITRE ATT&CK и Cyber Kill Chain

Модели атак вроде **MITRE ATT&CK** или **Cyber Kill Chain** показывают, что атака – это всегда цепочка:

1. Разведка цели.
2. Первичный доступ (фишинг, уязвимости).
3. Закрепление в системе.
4. Повышение привилегий.
5. Обход защитных средств.
6. Сбор данных.
7. Их вывод за пределы организации.

Таким образом, скрытое получение информации – это не один прием, а целая стратегия, где шаг за шагом атакующий приближается к своей цели. И знание этих шагов – ключ к тому, чтобы прервать цепочку вовремя.

Таблица 2

Сравнение локальных и удаленных методов скрытого получения информации

Критерий	Локальный доступ	Удаленный доступ
Определение	Доступ осуществляется при физическом контакте с компьютером или носителем информации	Доступ осуществляется через сеть (интернет или локальная сеть), без физического присутствия
Примеры методов	– хищение жесткого диска/флешки; – прямое копирование данных; – использование открытого сеанса пользователя; – взлом слабого пароля; – загрузка с внешнего носителя (Linux-диск)	– сбор информации о сети (Whois, Traceroute, Nslookup); – сканирование сети (Nmap, Netcat); – взлом учетных записей через брутфорс или фишинг; – эксплуатация уязвимостей веб-сервисов; – установка бэкдора для дальнейшего доступа
Инструменты	Физический доступ к компьютеру, загрузочные USB/CD, программы подбора паролей (John the Ripper)	Сетевые утилиты (Nmap, Netcat, Wireshark), скрипты на Python для сканирования, эксплойты, RAT (Remote Access Trojan)
Примеры ситуаций	– пользователь оставил ПК без блокировки, злоумышленник скопировал файлы; – украден ноутбук с конфиденциальными данными; – установлен «чужой» жесткий диск	– хакер сканирует корпоративную сеть и находит уязвимый сервер SSH; – проведен фишинг для кражи паролей; – установлен троян для удаленного управления системой
Уровень риска	Ограничен физическим доступом к объекту	Практически не имеет географических ограничений – риск глобален. – межсетевые экраны и IDS/IPS; – регулярные обновления ПО; – сегментация сети; – мониторинг активности и журналирование; – обучение сотрудников противодействию фишингу

§ 4. Методики кибератак MITRE ATT&CK и технология Cyber Kill Chain

В современном киберпространстве злоумышленники действуют не хаотично, а по четко выстроенным сценариям. Чтобы понять логику атак, специалисты используют две широко признанные методологии: **MITRE ATT&CK** и **Cyber Kill Chain**. Они помогают систематизировать действия атакующих и выстраивать защиту на каждом этапе [83].

Cyber Kill Chain

Модель **Cyber Kill Chain**, разработанная компанией *Lockheed Martin*, описывает кибератаку как последовательность из семи этапов [84]:

1. **Разведка (Reconnaissance)** – сбор информации о цели. Злоумышленники исследуют публичные данные, используют утилиты типа *whois*, *traceroute*, *nslookup* для анализа сети. Например, можно выяснить IP-адреса серверов и контакты администраторов.

2. **Вооружение (Weaponization)** – подготовка вредоносного ПО или эксплойта. Это может быть троян в офисном документе или специально подготовленный фишинговый сайт.

3. **Доставка (Delivery)** – отправка заряженного объекта жертве. Чаще всего – электронное письмо с вложением, зараженная флешка или ссылка на фальшивый сайт.

4. **Эксплуатация (Exploitation)** – использование уязвимости. Например, открытие зараженного файла запускает вредоносный код.

5. **Установка (Installation)** – закрепление в системе: установка *бэкдора* или *RAT* (Remote Access Trojan), который открывает канал для удаленного управления.

6. **Управление и контроль (Command & Control, C2)** – связь с сервером злоумышленника для удаленного управления зараженной системой.

7. **Достижение целей (Actions on Objectives)** – кража данных, разрушение инфраструктуры или проведение DoS-атаки.

Эта модель наглядна тем, что позволяет разложить атаку по шагам и понять, на каком этапе ее можно остановить.

MITRE ATT&CK

В отличие от Kill Chain **MITRE ATT&CK** – это постоянно пополняемая матрица тактик, техник и процедур (TTP), используемых атакующими [85]. Она фиксирует **что конкретно делают злоумышленники**:

– тактики (высокоуровневые цели атак, например «Первоначальный доступ» или «Закрепление»);

– техники (конкретные способы, например фишинг по e-mail, «эксплуатация публичных сервисов»);

– подтехники (детализация методов, например вложения Office с макросами).

Для практиков MITRE ATT&CK ценна тем, что она позволяет сопоставить **наблюдаемые признаки атаки** с реальными сценариями, описанными в базе MITRE. Это значит, что при расследовании можно быстро понять: «то, что мы видим, – это, скорее всего, техника *Credential Dumping* (сбор хэшей паролей), и дальше злоумышленник попытается повысить привилегии».

Иллюстрация на примере атаки

Рассмотрим типовую схему:

1. На этапе разведки злоумышленник запускает *nmap* и видит, что у сервера открыт порт 22 (SSH).

2. Далее он находит уязвимую версию OpenSSH и готовит эксплойт (этап вооружения).

3. С помощью фишингового письма он доставляет жертве «невинный» PDF, внутри которого спрятан троян (доставка + эксплуатация).

4. После успешного проникновения устанавливается *бэкдор* (*Netcat* или *Meterpreter*) для постоянного доступа.

5. Через командный сервер злоумышленник управляет системой и постепенно повышает свои привилегии.

6. Завершающий этап – кража базы данных клиентов и ее вывод на удаленный сервер в зашифрованном виде.

Таким образом, в действии можно увидеть и **Kill Chain** (последовательность шагов), и **MITRE ATT&CK** (конкретные техники вроде Phishing: Spearphishing Attachment, Exploitation for Client Execution).

Практическая ценность

Для специалистов по ИБ понимание этих моделей критически важно. **Cyber Kill Chain** учит видеть общую логику атаки: от разведки до уничтожения данных. **MITRE ATT&CK** помогает разложить атаку на атомы и сравнить ее с накопленной базой знаний. Вместе они позволяют строить защиту не хаотично, а системно:

– на этапе разведки – скрывать информацию об инфраструктуре;

– на этапе доставки – фильтровать почтовый трафик и использовать антифишинговые средства;

– на этапе закрепления – применять системы мониторинга и выявления аномалий;

– на этапе вывода данных – отслеживать необычные каналы связи и использование VPN.

Как мы видим, кибератака – это многоэтапный и тщательно выстроенный процесс, в котором злоумышленники используют широкий спектр методов: от социальной инженерии до эксплуатации уязвимостей и внедрения вредоносного кода. На каждом этапе MITRE ATT&CK или Cyber Kill Chain они стремятся закрепиться в системе и расширить свой контроль. Однако, если у атакующих есть собственная тактика и инструменты, то и у защитников должна быть своя стратегия.

Именно здесь на первый план выходит **автоматизация информационной безопасности**. В условиях, когда скорость атаки измеряется секундами, а объем угроз растет лавинообразно, человек физически не успевает реагировать на все инциденты вручную. Поэтому все большую роль играют **антивирусные комплексы, межсетевые экраны, VPN, IDS/IPS, системы-ловушки HoneyPot и другие автоматизированные средства защиты**.

Таким образом, раздел 5 логично продолжает рассмотрение проблемы: если раздел 4 показал, *как атакуют* злоумышленники, то теперь мы рассмотрим, *как защищаться* – и именно автоматизация становится ключом к эффективной обороне.

§ 5. Автоматизация информационной деятельности при получении информации из защищенных компьютерных систем

Переходя от методов атак к методам защиты, важно подчеркнуть: современный специалист по информационной безопасности должен мыслить, как атакующий. Только понимая, *какими путями злоумышленник проникает в систему*, можно правильно построить защиту. Здесь на первый план выходит **автоматизация процессов защиты** – системы, которые круглосуточно

анализируют потоки данных, фиксируют аномалии и реагируют на угрозы быстрее, чем это способен сделать человек.

Автоматизация не исключает роль человека, но снимает с него рутинную нагрузку: сканирование журналов, проверку сетевого трафика, выявление подозрительных действий. В результате специалист получает уже обработанные сигналы и может сосредоточиться на анализе и принятии решений.

5.1. Антивирусное программное обеспечение

Антивирус – это, пожалуй, первый слой защиты, знакомый даже неспециалистам. Его основная функция – обнаружить, блокировать и удалить вредоносное ПО: вирусы, трояны, шифровальщики, шпионские модули.

Современные антивирусные системы используют два подхода:

– **сигнатурный анализ** – сравнение файлов с базой отпечатков известных вирусов (работает быстро, но не ловит новые угрозы);

– **эвристический анализ** – выявление подозрительного поведения, например массовое шифрование файлов или попытки скрытой передачи данных [66].

Пример: в 2021 г. одна российская компания столкнулась с атакой программы-шифровальщика. Сигнатуры для нее еще не существовало, но антивирус заблокировал процесс на половине машин, заметив характерные действия – массовое переименование файлов.

Согласно ГОСТ Р 56939–2016, «Антивирусное программное обеспечение – это программные средства защиты информации, предназначенные для обнаружения, предупреждения, удаления и восстановления последствий воздействия вредоносного программного обеспечения».

5.2. Межсетевые экраны (брандмауэры, firewall)

Если антивирус работает внутри системы, то межсетевой экран стоит на входе. Его задача – фильтровать сетевой трафик по заранее заданным правилам, не допуская подозрительных соединений.

Выделяют три класса брандмауэров:

– **пакетные фильтры** (анализ отдельных пакетов, сегодня почти не используются);

– **экраны с контролем соединений** (отслеживают состояние сессии, особенно важно для TCP/UDP);

– **экраны прикладного уровня** (application firewall): анализируют трафик на уровне приложений, могут работать в «песочнице» [68].

Пример: в 2020 г. в одном из университетов внедрение корректно настроенного брандмауэра позволило остановить попытку сканирования портов извне – атакующие видели сеть как пустую, без доступных сервисов.

Определение: «Межсетевой экран – это средство защиты информации, предназначенное для контроля и фильтрации сетевых потоков на основе правил безопасности» (ФСТЭК России, приказ № 17 от 11.02.2013).

5.3. Виртуальные частные сети (VPN)

VPN создает защищенный «туннель» поверх незащищенной сети (обычно Интернета). Передаваемые данные шифруются и становятся недоступными для перехвата.

Схемы применения:

– «сеть – сеть» – объединение филиалов в единую сеть;

– «точка – сеть» – удаленный доступ сотрудника к корпоративной системе;

– «клиент – сервер» – защищенная передача данных внутри организации.

Пример: в период пандемии COVID-19 многие российские компании массово перевели сотрудников на удаленку. Только внедрение VPN позволило безопасно подключать работников из разных городов к корпоративным базам данных.

Определение: «Virtual Private Network (VPN) – технология построения защищенных соединений поверх общедоступных сетей, обеспечивающая конфиденциальность и целостность передаваемых данных» (ISO/IEC 27033-1:2015).

5.4. Виртуальные локальные сети (VLAN)

VLAN позволяют расчленить, как бы разрезать физическую сеть на логические сегменты. Благодаря этому бухгалтерия, IT-отдел и, например, служба безопасности могут работать в одной физической сети, но логически быть изолированы друг от друга.

Пример: в 2019 г. в одном российском банке изоляция сетей через VLAN не позволила злоумышленникам, проникшим в сегмент Wi-Fi для гостей, добраться до критической банковской инфраструктуры.

Определение: «VLAN (Virtual Local Area Network) – технология логического разделения сети на изолированные сегменты с целью повышения управляемости и безопасности трафика» (IEEE 802.1Q).

5.5. Сканеры уязвимостей

Это инструменты, которые автоматизируют поиск слабых мест в системе. Они проверяют настройки, ПО, версии сервисов и сравнивают их с базой известных уязвимостей.

Популярные примеры: **Nessus, OpenVAS, Qualys**.

Пример: при внутреннем аудите в 2022 г. в одной из энергетических компаний сканер OpenVAS выявил использование устаревшей версии Apache Struts. Исправление уязвимости предотвратило возможную атаку, аналогичную печально известному взлому Equifax в 2017 г.

Определение: «Сканер уязвимостей – это программное средство автоматизированного анализа состояния информационной системы с целью выявления ошибок конфигурации и известных уязвимостей» (NIST SP 800-115).

5.6. Системы обнаружения и предотвращения атак (IDS/IPS)

Эти системы можно назвать сигнализацией сети. IDS фиксирует подозрительную активность, IPS – блокирует ее в реальном времени.

Методы:

– сигнатурный анализ (сравнение с базами атак);

– поведенческий анализ (обнаружение аномалий);

– расшифровка протоколов;

– статистический контроль.

Пример: в 2021 г. IPS-система в одном из телеком-операторов остановила атаку на DNS-серверы компании, заметив резкий рост трафика на порт 53.

5.7. Honeypot и Honeynet

Это ловушки для атакующих – системы, имитирующие настоящие серверы и сервисы. Злоумышленник считает, что взломал сеть, а на самом деле его действия записываются и анализируются.

Пример: в 2020 г. исследователи Positive Technologies развернули honeypot-сеть для наблюдения за злоумышленниками. За первые двое суток система зафиксировала более 30 тыс. попыток перебора паролей по SSH.

Определение: «Honeypot – это изолированная информационная система или сервис, намеренно созданные для имитации уязвимого ресурса с целью изучения действий злоумышленников» (CERT/CC).

Автоматизация в информационной безопасности – это не роскошь, а необходимость. Она позволяет организациям обрабатывать гигантские объемы событий, быстро выявлять аномалии и минимизировать риски. Однако никакой антивирус или IDS не обеспечат полной защиты, если сотрудники используют слабые пароли, а системы не обновляются месяцами.

Поэтому современная модель безопасности – это **«человек + машина»**. Автоматизированные средства дают скорость и масштаб, а человек – понимание и стратегию. Только вместе они образуют устойчивую систему противодействия киберугрозам.

Учебно-методический раздел к главе 3

Цели изучения темы

1. Освоить базовые понятия угроз, уязвимостей и объектов воздействия в информационной безопасности.

2. Научиться различать основные свойства защищенной информации (конфиденциальность, целостность, доступность, подлинность и др.).

3. Понять источники угроз (внешние, внутренние, третьи лица, силы природы) и способы их реализации.

4. Освоить классификацию уязвимостей (код, конфигурация,

архитектура, организационные слабости и их сочетания) и методы их оценки (CVSS, базы CVE, БДУ ФСТЭК и др.).

5. Научиться анализировать объекты воздействия и последствия вредоносных воздействий (триада CIA).

6. Развить навыки применения принципа многоуровневой защиты и моделирования реальных атак.

Вопросы для семинарского занятия

1. Какие свойства информации обеспечивают ее защищенность? Приведите примеры нарушения каждого из них.

2. Чем отличаются внешние и внутренние источники угроз? Какая категория наиболее опасна на практике?

3. Какие основные виды уязвимостей вы знаете? Как связаны уязвимости кода и конфигурации?

4. Что такое многофакторная уязвимость? Приведите пример.

5. Назовите наиболее распространенные способы реализации угроз. Какие из них чаще всего используются в кибератаках?

6. Какие объекты воздействия выделяются в информационной безопасности? Почему именно человеческий фактор считается самым слабым звеном?

7. Объясните на примерах, как вредоносное воздействие может нарушить триаду CIA.

Практические задания

1. **Классификация угроз для банка.** Составьте таблицу, где угрозы распределены по категориям: внешние (хакеры, киберпреступники), внутренние (инсайдеры), третьи лица (аудиторы, регуляторы), силы природы (пожар, наводнение).

2. **Анализ уязвимости.** Найдите описание одной известной уязвимости (например, CVE-2021-44228 – Log4Shell) и проанализируйте:

– какой тип уязвимости (код, конфигурация, архитектура и т. д.);

– какой уровень критичности по CVSS;

– какие меры защиты могли бы предотвратить эксплуатацию.

3. **Практикум по SQL-инъекции.** Объясните на примере, как злоумышленник может с помощью SQL-запроса получить доступ к базе данных. Какие меры защиты (валидация ввода, использование параметризованных запросов) помогают избежать этой атаки?

4. **Разбор DDoS-атаки.** Проанализируйте гипотетическую ситуацию: сайт подвергся SYN-flood атаке. Определите:

– какое свойство информации пострадало;

– каковы последствия для пользователей;

– какие технические и организационные меры могли бы смягчить ущерб.

5. **Моделирование сценария.** Постройте схему, показывающую, как совокупность организационной слабости (например, отсутствие обучения сотрудников) и технической уязвимости (например, слабые пароли) может привести к успешной атаке.

Учебные ситуации

1. Классификация атак.

Фабула: в Университете зафиксированы:

– перехват паролей студентов в Wi-Fi-сети;

– попытка взлома серверов через подбор паролей;

– кража ноутбука сотрудника с конфиденциальными данными.

Задание: определите, где был физический доступ, где логический; какие атаки активные, а какие пассивные.

2. Определение методов на примерах.

Фабула: сотрудникам банка пришло письмо «Срочно обновите пароль», содержащее ссылку на поддельный сайт. В то же время на сервере зафиксирована перегрузка из-за множества одновременных соединений.

Задание:

– Какие методы использовали злоумышленники?

– Какие меры защиты могли бы предотвратить атаку?

3. Демонстрация утилит.

Фабула: администратор заметил подозрительные подключения к корпоративной сети. Вам нужно поставить себя на место злоумышленника, чтобы понять, как он работает.

Задание:

– используя утилиты whois, traceroute, nmap, составьте краткий отчет: какие данные об инфраструктуре можно собрать за 10 минут работы;

– объясните, какие риски несет наличие открытых портов.

4. MITRE ATT&CK и Cyber Kill Chain

Фабула: компания «ИнфоСеть» стала жертвой атаки:

– злоумышленник отправил зараженное резюме в формате .docx;

– после открытия документа появился троян;

– через неделю были похищены бухгалтерские данные.

Задание: опишите действия атакующего по шагам, применяя модель Cyber Kill Chain (от разведки до вывода данных).

5. Разработка плана защиты

Фабула: у вас есть гипотетическая компания «ТехноСофт», где:

– сотрудники работают удаленно;

– база клиентов хранится на сервере;

– сеть компании соединена с Интернетом без сегментации.

Задание: составьте мини-план защиты (5–6 пунктов), включив антивирус, МЭ, VPN, IDS/IPS, HoneyPot.

6. Анализ инцидентов

Фабула: в 2021 г. в одном российском университете произошла утечка данных студентов через уязвимость в системе дистанционного обучения (SQL-инъекция).

Задание:

– Укажите, в чем заключалась ошибка в защите.

– Какие организационные и технические меры могли бы предотвратить инцидент?

– Какие уроки стоит извлечь другим образовательным учреждениям?

Пример решения

Учебная ситуация: в компании «ЭнергоСеть» зафиксированы следующие события:

1. Несколько сотрудников получили письма с вложением *invoice.pdf.exe*. Двое открыли файл, после чего их компьютеры начали работать медленнее.

2. В журнале безопасности сервера обнаружено множество попыток входа под администратором с разных IP-адресов.

3. Через час после этих событий часть корпоративных файлов оказалась зашифрована, а на экране появилось сообщение с требованием выкупа.

Задание:

Определите:

1. Какие методы атаки использовали злоумышленники?

2. Какие этапы Cyber Kill Chain прослеживаются в этой ситуации?

3. Какие меры защиты могли бы предотвратить инцидент?

Пример решения (образец)

1. Методы атаки:

– Фишинг (social engineering) – сотрудники получили письма с вредоносным вложением.

– Вредоносное ПО (ransomware) – запуск трояна, который зашифровал файлы.

– Brute-force атака – многочисленные попытки входа под администратором.

2. Этапы Cyber Kill Chain:

– Reconnaissance (разведка): злоумышленники нашли адреса сотрудников.

– Delivery (доставка): вредоносное вложение в письме.

– Exploitation (эксплуатация): запуск трояна при открытии вложения.

– Installation (установка): закрепление вредоносного кода.

– Command & Control (управление): связь с сервером атакующего.

– Actions on Objectives (реализация целей): шифрование файлов и вымогательство.

3. Меры защиты:

– Обучение сотрудников распознаванию фишинга.

– Внедрение антивируса с функцией сэндбоксинга.

– Ограничение прав пользователей (чтобы вложения не запускались с админ-доступом).

– IDS/IPS для блокировки подозрительных соединений.

– Регулярное резервное копирование файлов.

Библиографический список к главе 3

Нормативные документы и стандарты

1. Национальный стандарт Российской Федерациигост. ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем». – М. : Стандартинформ, 2015.

2. Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.) // НПП «Гарант-сервис». – URL: https://www.garant.ru (дата обращения: 04.09.2025).

3. Common Vulnerability Scoring System (CVSS) v3.1 // FIRST. – URL: https://www.first.org/newsroom/news/cvss/2019 (дата обращения: 04.09.2025).

Электронные ресурсы и базы данных

4. Common Vulnerabilities and Exposures (CVE) // MITRE. –URL: https://cve.mitre.org (дата обращения: 04.09.2025).

5. National Vulnerability Database (NVD) // NIST. – URL: https://nvd.nist.gov (дата обращения: 04.09.2025).

6. CERT/CC. Computer Emergency Response Team Coordination Center. – URL: https://www.cert.org (дата обращения: 04.09.2025).

7. База данных уязвимостей ФСТЭК России (БДУ ФСТЭК) // Федеральная служба по техническому и экспортному контролю [сайт]. – URL: https://bdu.fstec.ru (дата обращения: 04.09.2025).

8. Microsoft. CVE-2021-34527 (PrintNightmare). Windows Print Spooler Remote Code Execution Vulnerability. – URL: https://msrc.microsoft.com (дата обращения: 04.09.2025).

9. Apache Software Foundation. CVE-2021-44228 (Log4Shell). Apache Log4j Remote Code Execution Vulnerability. – URL: https://logging.apache.org/log4j (дата обращения: 04.09.2025).

10. Spectre & Meltdown. Processor vulnerabilities. – URL: https://spectreattack.com (дата обращения: 04.09.2025).

11. MITRE ATT&CK Framework. – URL: https://attack.mitre.org (дата обращения: 04.09.2025).

12. Lockheed Martin. Cyber Kill Chain®. – URL: https://www.lockheedmartin.com/cyber-kill-chain (дата обращения: 04.09.2025).

Книги, статьи

13. Овчинский, С. С. Cyber Intelligence in Law Enforcement / С. С. Овчинский. – М. : Юрлитинформ, 2020.

14. Халяпин, Д. Б. Технические средства оперативного поиска / Д. Б. Халяпин. – СПб. : Питер, 2019.

15. Ржавский, В. К. Радиоэлектронная разведка: теория и практика / В. К. Ржавский. – М. : Академический проект, 2018.

16. Касперский, Е. Кибервойны XXI века / Е. Касперский. – М. : Эксмо, 2019.

17. Anderson, R. Security Engineering / R. Anderson. 3rd ed. Wiley, 2020.

18. Han, J. Data Mining: Concepts and Techniques / J. Han, M. Kamber, J. Pei. 4th ed. Elsevier, 2022.

19. Manning, P. Cybersecurity and Cyberwarfare: Threats and Responses / P. Manning, J. Nichols. Routledge, 2021.

20. Brandel, C. Cybersecurity Incident Response: Best Practices / C. Brandel. CRC Press, 2021.

21. CERT-FR. Guide d’analyse des attaques par déni de service distribué (DDoS). Paris, 2020.

22. Microsoft. Secure Development Lifecycle (SDL). Redmond: Microsoft, 2018.

23. Schneier, B. Secrets and Lies: Digital Security in a Networked World / B. Schneier. 2nd ed. Wiley, 2021.

Глава 4. ИНФОРМАЦИОННЫЕ РЕСУРСЫ: ПОНЯТИЕ, КЛАССИФИКАЦИЯ И ИСПОЛЬЗОВАНИЕ ПРИ СБОРЕ ИНФОРМАЦИИ

ВВЕДЕНИЕ

Индустриальная цивилизация строилась на энергии угля, нефти, газа и электричества. **Постиндустриальная** – на энергии и скорости **информации**. Для экономики это означает, что стоимость создается не столько станками и цехами, сколько данными, знаниями и алгоритмами; для полиции – что **цифровой след** становится таким же материальным, как отпечаток на стекле, а грамотная работа с базами, логами и открытыми источниками (OSINT) – столь же важной, как осмотр места происшествия. Эту смену парадигмы еще в конце XX в. предсказал Д. Белл, описав постиндустриальное общество, где ядром выступают знания и их производство.

Отсюда практический вывод для сотрудника полиции: **информационные ресурсы** – не отвлеченная теория, а основа, базис для раскрытия преступлений в цифровой среде. Журналы подключения к сервису, массивы транзакций, архивы видеонаблюдения, базы миграционного учета, публикации в соцсетях – все это ресурсы, которые нужно **обнаружить, получить законно, сохранить процессуально и правильно интерпретировать**.

Каждый электронный документ, сообщение в социальной сети, запись в базе данных или метаданные фотографии – все это разновидности информационных ресурсов. И именно они могут дать следователю ключ к раскрытию преступления. Например, в ходе расследования телефонного мошенничества IP-адрес, за-

фиксированный в логах оператора связи, становится тем самым фрагментом ресурса, который позволяет выйти на злоумышленника.

В этой теме мы рассмотрим:

– что такое информационные ресурсы и как они появились;

– их правовое закрепление в законодательстве;

– задачи, которые они решают в сфере государственного и оперативного управления;

– существующие классификации ресурсов и их значение для следственной практики;

– роль информационных услуг и рынка информации в современном мире.

Таким образом, понимание природы информационных ресурсов – это не отвлеченная теория, а конкретная профессиональная необходимость для будущего полицейского. Это знания, которые помогут правильно оценить цифровые следы, выстроить следственные версии и использовать информационные массивы в качестве доказательной базы.

§ 1. Понятие «информационные ресурсы»

1.1. Смысл категории: от «угля и нефти» к «данным и знаниям»

Если индустриальную эпоху двигали материальные энергоресурсы, то сегодня роль двигателя выполняет **информация как ресурс**: она накапливается, перерабатывается, обменивается и превращается в блага – деньги, безопасность, управленческие решения, доказательства в суде. Это и есть новая энергия общества: чем быстрее она циркулирует и чем лучше структурирована, тем выше производительность и качество управления.

В «Словаре русского языка» С. И. Ожегова «ресурс» определяется как «запас, источник чего-либо». Следовательно, информационные ресурсы – это **источники информации, которыми располагает общество и которые оно может использовать в своей деятельности**.

Особенность здесь в том, что в отличие от природных или материальных ресурсов информационные ресурсы:

– **создаются человеком** (будь то научная статья, база данных или судебное решение);

– **отчуждаются от своих создателей** и могут использоваться другими людьми или организациями;

– **имеют ценность** не только в практическом применении, но и как фактор развития общества.

Для полицейского это означает: работа с информационными ресурсами требует понимания их природы, структуры и способов доступа. Документ, база данных или архив могут содержать решающие сведения для раскрытия дела.

1.2. Общее определение

В постиндустриальном обществе именно информация становится основным капиталом. Она фиксируется в книгах, архивах, библиотеках, электронных базах данных, научных отчетах, патентах, программном обеспечении.

Важно различать просто сведения и **информационные ресурсы**. Чтобы поток данных превратился в ресурс, он должен быть:

– **организованным** (структурированным и упорядоченным);

– **доступным** для практического использования;

– **социально значимым** (т. е. имеющим ценность для общества или конкретных сфер деятельности).

Так, случайное сообщение в чате – это информация, но не ресурс. А вот собранные и систематизированные переписки, включенные в архив оперативного дела, становятся полноценным информационным ресурсом.

Следовательно, информационные ресурсы можно определить как **организованные массивы информации, подготовленные для социального использования и закрепленные в материальной форме** – документ, база данных, архив, библиотека, информационная система.

С полицейской точки зрения информационный ресурс – это **организованная совокупность сведений**, уже приведенная в форму, удобную для практического применения: поиск, отбор, корреляция и визуализация. Иначе говоря, это не море сырых данных, а **подготовленная база** для действий. Несколько типичных ситуаций:

1. **Трафик**. По делу о фишинговой рассылке изымаются логи веб-сервера: IP-адреса, метки времени, агенты браузера. Эти логи – информационный ресурс. Их корреляция с биллингом провайдера и событиями из мессенджера позволяет выйти на конкретный абонентский договор.

2. **Соцсети**. Угроза насилием публикуется и удаляется. Пост исчез, но кэш поисковой системы и бэкап страницы в мониторинговом сервисе – тоже информационные ресурсы – сохраняют текст и время публикации, что критично для фиксации умысла.

3. **Видео**. Фрагменты с уличных камер разных ведомств попадают в распределенное хранилище. Только после унификации метаданных (время, координаты, номер камеры) ресурс становится работающим: строится траектория, подтверждается версия.

Важно: **ресурсом** информация становится лишь тогда, когда **организована** (структурирована, каталогизирована, снабжена метаданными), иначе это набор разрозненных сигналов. Поэ-

тому в профессиональной практике мы оперируем не данными вообще, а базами, фондами, архивами, хранилищами, реестрами и информационными системами, обеспечивающими воспроизводимость и проверяемость результата.

1.3. Правовое определение и рамки обращения

Российское право специально фиксировало эту категорию. Впервые на уровне закона термин «информационные ресурсы» был раскрыт в Федеральном законе от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации», где под ними понимались **отдельные документы и массивы документов**, в том числе в информационных системах (библиотеках, архивах, банках данных и др.). Аналогичный подход содержал Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене».

Действующий базовый закон – Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» – не относит данный термин к перечню основных, однако прямо закрепляет **правовой режим информации** и **возможность признания информационных ресурсов объектом права собственности** с регулированием по нормам гражданского законодательства. Для полиции это означает два ключевых практических следствия:

1) **доступ и изъятие** должны происходить строго в рамках процессуальных норм и с учетом прав владельца ресурса (в том числе его коммерческой тайны, персональных данных);

2) **процессуальная пригодность** результата зависит от корректной фиксации источника, целостности массива и верифицируемости его происхождения (кто владелец, где хранится, как получено).

Суммируя, под **информационными ресурсами** в учебно-практическом ключе будем понимать **организованную и структурированную документированную информацию (включая электронную), закрепленную в фондах, архивах, базах данных и информационных системах, пригодную для повторного использования в управленческих, оперативно-разыскных и процессуальных целях**.

§ 2. Задачи информационных ресурсов по реализации функций основной и информационной деятельности

Если признать, что в XXI в. информация – такой же стратегический ресурс, как раньше уголь, нефть или электроэнергия, то следующим шагом будет вопрос управления: кто производит этот ресурс, кто его хранит, кто обеспечивает доступ и как он помогает государству выполнять свои функции? Уровень зрелости информационных ресурсов во многом определяет место страны в глобальном мире. И Россия здесь не исключение. Объем и разнообразие наших информационных массивов соответствуют масштабу территории, экономики и человеческого потенциала: они создаются в органах власти, на предприятиях и в научных организациях, аккумулируются в библиотеках и архивах, обслуживают образование, здравоохранение, безопасность и правосудие.

С точки зрения государственной политики можно выделить четыре взаимосвязанные цели управления информационными ресурсами (ИР):

1) **создание первичных и производных массивов** – тех самых «кирпичиков» принятия решений: от сырых сведений до аналитических продуктов, необходимых и для государственного управления, и для реализации конституционного права граждан на доступ к информации;

2) **надежное хранение и защита ИР** – чтобы данные не терялись, не искажались и не утекали (включая правовые режимы доступа, резервирование, аудит и контроль изменений);

3) **эффективное использование ИР** в работе органов власти и государственных учреждений – не «склад данных ради склада», а живой оборот информации в управленческих процессах (планирование, мониторинг, контроль исполнения);

4) **законный и удобный доступ** граждан и организаций к ИР – в объеме и порядке, установленном федеральным законодательством (включая ограничения по персональным данным и тайнам).

Для сотрудника полиции данные цели – это не абстракция. Каждая из них прямо влияет на выполнение повседневных задач: где и как запрашивать сведения, как быстро можно их получить, какой доказательственной силой они обладают и что делать, если источник закрыт по причине ограничения режима доступа.

Таблица 3

Примеры государственных информационных ресурсов в России

Тип ресурса	Пример	Описание и полицейская значимость
Библиотечные ресурсы	Российская государственная библиотека (РГБ)	Крупнейшая библиотека страны; более 47 млн единиц хранения. Источник справочно-энциклопедической и исторической информации; полезны при экспертизах, проверке источников и датировок
Архивный фонд	Государственный архив Российской Федерации (ГАРФ)	Документы по истории России, в том числе фонды органов власти. Важен при проверке подлинности документов и исследовании истории имущества/прав
Научно-техническая информация	Всероссийский институт научнй и технической информации (ВИНИТИ)	Базы по публикациям и патентам. Полезна при расследовании хищений НИОКР, нарушений ИС, псевдоэкспертной деятельности

Окончание табл. 3

Статистика	Росстат	Официальные статистические данные. Удобны для контрольных сопоставлений в экономиеских и коррупционных делах (вырисовываются аномалии)
Правовая информация	Официальный интернет-портал правовой информации (pravo.gov.ru)	Действующие НПА и их редакции. Базовый истчник валидации правовой позиции и правильной квалификации [8 10; 11]
Геоданные	Роскартография, ГИС	Картографические данные и геоинформационные системы. Полезны при реконструкции событий, маршрутов, зон связи (с привязкой к местности)
Образование	Федеальный портал «Россиисое образование» (edu.ru)	Сведения о вузах и программах. Используются при проверке анкетных данных, фактов обучения, липовых дипломов
Госуслуги	Портал государственных и муниципальных услуг (gosuslugi.ru)	Точки входа в услуги и учетые записи граждан. Имеют значение для установления цифровых следов заявителя, временных меток, маршрутов обращения

Пример. В делах о подделке документов нередко сходится пазл из трех источников: запись действий пользователя в личном кабинете на «Госуслугах», правовой статус формы и срока действия документа (pravo.gov.ru) и картографическая привязка события (ГИС). Такое трехлучевое подтверждение сильно повышает доказательственную устойчивость материала.

2.1. Ключевые государственные массивы (их значение для полиции)

Библиотечные ресурсы. В России действуют около 150 тыс. библиотек, более 2,5 тыс. из них уже используют автоматизированные базы данных. Для полицейского это не просто фонды книг, а источник справочной информации, отраслевых стан-

дартов, редких изданий, которые могут подтвердить или опровергнуть факты в экспертизе.

Архивный фонд Российской Федерации. Более 460 млн единиц хранения, из которых свыше 193 млн ведет Росархив. Архивы – это своеобразная память государства, где фиксируются юридические факты, решения и права, к которым следствие обращается при восстановлении цепочки событий.

Государственная система научно-технической информации (ГСНТИ). Более 30 федеральных и отраслевых организаций и 69 региональных центров формируют массивы по результатам НИОКР. Для полиции это возможность выявить несанкционированные заимствования, утечку технологий или теневые каналы их распространения.

Государственная статистика. Интегрированные базы (включая ЕГРПО и первичные формы) позволяют выявлять аномалии – несоответствия отчетности, резкие выбросы в данных, которые становятся сигналом для проверки.

Правовые ресурсы. Массивы Минюста России, центров правовой информатизации и судебных органов образуют каркас правовой квалификации. Для дознания это база, на которую можно опираться при построении юридически безупречных обвинений.

Массивы органов власти. Управленческие реестры, учеты и обращения граждан дают полицейскому представление о социальных процессах и точках напряжения, которые нередко предшествуют правонарушениям.

Природные и пространственные данные. Картографические, геодезические и топографические массивы (ГИС) содержат сведения о недрах, воде, лесах. Они полезны при следственных осмотрах, моделировании и планировании операций на местности.

Системный обзор состава и состояния государственных информационных ресурсов (ИР) регулярно публикуется в Национальном докладе «Информационные ресурсы России», Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России). Для полицейского это своего рода опорная карта: где именно формируются данные и кто несет ответственность за их ведение.

2.2. Ближайшие задачи эффективного управления ИР (в призме полицейской практики)

1. **Определение перечня приоритетных федеральных ИР.** Четкое понимание того, что главное, избавляет от бесконечной переписки: запросы направляются точечно – к известным держателям массива.

2. **Нормативное закрепление обязанностей органов власти.** Разделение межведомственных и ведомственных функций гарантирует полиции прозрачные каналы доступа и предсказуемые сроки ответа.

3. **Разведение полномочий Федерации и субъектов Российской Федерации.** Зафиксированные договоры позволяют субъекту знать, какие сведения и в какие сроки он обязан передать, а федеральному центру – агрегировать их и контролировать полноту.

4. **Государственная регистрация ИР и система метаданных.** Для следствия это означает, что массив не безымянный: у него есть владелец, регламент и контактное лицо.

5. **Единые классификации и стандарты описания ИР.** Унификация форматов и атрибутов записей дает возможность быстро объединять данные из разных регионов и автоматизировать поиск. Экономия времени в расследовании измеряется неделями.

6. **Учет ИР как государственного имущества.** Информационные массивы – не ничьи файлы, а активы государства. За их утрату или искажение несут ответственность конкретные должностные лица.

2.3. Примеры из практики

Мошенничества с государственными выплатами. *Расследование серии преступлений продвинулось, когда удалось оперативно сопоставить данные портала «Госуслуги», региональных реестров выплат и ведомственной системы учета адресной помощи. Межведомственный обмен позволил выявить мультиаккаунты – одни и те же паспортные данные использовались для регистрации нескольких личных кабинетов. Перекрестная проверка показала повторное получение выплат на разные банковские карты. Этот набор цифровых следов лег в основу доказательств и позволил предъявить обвинение.*

Незаконный оборот лекарственных средств. *Государственная регистрация ИР позволила быстро определить, кто отвечает за ведение базы Росздравнадзора. В результате следствие получило актуальный список серий препаратов, отозванных из оборота, и сопоставило его с данными онлайн-аптек. Несколько сайтов продолжали реализовывать препараты, снятые с регистрации. Этот факт стал прямым доказательством систематического нарушения закона.*

§ 3. Типология информационных ресурсов

Современное информационное пространство отличается огромным разнообразием источников данных. Для удобства анализа и практического применения их принято систематизировать

и выделять отдельные типы. Такая классификация позволяет не только структурировать информацию, но и определить ее ценность и возможности использования в учебных, управленческих и прикладных целях.

3.1. Средства массовой информации

К этой категории относятся телевидение, радио, печатные и электронные издания, новостные порталы и семантические сайты. Их ключевые особенности – высокая посещаемость, оперативное обновление материалов и наличие мультимедийного сопровождения (фото- и видеоматериалы). СМИ зачастую становятся первыми источниками сведений об актуальных событиях, формируя информационную повестку.

Для исследователя или практического специалиста работа с такими ресурсами позволяет отследить динамику событий, выявить общественные настроения и зафиксировать факты, требующие последующей проверки в официальных источниках.

3.2. Электронные библиотеки

Электронные библиотеки представляют собой распределенные системы хранения, обеспечивающие доступ к разнообразным коллекциям документов в цифровом виде. Их ценность заключается в возможности долговременного сохранения и быстрого поиска научных трудов, учебных материалов, нормативных актов и архивных документов.

Особое значение они имеют для образовательных и экспертных задач: студент получает доступ к первоисточникам, преподаватель – к методическим разработкам, а специалист – к специализированным справочным фондам.

3.3. Электронные базы данных

Базы данных – это структурированные массивы информации, организованные таким образом, чтобы обеспечивать удобное хранение, быстрый поиск и обработку. Они могут включать самые разные форматы – от текстовых документов и электронных таблиц до мультимедийных файлов.

Сильная сторона баз данных заключается в систематизации и возможности автоматизированного анализа. Это делает их незаменимыми в управленческой, аналитической и исследовательской деятельности.

3.4. Веб-сайты

Сайт – это совокупность взаимосвязанных веб-страниц, объединенных общей тематикой и структурой. Они могут создаваться государственными органами, коммерческими организациями или частными лицами и служить целям информирования, рекламы, продажи товаров и услуг, взаимодействия с пользователями.

Содержимое сайта может включать тексты, изображения, аудио- и видеоматериалы, а также интерактивные элементы: формы обратной связи, поисковые механизмы, встроенные сервисы. Надежность и ценность информации напрямую зависят от владельца ресурса и уровня его ответственности.

3.5. Сетевые сервисы

Под сервисами понимаются сайты или платформы, предоставляющие пользователям прикладные услуги: электронную почту, блоги, поисковые системы, каталоги, справочники, сло-

вари, прогнозы погоды, телепрограммы, курсы валют. В российской практике к известным примерам относятся «Яндекс», «Рамблер» и другие комплексные сервисные порталы.

Их значимость в том, что они обеспечивают не только доступ к информации, но и удобные инструменты для ее обработки и обмена.

3.6. Информационные порталы

Информационный портал – это многоуровневая система, объединяющая различные ресурсы и сервисы, функционирующая в режиме постоянного обновления. Примером может служить портал информационной поддержки единого государственного экзамена (ЕГЭ), где собраны нормативные документы, справочные материалы и инструменты взаимодействия для всех участников образовательного процесса.

Такие порталы ценны тем, что концентрируют в одном месте большой объем информации и обеспечивают пользователям быстрый и упорядоченный доступ к ней.

§ 4. Иерархическая природа информационных ресурсов

Эффективное управление информационными ресурсами невозможно без четкой организации уровней власти и институтов, ответственных за их формирование, хранение, использование и защиту. Сложность этого процесса обусловлена многоуровневой структурой управления в Российской Федерации, где задачи и полномочия распределяются между федеральными органами власти, субъектами Российской Федерации, органами местного самоуправления и отдельными организациями.

Федеральный уровень

На федеральном уровне формируются ключевые нормативные акты, определяющие единые правила обращения с информационными ресурсами. Здесь принимаются федеральные законы, устанавливаются стандарты защиты информации, создаются крупные межведомственные базы данных и метасистемы.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) отвечает за общую стратегию развития цифровой инфраструктуры и координацию информационной политики. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) занимается защитой государственных информационных ресурсов от киберугроз и несанкционированного доступа, а Федеральная служба безопасности Российской Федерации (ФСБ России) обеспечивает защиту данных в сферах, напрямую связанных с национальной безопасностью.

Таким образом, федеральный уровень задает рамки и правила, обязательные для всех участников системы, и выступает гарантом единой государственной политики в информационной сфере.

Уровень субъектов Российской Федерации

Субъекты Российской Федерации формируют и поддерживают собственные информационные системы, отражающие региональные особенности и потребности. Региональные органы исполнительной власти создают базы данных по вопросам здравоохранения, образования, социального обеспечения, транспорта и других сфер.

К примеру, департамент информационных технологий города Москвы координирует развитие цифровой инфраструктуры в столице, внедрение электронных билетов и систем мониторин-

га транспорта. Подобные структуры есть и в других регионах, где они отвечают за организацию доступа к региональным информационным ресурсам и их защиту.

Региональный уровень выполняет двоякую функцию: с одной стороны, обслуживает локальные потребности, с другой – интегрируется в общегосударственные системы. Такое взаимодействие позволяет сопоставлять и агрегировать данные в масштабах всей страны.

Муниципальный уровень

Органы местного самоуправления формируют и используют муниципальные информационные ресурсы. Это базы данных по вопросам жилищно-коммунального хозяйства, регистрации граждан, предоставления муниципальных услуг.

Хотя такие ресурсы не всегда являются государственной собственностью, они часто служат основой для формирования региональных и федеральных массивов данных. Поэтому законодательное регулирование, договорные отношения и экономические стимулы (например, финансирование из бюджетов разных уровней) становятся важными инструментами их развития.

Уровень организаций и предприятий

Организации – как государственные, так и частные – ведут учетные системы, базы данных и реестры, напрямую связанные с их деятельностью. Руководители несут персональную ответственность за организацию работы с информацией и за предоставление сведений государственным органам и гражданам.

В этой сфере особое значение имеет унификация стандартов: если базы данных ведутся по единым правилам, это облегчает их интеграцию и делает возможным быстрый обмен информацией между ведомствами.

Взаимосвязь и координация

Ключевым вопросом управления является разграничение функций ведомственного и межведомственного управления. Ведомственная схема работает по вертикали, когда каждое министерство контролирует свои структуры и ресурсы. Межведомственная схема обеспечивает координацию на федеральном уровне и унификацию практик работы с данными.

Для обеспечения согласованности в управлении государственными информационными ресурсами важна деятельность полномочных представителей Президента Российской Федерации в федеральных округах. Они играют роль координаторов, обеспечивая баланс интересов между федеральным центром и регионами.

На современном этапе в нашей стране координация управления государственными информационными ресурсами осуществляется в рамках взаимодействия Минцифры (координация межведомственного взаимодействия и обеспечении единой политики в области информационных ресурсов), Федеральной служба по техническому и экспортному контролю (ФСТЭК; отвечает за защиту государственных информационных ресурсов от киберугроз и несанкционированного доступа), ФСБ России (обеспечение безопасности государственных информационных ресурсов, особенно в сферах, связанных с национальной безопасностью), региональных органов власти и других структур, что позволяет обеспечивать эффективное использование и защиту информационных ресурсов.

При управлении информационными ресурсами региональных и межрегиональных органов, а также организаций федерального подчинения, важно сочетать два подхода: ведомственный (когда управление идет по вертикали, от вышестоящих органов к подчиненным) и территориальный (когда управление

осуществляется на уровне регионов). Общую координацию формирования и использования этих ресурсов, а также их взаимодействие с информационными ресурсами субъектов Российской Федерации должны обеспечивать полномочные представители Президента в федеральных округах. При этом нужно учитывать утвержденные Правительством Российской Федерации схемы взаимодействия между федеральными органами власти и этими представителями.

На региональном уровне управление информационными ресурсами должно быть согласовано между исполнительной и законодательной властью субъектов Российской Федерации. В каждом регионе должен быть определен орган или организация, отвечающая за координацию, организационное и методическое обеспечение работы с информационными ресурсами.

На уровне предприятий и организаций управление информационными ресурсами направлено на поддержку их основной деятельности и выполнение обязательств по предоставлению информации государственным органам, другим организациям и гражданам. Руководители государственных предприятий и учреждений несут ответственность за реализацию государственной политики в этой области.

Особое значение имеет взаимодействие с органами местного самоуправления. Муниципальные информационные ресурсы, хотя и не являются государственной собственностью, часто служат основой для создания государственных ресурсов. Регулирование их формирования и использования должно строиться на законодательной основе (например, обязательное предоставление информации) и договорной (взаимный обмен или покупка данных). Экономическое стимулирование, например избирательное финансирование, может играть важную роль в развитии информационной деятельности и обеспечении населения информацией.

Организация управления государственными информационными ресурсами может меняться в зависимости от задач и структуры государственного управления, адаптируясь к новым условиям и вызовам.

Таким образом, иерархическая природа управления информационными ресурсами отражает сложную систему взаимодействия органов власти и организаций разных уровней. Федеральные структуры задают рамки и стандарты, субъекты Российской Федерации и муниципалитеты адаптируют их к своим задачам, а организации реализуют работу на практическом уровне. Такая система позволяет учитывать интересы разных участников и одновременно поддерживать единую политику в области информационной безопасности и управления данными.

§ 5. Классификация и использование информационных ресурсов при сборе информации

Классифицировать информационные ресурсы непросто. Они слишком разнообразны по форме, содержанию и назначению. Тем не менее для удобства работы с ними принято выделять несколько **основных критериев классификации** (рис. 4.5.1).



Рис. 4.5.1. Основные критерии классификации

Критерии классификации

1. По форме представления информации:

– текстовая;

– графическая.

Это самый общий и простой критерий: достаточно взглянуть на документ, чтобы понять, в какой группе он находится.

2. По доступу и защите:

– сведения, составляющие государственную тайну;

– персональные данные;

– коммерческая тайна.

Важно помнить: принадлежность к этим категориям определяется только законом. Именно законодательство (например, Федеральный закон № 152-ФЗ «О персональных данных») задает рамки допустимого обращения с такими ресурсами.

3. По тематике:

Самый объемный критерий, поскольку один и тот же ресурс может относиться сразу к нескольким видам. Например:

– законодательные;

– статистические;

– обучающие и др.

При этом внутри каждой группы возможна более детальная разбивка: законодательные – на международные и национальные акты, статистические – на демографию, экономику, здравоохранение и т. д.

Таким образом, классификация – это инструмент не ради красоты, а для практической навигации. Для специалиста, работающего с большими массивами данных, это способ быстрее находить нужные сведения и выстраивать систему доступа.

Коммерческие и некоммерческие ресурсы

С точки зрения формы предоставления ресурсы можно разделить на **коммерческие** и **некоммерческие**.

К некоммерческим относятся:

– центральное телевидение (новости, образовательные передачи, документальные циклы);

– радиоэфир (новости, познавательные программы);

– бесплатные печатные издания, листовки, рассылки.

Коммерческие ресурсы – это платное телевидение (в том числе зарубежные каналы), специализированные базы данных и системы, доступ к которым предоставляется по подписке.

Особое место занимает **Интернет**. Сегодня практически все СМИ имеют онлайн-версии, где информация доступна бесплатно. Но при этом специализированные сервисы (например, базы правовой информации, финансовые отчеты или аналитика) чаще всего относятся к коммерческим ресурсам.

Отдельная категория – **библиотечные фонды**. Они занимают промежуточное положение: доступ к ним формально бесплатный, но на практике может требовать оплаты за абонемент или услуги.

Пример. *Покупая газету, человек получает ограниченный объем информации. Но, зайдя в Интернет, он открывает кладовую мировых ресурсов: от мировых новостей до архивных изданий. Более того, одно и то же интервью, опубликованное на сайте официального органа власти, мгновенно превращается в глобальный ресурс, как только его перепечатывают зарубежные СМИ.*

По классам собираемой информации

1. **Первичная информация** возникает естественным образом и отражает свойства источника. Например, количество годичных колец дерева указывает на его возраст.

2. **Снимаемая информация** фиксирует социальные и экономические процессы (например, статистика по рождаемости или миграции).

3. **Производная (вторичная)** создается в результате научных исследований, обработки и анализа уже имеющихся данных.

4. **Интеллектуальная** – продукты творческой и исследовательской деятельности (литература, искусство, научные статьи).

Здесь важно подчеркнуть: именно интеллектуальные ресурсы формируют своего рода зону роста общества. Это открытия, прогнозы, новые модели и идеи, которые двигают цивилизацию вперед.

Дополнительные классификационные признаки

Информационные ресурсы можно также разделять:

– **по целевому назначению**: личные, корпоративные, образовательные, политические, культурные, сервисные и др.;

– **по способу представления**: веб-страницы, базы данных, файловые серверы, телеконференции;

– **по носителю**: бумажные, машиночитаемые (CD, флеш-накопители), каналы связи (радио, ТВ);

– **по форме собственности**: государственные, муниципальные, частные, общенациональное достояние;

– **по содержанию**: научные публикации, справочная, рекламная и новостная информация.

Информационные ресурсы как товар

Развитие цифровых технологий привело к тому, что информация превратилась в самостоятельный товар.

Этапы становления рынка. Первые профессиональные информационные службы появились в 1950-х гг. с развитием ЭВМ. Массовый рост пришелся на 1980-е гг., когда началась

глобализация обмена базами данных и услугами. Сегодня лидеры мирового рынка – США, Япония, Европа. Россия постепенно догоняет, формируя собственный рынок информационных продуктов.

Примеры товаров и услуг: научно-технические публикации, патенты, программное обеспечение, базы данных, информационные системы.

Поставщики: государственные и частные центры обработки данных, телекоммуникационные компании, консалтинговые фирмы, биржи, СМИ и даже отдельные лица.

Потребители: частные пользователи, предприятия, органы власти. Для всех них информация становится столь же важным ресурсом, как сырье или энергия.

Пример. *Рынок программного обеспечения в России мог бы быть одним из самых развитых, если бы не массовое распространение пиратских копий. С ростом правовой культуры и улучшением законодательства ситуация постепенно меняется: информация все чаще воспринимается как ценность, за которую нужно платить.*

В результате получается, что классификация и использование информационных ресурсов – это не отвлеченная теория, а **рабочий инструмент**. Для органов власти и организаций она обеспечивает прозрачность и контроль. Для бизнеса – конкурентные преимущества. Для общества в целом – основу для развития науки, культуры и экономики.

§ 6. Информационные услуги – особый вид товара на информационном рынке

Информационные услуги представляют собой уникальный вид товара, который играет ключевую роль в современной эко-

номике. Их суть заключается в предоставлении информации, ее обработке, анализе и адаптации под нужды заказчика. Эти услуги могут быть как простыми, так и сложными, в зависимости от запросов клиента и уровня развития информационной инфраструктуры. Рассмотрим несколько самых распространенных видов информационных услуг (рис. 4.6.1).

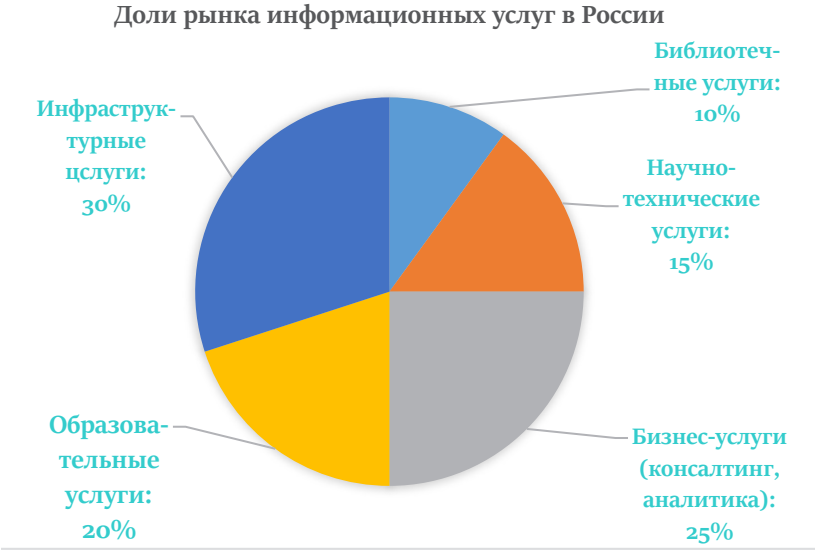


Рис. 4.6.1. Рынок информационных услуг

Основные виды информационных услуг

Библиотечные услуги. Классическим примером информационных услуг являются библиотечные фонды. Современные библиотеки не ограничиваются выдачей книг – сотрудники помогают в подборе литературы, осуществляют поиск по внешним базам и справочным системам, обеспечивая пользователя максимально полной информацией. Это важно для студентов, исследователей и практиков, работающих с большими массивами данных.

Информационные центры и институты. В России и за рубежом действуют специализированные организации, которые аккумулируют и обрабатывают сведения по отдельным областям науки и практики. Они выпускают аналитические обзоры, рефераты и справки, позволяя специалистам быстро ориентироваться в профессиональной информации.

Бизнес-услуги. Для компаний информационные услуги включают рыночную аналитику, мониторинг конкурентов, подготовку отчетов и прогнозов, а также консультации по юридическим, маркетинговым и управленческим вопросам. Это снижает уровень неопределенности и повышает качество управленческих решений.

Инфраструктурные услуги. Операторы связи и интернет-провайдеры предоставляют пользователям доступ к сети, хостинг сайтов, облачные сервисы. Эти услуги стали базовой инфраструктурой информационного общества, обеспечивая обмен данными в режиме реального времени.

Образовательные услуги. Важным направлением выступает дистанционное обучение: доступ к лекциям, учебным материалам и консультациям через интернет. Такие форматы позволяют получить образование независимо от географии и времени, что особенно важно для регионов.

Роль баз данных

Все перечисленные услуги немыслимы без баз данных – как традиционных (например, библиотечных каталогов), так и электронных. Именно они формируют основу для поиска, обработки и последующего предоставления информации.

Значение для общества и экономики

Развитие сферы информационных услуг – показатель приближения государства к полноценному информационному об-

ществу. Чем выше уровень их развития, тем доступнее знания для граждан, тем выше качество образования, научной и деловой деятельности (рис. 4.6.2).



Рис. 4.6.2. Динамика роста рынка информационных услуг в России

Информационные ресурсы и услуги становятся фундаментом экономического, социального и технологического прогресса. Они ускоряют процессы принятия решений, способствуют формированию культуры ответственного использования информации.

Для России развитие рынка информационных услуг – стратегическая задача. Совершенствование технологий и законодательства, подготовка специалистов и формирование спроса на качественные информационные продукты позволят укрепить позиции страны на мировом рынке, повысить качество жизни граждан и обеспечить устойчивое развитие в долгосрочной перспективе.

Учебно-методический раздел к главе 4

Цели изучения темы

1. Освоить понятие и значение классификации информационных ресурсов.

2. Изучить основные подходы и критерии классификации (по форме, содержанию, уровню доступа, назначению и др.).

3. Научиться анализировать взаимосвязь между видами информационных ресурсов.

4. Понять роль государства, организаций и пользователей в управлении информационными ресурсами.

5. Развить практические навыки построения схем и классификационных моделей.

Вопросы для семинарского занятия

Теоретические вопросы

1. Что понимается под классификацией информационных ресурсов?

2. Какие существуют основные критерии классификации?

3. Чем отличается государственный уровень управления ресурсами от регионального и локального?

4. В чем значение систематизации для работы с информацией в правоохранительной деятельности?

Практические вопросы

1. Опишите структуру конкретного информационного ресурса (например, базы данных МВД России).

2. Определите, по каким признакам можно классифицировать интернет-ресурсы.

3. Составьте схему классификации информационных ресурсов для выбранной организации.

Проблемные вопросы

1. Насколько универсальна классификация информационных ресурсов? Можно ли создать единую систему для всех отраслей?

2. Какие проблемы возникают при попытке интеграции государственных и корпоративных ресурсов?

3. Как классификация влияет на доступность и безопасность информации?

Дискуссионные вопросы

1. Нужно ли вводить государственный стандарт классификации информационных ресурсов?

2. Должен ли доступ к определенным видам ресурсов быть свободным или ограниченным?

3. Что важнее: открытость информации или ее безопасность?

Варианты практических заданий

1. **Составление классификационной таблицы.** Возьмите 10 различных информационных ресурсов (например, библиотека, база данных полиции, новостной портал, Telegram-канал, база судебных решений). Классифицируйте их по форме представления, тематике и уровню доступа.

2. **Построение схемы управления.** Изобразите схему управления информационными ресурсами на федеральном, региональном и локальном уровнях.

3. **Кейс-анализ.** Разберите пример: как в правоохранительной деятельности используются классифицированные базы данных (например, «Розыск» или «Свод-ГАИ»).

4. **Сравнительный анализ.** Сравните классификацию информационных ресурсов в России и в международной практике (например, ООН или Европейский Союз).

5. **Практикум по визуализации.** Постройте инфографику (таблицу или схему), отражающую взаимосвязь основных информационных ресурсов.

Учебные ситуации

1. **Ошибка классификации.** Сотрудник неправильно отнес ресурс к категории открытых, и данные оказались в свободном доступе.

Задание: определите, какие последствия это может иметь и какие меры следовало предпринять.

2. **Доступ к базе данных.** В отдел полиции поступил запрос на предоставление информации из федеральной базы.

Задание: опишите, какие уровни классификации информации будут задействованы и как регулируется доступ.

3. **Пересечение классификаций.** Один и тот же ресурс может быть классифицирован сразу по нескольким критериям.

Задание: приведите пример и определите, какие сложности это вызывает при работе с ресурсом.

Библиографический список к главе 4

Книги, учебные пособия, статьи

1. Громов, Г. Р. Национальные информационные ресурсы: проблемы промышленной эксплуатации / Г. Р. Громов. – М. : Наука, 2020.

2. Когаловский, М. Р. Информационные ресурсы и технологии в современном обществе / М. Р. Когаловский. – М. : Финансы и статистика, 2019.

3. Костров, А. В. Основы информационной безопасности : учебник / А. В. Костров. – М. : КНОРУС, 2021.

4. Лапина, М. А. Информационные системы и технологии в экономике / М. А. Лапина, А. Г. Ревин, В. И. Лапин. – М. : Юнити-Дана, 2020.

5. Симонович, С. В. Информационные ресурсы и технологии : учебное пособие / С. В. Симонович. – М. : Инфра-М, 2018.

6. Хорошилов, А. В. Мировые информационные ресурсы : учебное пособие / А. В. Хорошилов, С. Н. Селетков. – СПб. : Питер, 2004.

7. Иванов, А. А. Информационные ресурсы как основа цифровой экономики / А. А. Иванов // Информационные технологии. – 2021. – № 4. – С. 15–22.

8. Лузан, А. Ю. Понятие и виды информационных ресурсов. Мировые информационные ресурсы / А. Ю. Лузан, Т. А. Серебрякова // Вестник науки. – 2018. – Т. 4. – № 7 (7). – С. 51–54.

9. Петров, В. И. Классификация информационных ресурсов: современные подходы / В. И. Петров // Информационные ресурсы России. – 2020. – № 3. – С. 12–18.

10. Сидорова, Е. А. Управление государственными информационными ресурсами: проблемы и перспективы / Е. А. Сидорова // Государственное управление. – 2022. – № 5. – С. 44–51.

11. Федоров, Д. С. Большие данные и их роль в управлении информационными ресурсами / Д. С. Федоров // Цифровая экономика. – 2021. – № 2. – С. 33–41.

12. Шевченко, О. В. Этические аспекты использования информационных ресурсов / О. В. Шевченко // Информационное право. – 2020. – № 6. – С. 27–33.

Нормативные правовые акты

13. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Официальный интернет-портал правовой информации [сайт]. – URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102152685 (дата обращения: 04.09.2025).

14. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Официальный интернет-портал правовой информации [сайт]. – URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102152757 (дата обращения: 04.09.2025).

15. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Официальный интернет-портал правовой информации [сайт]. – URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102409979 (дата обращения: 04.09.2025).

16. Постановление Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации "Информационное общество"» // Официальный интернет-портал правовой информации [сайт]. – URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102255885 (дата обращения: 04.09.2025).

Электронные ресурсы

17. Национальный доклад «Информационные ресурсы России» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [сайт]. – URL: https://digital.gov.ru/ru/activity/reports/ (дата обращения: 04.09.2025).

Глава 5. СОЦИАЛЬНЫЕ СЕТИ: ВИДЫ, ХАРАКТЕРИСТИКА, СОДЕРЖАЩАЯСЯ ИНФОРМАЦИЯ

ВВЕДЕНИЕ

Представьте себе обычную городскую улицу. На ней кипит жизнь: кто-то разговаривает, кто-то спорит, кто-то продает или покупает, а кто-то прячется в тени и высматривает жертву. Теперь перенесите эту улицу в виртуальное пространство – это и будут социальные сети. Только здесь все происходит быстрее, шумнее и гораздо опаснее: преступник может за секунду скрыть следы, сменить маску и начать охоту заново.

Социальные сети – это не просто сайты для общения или развлечений. Для полицейского – это **новая криминальная среда**, где преступления совершаются онлайн. Здесь торгуют наркотиками через закрытые группы, здесь выманивают деньги с помощью поддельных аккаунтов, здесь экстремисты вербуют сторонников и координируют действия.

Важно понять: преступления в социальных сетях – это не абстракция, не что-то далекое. Это **сегодняшний день, повседневность каждого оперативника**. Аккаунт, фотография, пост, комментарий или пересланное сообщение могут оказаться ниточкой, ведущей к целой преступной сети.

Поэтому изучение социальных сетей для будущего сотрудника правоохранительных органов – не академический интерес, а **необходимый инструмент для раскрытия преступлений и защиты общества**.

§ 1. Возникновение. Понятие. Формы

1.1. История возникновения социальных сетей

История социальных сетей уходит корнями в далекое прошлое и начинается задолго до появления компьютеров и интернета. Еще в древности люди объединялись в племена, кланы и сообщества по признаку родства, веры или интересов. Уже тогда складывались устойчивые формы коммуникации, которые можно считать прообразами современных социальных сетей.

В античности такими площадками стали **форумы и агоры Древней Греции**, где граждане обсуждали политику, философию и культуру. В Древнем Риме роль социальных центров выполняли **термы** – общественные бани, где римляне встречались, обсуждали дела и обменивались новостями.

Позднее особое значение приобрела **переписка** – письма стали основным средством общения и обмена информацией. Этот жанр даже выделился в отдельное направление – **эпистолярная литература**. Переписка Сенеки с Луцилием, письма Цицерона к Аттику, письма Достоевского брату Михаилу или Толстого к Черткову – все это примеры того, как личная коммуникация превращалась в источник культурного наследия.

С развитием массовых коммуникаций появились новые формы «сетей». Радио и телевидение с их клубами по интересам («В мире животных», «Клуб кинопутешественников») стали объединять огромные аудитории вокруг общих тем.

Настоящий прорыв произошел в конце XX в. В 1969 г. в США был создан ARPANET – предшественник интернета. В 1991 г. появился первый веб-сайт, и интернет начал стремительно распространяться по миру. В России первые подключе-

ния состоялись в 1990 г. в Институте проблем передачи информации РАН.

Интернет изменил природу коммуникаций:

1) обеспечил **глобальный доступ** к общению без географических барьеров;

2) повысил **скорость обмена информацией** – от дней (как в письмах) до секунд;

3) создал условия для формирования **онлайн-сообществ**, где люди начали строить собственные профили и взаимодействовать друг с другом.

Первые социальные сети напоминали **электронные доски объявлений** (BBS). Первая из них – CBBS – появилась в 1978 г. Вскоре развился **Usenet** (1979), а в середине 1990-х гг. заработали сайты **Classmates.com** и **SixDegrees.com**, позволившие пользователям создавать профили и находить знакомых.

Настоящий бум пришелся на начало 2000-х гг. Тогда появились **MySpace**, **LinkedIn**, **Friendster**, а в 2004 г. – **Facebook**, который предложил принципиально новый подход: объединение реальных и виртуальных связей. Рост был колоссальным – 100 млн пользователей всего за 9 месяцев.

В России история социальных сетей началась с проектов «**Мой Мир» (2003)**, «**Одноклассники» (2006)** и «**ВКонтакте» (2006)**. Последняя, созданная Павлом Дуровым, быстро стала самой популярной площадкой в стране, объединившей миллионы пользователей.

Сегодня социальные сети – это неотъемлемая часть жизни миллиардов людей. По данным на 2024 г., число пользователей соцсетей в мире достигло **5,17 млрд человек** (63,7 % населения планеты), и ожидается, что к 2027 г. оно превысит **5,8 млрд**.

1.2. Социальные сети: понятие и основные концепции

Термин «социальная сеть» впервые был введен в научный оборот в 1954 г. социологом Джеймсом Барнсом, изучавшим связи внутри норвежского общества. Он определял социальную сеть как систему отношений между людьми, объединенных знакомством или взаимодействием. С тех пор понятие значительно расширилось. Сегодня социальные сети – это глобальные цифровые платформы, которые соединяют миллиарды людей, организаций и сообществ.

Основные понятия

Социальная сеть строится на двух базовых элементах:

– **узлы (nodes)** – пользователи, группы или организации;

– **связи (ties)** – отношения между ними (дружба, профессиональные контакты, семейные узы, совместные интересы).

На основе этих связей формируются сложные структуры:

– **центральность (centrality)** – степень влияния участника в сети;

– **кластеризация (clustering)** – образование групп и сообществ, объединенных схожими интересами или характеристиками.

Современная интерпретация

Сегодня социальные сети – это не только площадки для общения с друзьями, но и масштабные **цифровые экосистемы**. Они позволяют:

– поддерживать и расширять связи;

– обмениваться информацией и опытом;

– формировать общественное мнение и даже влиять на политические процессы;

– продвигать бизнес, товары, услуги или личный бренд;

– находить единомышленников и создавать новые сообщества.

Практическое значение

Социальные сети стали универсальным инструментом:

– **в личной жизни** они поддерживают дружбу и родственные связи;

– **в профессиональной сфере** способствуют развитию карьеры и бизнес-коммуникаций (LinkedIn, HeadHunter);

– **в общественной жизни** помогают мобилизовать граждан, организовывать акции, формировать новые социальные движения.

Таким образом, социальные сети представляют собой **структурированное пространство коммуникации**, где каждый пользователь может быть одновременно источником и потребителем информации. Их универсальность делает их важнейшей частью современного общества, а понимание ключевых концепций необходимо для эффективного и безопасного использования этих платформ.

1.3. Виды и формы социальных сетей

Социальные сети отличаются огромным разнообразием. Их можно классифицировать по структуре, целям использования и особенностям взаимодействия пользователей. Такая классификация позволяет понять, каким образом формируется социальное поведение в онлайне и какие риски или возможности скрыты за разными форматами сетей.

Теоретические основы

Еще в середине XX в. ученые выделили разные типы социальных связей и форм сетевых структур. Например, Р. Эмерсон

разграничивал связи, основанные на личной симпатии, и отношения, выстроенные на взаимной зависимости. Дж. Коулман ввел в научный оборот понятие **«социальный капитал»** – совокупность ресурсов, которые человек получает благодаря своим связям. А. М. Кастельс сформулировал концепцию **«сетевого общества»**, где горизонтальные цифровые сети становятся ключевым механизмом современной экономики, политики и культуры.

Структурные формы сетей

По характеру связей и расположению узлов можно выделить:

– **вертикальные сети** – иерархические структуры, в которых информация и команды передаются сверху вниз. Примером служат корпоративные сети управления;

– **горизонтальные сети** – связи строятся на равных, без жесткой иерархии. Чаще всего это сообщества по интересам, где пользователи объединяются для обмена опытом;

– **децентрализованные сети** – система без единого центра, где взаимодействие распределено равномерно. Такие структуры характерны для глобальных интернет-сообществ.

Типология социальных сетей

В современной практике различают несколько основных видов:

– **общие (универсальные) социальные сети** – крупнейший сегмент, предназначенный для общения, публикации личного контента и обмена новостями. Примеры: «ВКонтакте», Facebook, Instagram, Twitter;

– **профессиональные сети** – ориентированы на карьеру и деловые связи. Здесь пользователи создают резюме, обмениваются опытом и ищут работу. Примеры: LinkedIn, HeadHunter;

– **однородные сети** – объединяют людей с общими интересами, хобби или увлечениями. Примеры: Last.fm для любителей музыки, Goodreads для читателей;

– **географические сети** – строятся по принципу территориальной близости. Они позволяют искать соседей и решать локальные задачи. Примеры: Nextdoor, «Соседи.ру»;

– **сети знакомств** – помогают устанавливать романтические или дружеские контакты. Примеры: Tinder, Badoo, Bumble.

– **медиасети** – специализируются на распространении фото, видео и музыки. Примеры: YouTube, TikTok, SoundCloud;

– **мессенджеры** – коммуникационные платформы, которые во многом выполняют функции социальных сетей. Примеры: Telegram, WhatsApp, WeChat.

Сетевые модели

Исследователи выделяют также несколько типов графовых структур:

– **клубная сеть** – закрытая группа пользователей;

– **веерная сеть** – один узел связан со множеством других, но они не взаимодействуют между собой;

– **централизованная сеть** – существует главный узел, контролирующий всю коммуникацию;

– **децентрализованная сеть** – множество равнозначных узлов без доминирующего центра.

Практическое значение

Каждый тип сети имеет свои преимущества и риски. Универсальные сети дают огромный охват, но несут угрозу распространения дезинформации. Профессиональные сети способствуют развитию карьеры, но требуют строгого соблюдения правил этики. Медиасети становятся площадкой для самовы-

ражения, но одновременно вызывают зависимость от лайков и просмотров.

В современной интерпретации структура социальных сетей может быть представлена в виде графа, где узлами являются пользователи, а ребра – связи между ними.

На рис. 5.1.3. представлен пример графа простой социальной сети: узлы представляют людей или акторов, а грани между узлами – некоторые отношения между акторами.

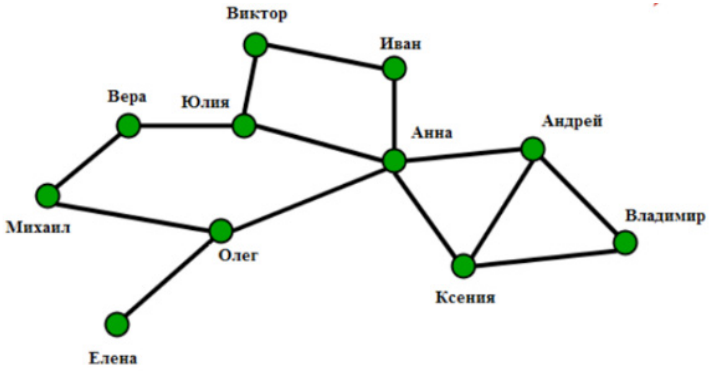


Рис. 5.1.3. Пример графа социальной сети

Таким образом, социальные сети представляют собой разнообразные платформы для общения, обмена информацией и поиска контактов. Их структура и типология зависят от множества факторов, таких как тип пользователей, цель использования и принцип взаимодействия.

Каждый вид социальной сети имеет свои особенности, предназначение и аудиторию. Пользуясь различными социальными сетями, пользователи могут находить единомышленников, делиться опытом, получать информацию, продвигать свои идеи и проекты, а также поддерживать личные и профессиональные связи.

Понимание этих аспектов позволяет более эффективно использовать социальные сети для личного и профессионального развития, а также минимизировать потенциальные риски.

Социальные сети прочно вошли в современную жизнь, став универсальными площадками для общения, обмена информацией и самоорганизации пользователей. Их значение выходит далеко за рамки развлечения: это мощный инструмент социальной динамики, политики, бизнеса и культуры. Чтобы понять специфику сетевого взаимодействия, необходимо рассмотреть их ключевые характеристики, особенности, а также виды информации, которая в них циркулирует.

Основные характеристики социальных сетей

1. **Пользовательский профиль.** Каждый зарегистрированный участник создает себе цифровую визитную карточку: указывает имя, размещает фото, информацию об интересах, образовании, работе, публикует личные материалы. Профиль становится не только средством самопрезентации, но и точкой входа в социальное взаимодействие.

2. **Социальные связи: друзья и подписчики.** Формы связи в соцсетях разнообразны. Это может быть взаимная дружба (как в «ВКонтакте» или Facebook), односторонняя подписка (Instagram, Twitter/X), членство в группах и сообществах. Такая система позволяет поддерживать контакт и с близким кругом, и с широкой аудиторией.

3. **Интерактивность и коммуникация.** Чаты, комментарии, реакции (лайки, эмодзи), репосты, видеостримы создают постоянный цикл обратной связи. Это формирует эффект присутствия, стирает границы между отправителем и получателем, превращая общение в живой процесс.

4. **Группы и сообщества.** Соцсети позволяют объединяться по интересам и целям – от небольших локальных клубов до глобальных профессиональных сетей. Именно сообщества становятся важным фактором социализации и формирования идентичности.

5. **Сетевой язык.** Со временем сформировался специфический словарь: «лайк», «репост», «сториз», «хэштег», «мем», «тролль». Эти слова давно перешли в офлайн-речь и стали частью массовой культуры.

6. **Алгоритмизация контента.** Современные соцсети работают на основе сложных алгоритмов. Они формируют индивидуальную ленту новостей, подстраиваясь под интересы пользователя. С одной стороны, это повышает комфортность общения, с другой – создает информационные пузыри.

7. **Публичность и приватность.** Пользователь сам определяет уровень доступности своей информации: полностью открытый, частично ограниченный или закрытый. Но на практике барьеры не всегда работают, что повышает риск утечки данных.

8. **Массовый охват и влияние.** Социальные сети мгновенно распространяют информацию, формируют общественное мнение, способны влиять на политические процессы и социальную активность.

9. **Самовыражение и идентичность.** Сеть становится ареной конструирования образа: многие сознательно транслируют идеальную версию себя, стремясь к признанию аудитории. Это усиливает как возможности самопрезентации, так и риски психологического давления.

1.4. Информация в социальных сетях

Содержание социальных сетей чрезвычайно разнообразно и динамично. Выделим основные виды информации.

1. **Личные данные.** Профили содержат имена, фотографии, контакты, интересы, биографию. Эти данные часто используются не только для общения, но и для коммерческих или преступных целей.

2. **Новости и обновления.** Пользователи публикуют статьи, посты, мнения, связанные с политикой, культурой, спортом. Соцсети превратились в альтернативу СМИ.

3. **Реклама и маркетинг.** Социальные платформы – один из главных каналов продвижения товаров и услуг. Алгоритмы позволяют таргетировать аудиторию с высокой точностью.

4. **Отзывы и мнения.** Важный источник информации для бизнеса, политиков и исследователей. Лайки, комментарии и репосты отражают реальные настроения аудитории.

5. **Информация о событиях.** Анонсы концертов, митингов, встреч, спортивных мероприятий распространяются мгновенно и широко.

6. **Образовательный и познавательный контент.** Онлайн-курсы, лекции, видеоуроки все чаще размещаются в соцсетях, что делает их важным инструментом самообразования.

7. **Инновации и технологии.** Новости о новых приложениях, гаджетах, цифровых сервисах активно распространяются именно через соцсети.

Особенности информации в социальных сетях

1. **Интерактивность.** Пользователи не только читают, но и создают контент, обсуждают, оценивают, дополняют его.

2. **Динамичность.** Сообщения распространяются мгновенно, что делает соцсети пульсом времени.

3. **Общедоступность.** Даже частные посты могут быть скопированы и опубликованы в других местах.

4. **Персонализация.** Ленты формируются под интересы конкретного пользователя, усиливая вовлеченность.

5. **Уязвимость.** Распространение фейков, кибербуллинг, утечки данных – неотъемлемые риски сетевой информации.

Социальные сети – это не просто площадка для общения, а многогранный феномен. Их характеристики (профиль, связи, алгоритмы, язык, публичность) тесно связаны с природой информации, которая в них циркулирует. Динамичность, массовость и интерактивность контента делают соцсети мощнейшим инструментом влияния, но одновременно порождают риски – от психологических проблем до угроз безопасности.

Проблема фейков и манипуляций

Соцсети создали благоприятную почву для распространения дезинформации. Быстрая передача сведений, отсутствие предварительной проверки и эмоциональность пользователей приводят к лавинообразному распространению слухов.

*Пример***:** в период выборов или кризисов фейки могут за считанные часы охватить миллионы пользователей и повлиять на поведение масс.

Как противостоять фейкам

Каждый пользователь обязан соблюдать цифровую гигиену:

1. **Проверять источник** – стремиться дойти до первоисточника.

2. **Сравнивать факты** – опираться на несколько проверенных СМИ.

3. **Не спешить делиться** – сохранять хладнокровие, даже если новость кажется достоверной.

4. **Использовать фактчекеры** – «Проверено», StopFake и др.

5. **Развивать критическое мышление** – анализировать, кому выгодно распространение информации.

6. **Обращаться к экспертам** – в спорных случаях лучше доверять специалистам.

Социальные сети – это одновременно **ресурс** и **угроза**. Они обеспечивают коммуникацию, образование и самовыражение, но требуют ответственного использования. Только сочетание цифровой грамотности, критического мышления и инструментов проверки информации может снизить негативные последствия.

§ 2. Технологии применения социальных сетей

Социальные сети сегодня вышли далеко за рамки обычного общения и стали полноценным инструментом, который активно используется в образовании, бизнесе, здравоохранении, гражданском обществе и даже в работе правоохранительных органов. Рассмотрим ключевые направления их применения.

2.1. Социальные сети в образовании

В образовательной сфере социальные сети стали средой для **нового формата обучения**:

– создаются виртуальные классы и сообщества;

– студенты и преподаватели обмениваются материалами в реальном времени;

– учителя отслеживают активность студентов, дают обратную связь;

– формируются навыки цифровой грамотности и работы в онлайн-команде.

Например, в университетах России активно используются закрытые группы в «ВКонтакте» для координации учебных

проектов, а также телеграм-каналы для публикации расписаний и материалов. Но важно помнить о рисках: ***неправильное разграничение личного и учебного пространства*** *может привести к нарушению приватности.*

2.2. Влияние на межличностные отношения

Социальные сети одновременно **укрепляют и разрушают связи**.

– Положительно: позволяют поддерживать отношения на расстоянии, находить новых знакомых и объединяться по интересам.

– Отрицательно: чрезмерное увлечение виртуальным общением часто приводит к **ослаблению офлайн-контактов**, зависимости и социальной изоляции.

В России известны случаи, когда конфликты в родительских чатах переходили в реальные драки, что подчеркивает необходимость цифровой этики и медиаграмотности.

2.3. Социальные сети в бизнесе

Для компаний социальные сети стали **каналом продаж и обратной связи**.

– Продвижение товаров и услуг через таргетированную рекламу.

– Работа с отзывами клиентов и репутацией бренда.

– Проведение маркетинговых исследований, анализ трендов и поведения конкурентов.

Например, российские интернет-магазины активно используют **телеграм-каналы и чаты**, а также интеграцию Instagram (организация признана экстремистской и запрещена в Российской Федерации) для прямых продаж.

2.4. Социальные сети в здравоохранении

Медицина применяет соцсети для:

– **онлайн-консультаций** и разъяснения медицинских рекомендаций;

– **просветительских кампаний** о вакцинации и здоровом образе жизни;

– **поддерживающих сообществ** для пациентов с хроническими заболеваниями.

Например, во время пандемии COVID-19 именно через соцсети распространялись инструкции Роспотребнадзора и Минздрава.

2.5. Социальные сети и гражданское общество

Соцсети стали важным инструментом **самоорганизации граждан**:

– координация митингов и акций;

– распространение петиций;

– мобилизация общественного мнения вокруг социальных проблем.

Примером служит активное обсуждение резонансных дел и общественных инициатив во «ВКонтакте» и Telegram, которые способны влиять даже на решения органов власти.

2.6. Социальные сети в профессиональной деятельности

LinkedIn (за рубежом) и HeadHunter (в России) – примеры того, как социальные платформы стали **карьерными инструментами**:

– публикация резюме и вакансий;

– установление профессиональных связей;

– обмен опытом в профессиональных сообществах.

Для российских специалистов Telegram заменил многие зарубежные площадки: здесь формируются закрытые каналы по IT, юриспруденции, маркетингу.

2.7. Социальные сети для саморазвития

Сегодня каждый пользователь может использовать соцсети как **персональный университет**:

– подписки на экспертные блоги и онлайн-курсы;

– участие в вебинарах и марафонах;

– формирование личного бренда и самопрезентация.

Соцсети помогают преодолевать географические барьеры, позволяя людям из разных регионов объединяться ради обучения и обмена знаниями.

2.8. Социальные сети в правоохранительной деятельности

В современном мире социальные сети перестали быть исключительно пространством для общения и развлечений. Сегодня они стали важным инструментом, который активно используется в работе правоохранительных органов. Их роль заключается не только в обмене информацией и налаживании контактов с гражданами, но и в выполнении стратегически значимых задач – от мониторинга угроз до сбора доказательств и профилактики преступлений.

Мониторинг и анализ данных

Одним из ключевых направлений применения социальных сетей является мониторинг информационного пространства. С помощью специальных алгоритмов и программ сотрудники

правоохранительных органов отслеживают ключевые слова, хэштеги, обсуждения и группы, связанные с противоправной деятельностью. Это помогает выявлять потенциальные угрозы – от планирования массовых беспорядков до признаков террористической активности.

Например, анализ цифрового следа позволяет в режиме реального времени фиксировать рост протестных настроений, распространение радикальной идеологии или появление новых мошеннических схем. Социальные сети становятся лакмусовой бумажкой общества, отражающей настроения граждан и указывающей на возможные очаги напряженности.

Формирование доказательственной базы

Социальные сети – это и источник ценных доказательств. Фотографии, видеозаписи, переписка, геолокация – все это может быть использовано для подтверждения факта преступления или установления причастности подозреваемого. Так, простая публикация селфи с места происшествия способна стать важным уличающим материалом.

Благодаря цифровым данным удается восстановить картину событий, подтвердить алиби или, наоборот, опровергнуть его. Более того, анализ публичных аккаунтов помогает устанавливать круг связей подозреваемого: друзей, коллег, виртуальных соратников.

Профилактика преступлений

Не менее значима и профилактическая функция социальных сетей. Через официальные аккаунты МВД России и иных структур граждан информируют о новых видах мошенничества, киберугрозах и способах защиты. Сообщения о пропавших людях, розыске преступников или чрезвычайных ситуа-

циях распространяются мгновенно и охватывают огромную аудиторию.

Кроме того, социальные сети позволяют полиции укреплять имидж открытой и доступной структуры. Примеры успешных спасательных операций, образовательные проекты, видеоролики с советами по безопасности – все это формирует доверие общества и способствует профилактике правонарушений.

Оперативная работа и скрытые методы

Отдельное направление – это использование социальных сетей в оперативной деятельности. Здесь речь идет о сборе информации о готовящихся преступлениях, выявлении участников незаконных акций, проникновении в закрытые группы.

Правоохранительные органы нередко создают легендированные аккаунты, которые позволяют взаимодействовать с подозреваемыми, входить в доверие и получать сведения, недоступные официальным путем. Такой метод применяется при выявлении экстремистских сообществ, наркосетей, а также в работе против интернет-мошенников.

Баланс возможностей и рисков

Вместе с тем использование социальных сетей в правоохранительной деятельности поднимает и ряд этических и юридических вопросов. Главный из них – баланс между эффективностью работы и защитой прав граждан. Мониторинг личной информации, использование открытых данных, внедрение в группы – все это должно строго регулироваться законодательством и не нарушать принципов конфиденциальности.

§ 3. Негативные влияния социальных сетей в процессе общения

Социальные сети стали зеркалом нашего времени. Они позволяют мгновенно делиться событиями жизни, обмениваться мнениями, поддерживать контакты. Однако вместе с удобством и доступностью они несут и целый спектр угроз, затрагивающих психику, социальные связи и безопасность личности.

Психическое здоровье и эмоциональное состояние

Стремление поддерживать идеальный образ в интернете приводит к стрессу и тревожности. Сравнение себя с другими, зависимость от лайков и подписчиков формируют эмоциональную перегрузку. К сожалению, это не абстрактные угрозы.

В России зафиксированы трагические случаи, когда подростки погибали, пытаясь сделать экстремальные селфи ради популярности. В 2021 г. в Екатеринбурге школьник сорвался с крыши многоэтажки во время съемки эффектного кадра. Другой пример – кибербуллинг, который привел к самоубийству московского подростка после травли в «ВКонтакте» в 2022 г.

Особую тревогу вызвала игра «Синий кит» и аналогичные деструктивные сообщества, манипулировавшие подростками через соцсети и подталкивавшие их к самоубийству. По данным СМИ, десятки смертей среди подростков в России связывали именно с этой игрой.

Конфиденциальность и безопасность данных

Одной из самых острых проблем остается защита персональных данных. Масштабные утечки, зафиксированные в 2024 г., когда в сеть попали миллионы записей о россиянах, показали уязвимость информационных систем. Утечка базы «Сбера», в ко-

торой оказались данные 90 % взрослых граждан страны, стала сигналом тревоги.

Социальные сети также активно используются мошенниками. Злоумышленники анализируют профили пользователей, собирают сведения о родных, увлечениях, адресах и используют их для обмана. В Санкт-Петербурге пенсионерка перевела более полумиллиона рублей «сотрудникам банка», которые в разговоре ссылались на данные из ее профиля в «Одноклассниках».

Этика и цифровое поведение

Конфликты в сети все чаще выходят за ее пределы. Так, в Волгограде в 2023 г. ссора в родительском чате привела к трагедии: мужчину избили до смерти после банальной перепалки в WhatsApp.

Не менее опасен язык вражды (hate speech). Несмотря на законодательные запреты, кибербуллинг и травля остаются массовым явлением. Один неосторожный пост способен вызвать лавину агрессии и травлю блогера или обычного пользователя.

Зависимость от социальных сетей

Среднестатистический россиянин проводит в соцсетях более двух часов в день. Это снижает продуктивность, ухудшает качество реальных отношений и подрывает здоровье. Врачи фиксируют рост числа тревожных расстройств и депрессий у молодежи, связанный именно с чрезмерным погружением в виртуальную жизнь.

Цифровой след и репутация

Каждое действие в сети оставляет след. Старые посты и комментарии могут повлиять на репутацию человека спустя годы. В Екатеринбурге сотрудник компании лишился работы после того, как коллеги нашли его резкие высказывания в «ВКонтакте».

Как противостоять угрозам

Каждый пользователь способен защитить себя, если будет соблюдать базовые правила цифровой безопасности:

1. Проверяйте источники информации и старайтесь находить первоисточники.

2. Сравнивайте факты и ориентируйтесь на проверенные СМИ.

3. Не спешите делиться сомнительным контентом.

4. Используйте сервисы фактчекинга и приложения для проверки достоверности новостей.

5. Развивайте критическое мышление и обучайте этому детей.

6. Ограничивайте время в соцсетях и не публикуйте лишние личные данные.

7. Относитесь к своим словам ответственно: виртуальное пространство напрямую влияет на реальную жизнь.

Социальные сети стали неотъемлемой частью нашей жизни. Для полиции – это ценный инструмент, для общества – мощная площадка коммуникации, для личности – возможность самореализации и одновременно источник угроз. Их грамотное использование требует баланса между пользой и рисками, а также формирования цифровой культуры, в основе которой – ответственность, критическое мышление и уважение к другим.

Учебно-методический раздел к главе 5

Цели изучения темы

1. Освоить ключевые понятия, связанные с социальными сетями: структура, виды, функции, особенности.

2. Понять их роль в жизни современного общества, включая образование, бизнес, здравоохранение, гражданское общество и правоохранительную деятельность.

3. Изучить как позитивные, так и негативные аспекты влияния социальных сетей.

4. Научиться выявлять и анализировать угрозы, связанные с дезинформацией, зависимостью, кибербуллингом и утечкой данных.

5. Развить навыки критического мышления и безопасного поведения в цифровой среде.

Вопросы для семинарского занятия

Теоретические вопросы

1. Каковы основные функции социальных сетей?

2. Какие виды и формы социальных сетей вы знаете?

3. Какую роль играют социальные сети в формировании общественного мнения?

4. Как социальные сети используются в профессиональной и правоохранительной деятельности?

Практические вопросы

1. Определите особенности структуры социальной сети на примере «ВКонтакте».

2. Объясните, какие возможности и угрозы несут социальные сети для подростков.

3. Приведите примеры использования соцсетей в профилактике преступлений.

Проблемные вопросы

1. Может ли чрезмерное использование социальных сетей быть фактором социальной изоляции? Обоснуйте ответ.

2. Каковы основные проблемы конфиденциальности и защиты данных в социальных сетях?

3. Следует ли ограничивать деятельность деструктивных интернет-сообществ только мерами блокировки?

Дискуссионные вопросы

1. Должны ли правоохранительные органы иметь доступ к данным соцсетей в расследованиях? Где проходит грань между безопасностью и правами человека?

2. Нужно ли ограничивать подросткам доступ к социальным сетям?

3. Социальные сети: больше инструмент развития или фактор риска?

Варианты практических заданий

1. **Анализ сетевых сообществ.** Составьте схему структуры выбранной социальной сети (например, «ВКонтакте» или Telegram). Отразите узлы (пользователи) и связи между ними.

2. **Кейс «Фейковая информация».** Найдите в открытых источниках пример фейковой новости, распространившейся через соцсети. Определите, какие признаки позволили бы ее выявить.

3. **Учебная ситуация «Правоохранители и соцсети».** Составьте сценарий, как полиция может использовать социальные сети для раскрытия преступления. Укажите плюсы и минусы этого подхода.

4. **Практикум по цифровой грамотности.** Составьте памятку для подростков «Пять правил безопасного поведения в социальных сетях».

5. **Исследование статистики.** Подготовьте краткий отчет о динамике роста пользователей соцсетей в России и мире (используйте свежие данные).

Учебные ситуации

1. **Опасное селфи.** Подросток погиб во время экстремальной съемки ради лайков.

Задание: определите, какие факторы (социальные, психологические, цифровые) повлияли на ситуацию. Какие профилактические меры могли бы предотвратить трагедию?

2. **Деструктивная игра («Синий кит»).** В закрытых группах подросткам предлагаются опасные задания, ведущие к суициду.

Задание: определите, как правоохранительные органы и школа должны действовать в подобных случаях.

3. **Конфликт в чате.** Ссора в родительском чате привела к драке и трагедии.

Задание: объясните, как виртуальное общение может перерасти в реальное насилие. Предложите меры профилактики.

Библиографический список к главе 5

Нормативные правовые акты

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru (дата обращения: 13.08.2025).

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ. «О персональных данных» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru (дата обращения: 03.07.2025).

3. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru (дата обращения: 18.12.2024).

4. Постановление Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru (дата обращения: 22.10.2024).

Книги, монографии, статьи

5. Castells, M. The Rise of the Network Society / M. Castells. – 2nd ed. Wiley-Blackwell, 2010.

6. Чвякин, В. А. Теория социальных сетей : учебник / В. А. Чвякин, А. С. Чертков. – Н. Новгород : НОО «Профессиональная наука», 2023.

7. Горошко, Е. И. Современная интернет-коммуникация: структура и основные параметры / Е. И. Горошко // Интернет-коммуникация как новая речевая формация : коллективная монография. – М. : Наука, 2012. – С. 45–68.

8. Винник, В. Д. Социальные сети как феномен организации общества: сущность и подходы к использованию и мониторингу / В. Д. Винник // Философия науки. – 2012. – № 4 (55). – С. 77–85.

9. Аникин, В. М. Социальные сети как феномен информационного общества / В. М. Аникин, Б. Н. Пойзнер // Вестник Томского государственного университета. – 2023. – № 483. – С. 33–41.

10. Алексеева, Е. Н. Социальная сеть как явление современного общества: история развития и общая характеристика / Е. Н. Алексеева, К. Г. Попов // Актуальные проблемы социального, экономического и информационного развития современного общества : материалы Всероссийской научно-практической конференции. – Уфа : БашГУ, 2016. – С. 92–97.

11. Barnes, J. A. Class and Committees in a Norwegian Island Parish / J. A. Barnes // Human Relations. – 1954. – Vol. 7. – № 1. – P. 39–58.

12. Битков, Л. А. Социальные сети: между массовой коммуникацией и межличностным общением / Л. А. Битков // Вестник Челябинского государственного университета. – 2012. – № 28 (282). – С. 121–128.

13. Васильева, Е. В. Трансформация социальных взаимодействий в цифровой среде / Е. В. Васильева // Социологические исследования. – 2023. – № 5. – С. 48–55.

14. Вронский, К. А. Программный модуль построения социальных графов сообществ сети «ВКонтакте» / К. А. Вронский, Е. А. Шеленок // Вестник Тихоокеанского государственного университета. – 2021. – № 2 (61). – С. 77–85.

15. Григорьев, М. С. Контент-анализ социальных сетей: методология и практика / М. С. Григорьев // Вестник МГУ. Сер. 18: Социология и политология. – 2023. – № 2. – С. 90–99.

16. Дубровский, М. О. История возникновения и развития социальных сетей / М. О. Дубровский // Инновации. Наука. Образование. – 2020. – № 23. – С. 12–19.

17. Дужникова, А. С. Социальные сети: современные тенденции и типы пользования / А. С. Дужникова // Мониторинг общественного мнения. – 2010. – № 5 (99). – С. 56–64.

18. Забарная, Э. Н. Социальный медиа-маркетинг (на примере системы образования) / Э. Н. Забарная, И. В. Куриленко // Вестник Волынского института экономики и менеджмента. – 2012. – № 5. – С. 22–27.

19. Иванова, А. Е. Цифровые социальные сети: структура и динамика развития / А. Е. Иванова // Мир России. Социология. Этнология. – 2023. – № 3. – С. 60–68.

20. Кураева, С. А. К методологии исследования социальных сетей / С. А. Кураева // Научные труды Московского гуманитарного университета. – 2017. – № 1. – С. 33–40.

21. Левин, Л. М. Социальные сети: основные понятия, характеристики и современные исследования / Л. М. Левин // Проблемы советского образования. – 2019. – № 4. – С. 15–22.

22. Морозова, А. А. Достоверность информации в социальных сетях и критерии ее верификации (на примере «ВКонтакте») / А. А. Морозова // Вестник Челябинского государственного университета. – 2017. – № 6 (402). – С. 100–107.

23. Огнева, А. С. Социальные сети: понятие, виды, технологические возможности продвижения / А. С. Огнева // Молодой ученый. – 2021. – № 9 (351). – С. 217–222.

24. Петров, Д. В. Социальные сети как инструмент / Д. В. Петров // Вестник электронных и печатных СМИ. – 2016. – № 1 (24). – С. 11–16.

25. Руденок, Д. В. Социальные сети как источник информации / Д. В. Руденок // Вестник электронных и печатных СМИ. – 2016. – № 1 (24). – С. 17–23.

26. Сергодеев, В. А. Сетевые интернет-сообщества: сущность и социокультурные характеристики / В. А. Сергодеев // Вестник Адыгейского государственного университета. Сер.: Регионоведение. – 2013. – № 1. – С. 33–41.

27. Шахмартова, О. М. Психологические аспекты общения в социальных сетях виртуальной реальности / О. М. Шахмартова, Е. Ю. Болтаг // Известия ПГПУ им. В. Г. Белинского. – 2011. – № 24. – С. 1002–1008.

28. Шевченко, О. В. Этические аспекты использования социальных сетей / О. В. Шевченко // Информационное право. – 2021. – № 4. – С. 44–49.

29. Петров, В. И. Классификация социальных сетей: современные подходы / В. И. Петров // Информационные ресурсы России. – 2020. – № 2. – С. 15–20.

Электронные ресурсы

30. Статистика утечек данных в Российской Федерации за 2024 год. – URL: https://example.ru/data-leaks-2024 (дата обращения: 02.09.2025).

31. We Are Social, Hootsuite. Digital 2024: Global Overview Report. – URL: https://wearesocial.com/ (дата обращения: 02.09.2025).

Глава 6. ОФИЦИАЛЬНЫЕ ЗАПРОСЫ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ С ЦЕЛЬЮ ПОЛУЧЕНИЯ ОПЕРАТИВНО ЗНАЧИМОЙ ИНФОРМАЦИИ

ВВЕДЕНИЕ

Преступность остается одной из ключевых проблем современного общества, а эффективность борьбы с ней во многом зависит от качества работы правоохранительных органов. Одним из важнейших показателей их деятельности является уровень раскрываемости преступлений. Он отражает не только состояние криминогенной обстановки, но и способность органов внутренних дел оперативно и качественно расследовать уголовные дела.

В последние годы в Российской Федерации фиксируется тенденция к снижению общего числа зарегистрированных преступлений. Однако на этом фоне сохраняется стабильно высокий уровень нераскрытых дел. Это свидетельствует о наличии системных проблем в организации расследований и в сборе оперативно значимой информации. Нераскрытые преступления формируют так называемую **латентную преступность**, которая подрывает доверие граждан к органам правопорядка и создает условия для повторных правонарушений.

В этих условиях особое значение приобретают **официальные запросы правоохранительных органов**, направленные на получение оперативно значимой информации. Запросы позволяют получить данные, необходимые для установления фактов, поиска подозреваемых и доказательства их вины. Эффективность их применения напрямую зависит от качества правовой базы, технических возможностей и уровня взаимодействия между ведомствами.

§ 1. Проблемы раскрываемости преступлений и роль официальных запросов в получении оперативно значимой информации

Современное состояние преступности в Российской Федерации демонстрирует противоречивую динамику. С одной стороны, статистика фиксирует снижение общего числа зарегистрированных преступлений: в 2024 г. их количество уменьшилось на 1,8 % и составило 1 911,3 тыс. деяний. Отмечается уменьшение преступлений против личности (–7,7 %), числа убийств и покушений на убийство (–9,8 %), случаев умышленного причинения тяжкого вреда здоровью (–8,1 %), а также значительное сокращение имущественных преступлений: квартирных краж (–28,7 %), краж автомобилей (–19,5 %), грабежей (–20,7 %) и разбоев (–16,3 %) [МВД России, 2025].

Однако за этой позитивной тенденцией скрывается серьезная проблема – рост преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Их доля достигла 40 % от общего числа зарегистрированных деяний, что на 13,1 % больше, чем в 2023 г. При этом увеличилась и тяжесть таких преступлений: количество тяжких и особо тяжких составов выросло на 7,8 %.

1.1. Нераскрытые преступления и латентная преступность

Несмотря на общее снижение преступности, количество нераскрытых преступлений остается стабильно высоким. В 2024 г. таких преступлений зарегистрировано 929,7 тыс., что на 2 % больше, чем годом ранее. Особенно тревожит тот факт, что треть из них – тяжкие и особо тяжкие составы, включая:

– 381 убийство и покушение на убийство (+62,8 %);

– 293 случая умышленного причинения тяжкого вреда здоровью (–12,8 %);

– 283,6 тыс. краж (–18,4 %);

– 2,2 тыс. грабежей (–37,2 %);

– 115 разбойных нападений (–20,7 %).

Причина кроется в том, что значительная часть уголовных дел возбуждается по факту совершения преступления без установления конкретного подозреваемого. В итоге дела приостанавливаются, формируя так называемую «латентную преступность». В 2024 г. 902,3 тыс. дел (+1,5 %) остались безрезультатными именно из-за невозможности установления лица, подлежащего привлечению к ответственности.

1.2. Информационные барьеры

Одной из ключевых проблем является неполучение правоохранительными органами информации от организаций, располагающих оперативно значимыми данными:

– финансово-кредитных учреждений;

– операторов связи;

– интернет-провайдеров;

– транспортных и логистических компаний;

– социальных сетей и онлайн-площадок.

Зачастую такие организации либо отказывают в предоставлении сведений, ссылаясь на ограничения законодательства (например, законы о банковской тайне или о персональных данных), либо игнорируют запросы. Нередки случаи, когда данные возвращаются из-за ошибок в оформлении самих запросов.

Согласно статистике МВД России, ежегодно территориальные органы внутренних дел направляют более 200 тыс. офици-

альных запросов. Однако их реальное число значительно выше, так как в этот показатель не входят запросы спецподразделений и иных правоохранительных структур.

1.3. Роль официальных запросов

Официальные запросы позволяют получить сведения, имеющие решающее значение для:

– установления личности подозреваемого;

– формирования доказательственной базы;

– розыска преступников;

– выявления каналов совершения и сокрытия преступлений.

Таким образом, запросы к организациям – это ключевой инструмент оперативно-разыскной деятельности, эффективность которого напрямую влияет на уровень раскрываемости.

§ 2. Нормативные правовые документы, регламентирующие понятие «запросы»

2.1. Общие положения и семантика термина

Термин *«запрос»* в русском языке имеет несколько значений: от «обращения за сведениями» до «официального требования предоставить информацию». В правоприменительной практике под ним чаще всего понимается **обязательное обращение уполномоченного органа** (или должностного лица) к обладателю информации о ее предоставлении.

Законодательство Российской Федерации не содержит единого нормативного определения запроса, однако этот термин регулярно встречается в ключевых законах, регламентирующих

деятельность полиции и органов, осуществляющих оперативно-разыскные мероприятия (ОРМ).

Особое значение в работе полиции имеет понятие **«мотивированный запрос»**. Хотя оно прямо не раскрыто в законе, под ним подразумевается наличие ссылки на законные основания (уголовное или административное дело, проверка сообщения о преступлении, проведение ОРМ), а также описание целей и обстоятельств, требующих истребования информации.

2.2. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»

Закон о полиции закрепляет широкий перечень полномочий, связанных с запросами информации:

– **Статья 13, ч. 1, пп. 3, 4** – право полиции истребовать сведения по расследуемым уголовным делам, материалам о преступлениях и административных правонарушениях.

– **Поручения следователя или дознавателя**: полиция вправе направлять запросы в адрес любых организаций и должностных лиц для выполнения следственных действий.

– **Специальные полномочия**: например, запрос информации при обеспечении авиационной безопасности (п. 27 ч. 1 ст. 13).

– **Налоговые сведения**: полиция может получать данные, составляющие налоговую тайну (п. 29 ч. 1 ст. 13).

Согласно ч. 4 ст. 13, запросы подлежат исполнению в сроки, указанные в документе, но не позднее 30 дней.

2.3. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»

Запросы рассматриваются в рамках ОРМ *«наведение справок»* (ст. 6). Это **обязательное обращение оперативного подразделения** к обладателю информации с требованием ее предоставить.

Основания для проведения (ст. 7 ФЗ):

1. Возбужденное уголовное дело.

2. Данные о признаках готовящегося, совершаемого или совершенного преступления.

3. Сведения о лицах, скрывающихся от органов дознания, следствия или суда.

4. Запросы других подразделений, ведущих ОРД.

5. Международные запросы в рамках договоров Российской Федерации.

Таким образом, даже на стадии доследственной проверки правоохранительные органы могут использовать запросы как инструмент выявления и пресечения преступлений.

2.4. Уголовно-процессуальное законодательство

УПК РФ (ст.ст. 144, 145) предусматривают возможность получения информации в рамках проверки сообщений о преступлении. Следователь или дознаватель направляют запросы в государственные и частные организации, которые обязаны их исполнить.

2.5. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»

Часть 1 ст. 6 обязывает организации предоставлять сведения, составляющие коммерческую тайну, по мотивированным

требованиям госорганов. Отказ возможен только в судебном порядке.

2.6. Ответственность за неисполнение

Нарушение сроков или отказ в предоставлении информации влечет ответственность по:

– **статье 19.7 КоАП РФ** – непредставление сведений:

– граждане – 100–300 руб.;

– должностные лица – 300–500 руб.;

– юридические лица – 3 000–5 000 руб.;

– **статье 17.7 КоАП РФ** – невыполнение требований следователя или дознавателя:

– граждане – 1 000–1 500 руб.;

– должностные лица – 2 000–3 000 руб. или дисквалификация до года;

– юридические лица – 50 000–100 000 руб. или приостановление деятельности до 90 суток.

2.7. Итоговое определение

Запросы полиции и иных подразделений МВД России – это **обязательная юридическая форма обращения уполномоченного органа к обладателю информации, применяемая для получения данных, значимых для проверки заявлений о преступлениях, расследования уголовных дел и проведения оперативно-разыскной деятельности.**

И хотя единое определение запроса в законодательстве отсутствует, совокупность норм ФЗ «О полиции», ФЗ «Об ОРД», УПК РФ, ФЗ «О коммерческой тайне» и КоАП РФ позволяет рассматривать его как инструмент, имеющий клю-

чевое значение для обеспечения законности и раскрытия преступлений.

§ 3. Формы и виды официальных запросов

3.1. Общая характеристика

В соответствии со ст.ст. 2 и 6 Федерального закона от 27 июля 2006 г. № 149-ФЗ *«Об информации, информационных технологиях и о защите информации»* лицо, создавшее информацию или получившее право распоряжаться ею, признается **обладателем информации**. К нему правоохранительные органы могут обращаться для предоставления сведений в двух формах: устной и письменной.

Выбор формы зависит от **ситуации, характера информации и степени ограничений на доступ**. При этом письменная форма обладает большей юридической силой и используется в подавляющем большинстве случаев.

3.2. Устные запросы

Устная форма обращения применяется при оперативной необходимости, когда информация:

– не имеет ограничений доступа;

– не затрагивает права и интересы обладателя;

– требуется для предотвращения или пресечения преступления.

Разновидности устных запросов

– **Бездокументарные** – обращение не фиксируется на материальном носителе (например, устный опрос сотрудника организации).

– **Документарные** – устное обращение сопровождается фиксацией на аудио- или видеоустройства (с учетом положений ст. 2 ФЗ № 149-ФЗ и ГОСТ Р 7.0.8–2013, где зафиксированная информация считается документированной).

Недостатки устных запросов:

– невозможность доказать факт отказа в предоставлении сведений;

– невозможность использования устного запроса как официального доказательства в суде;

– внутренние регламенты большинства организаций требуют письменного документа.

Поэтому устные формы носят **оперативно-тактический характер** и применяются в экстренных ситуациях, *например при розыске лица по горячим следам, уточнении информации о месте происшествия, предотвращении угрозы безопасности.*

3.3. Письменные запросы

Письменные запросы являются основным инструментом в деятельности полиции и иных органов, поскольку:

– обладают статусом официального документа;

– могут быть использованы в суде;

– фиксируют права и обязанности сторон;

– обеспечивают контроль над сроками и содержанием ответа.

К письменным запросам относятся:

– запросы к операторам связи (получение детализации звонков и SMS);

– запросы в банки (движение средств, сведения об операциях);

– запросы к интернет-провайдером (установление IP-адресов, трафика);

– запросы в государственные органы и коммерческие структуры (адресные данные, сведения о договорах, перемещении товаров).

Структура официального письма-запроса в обязательном порядке включает в себя:

1. Исходящий номер и дату.

2. Должность, звание и ФИО сотрудника, направившего запрос.

3. Четкую формулировку запрашиваемых сведений.

4. Ссылку на нормы законодательства, дающие право требовать информацию (например, ст. 13 ФЗ «О полиции», ст. 6 ФЗ «Об ОРД»).

5. Подпись уполномоченного лица и печать органа.

Преимущества письменной формы:

– фиксируется в делопроизводстве;

– позволяет точно сформулировать требуемые сведения;

– снижает риск отказа;

– облегчает контроль исполнения и последующее обжалование.

3.4. Практические примеры

– В рамках расследования дела о мошенничестве следователь направляет запрос в банк для получения сведений о движении средств по карте подозреваемого.

– При расследовании киберпреступлений дознаватель запрашивает у провайдера данные об IP-адресе, с которого велась переписка.

– В рамках розыска пропавшего лица полиция направляет письменный запрос оператору мобильной связи с целью установить местоположение абонента по данным базовых станций.

3.5. Итоговые выводы

Формы запросов в деятельности правоохранительных органов можно разделить на **оперативные (устные)** и **официальные (письменные)**. Первые удобны в экстренных условиях, но ограничены по юридической значимости. Вторые обеспечивают надежность, правовую силу и возможность последующего использования в суде.

Таким образом, **письменная форма является основной**, а устная выполняет вспомогательную функцию и применяется в оперативной тактике.

§ 4. Характеристики и особенности официальных запросов

Официальные запросы правоохранительных органов – это не просто формальные письма, а документы, обладающие юридической силой и подчиняющиеся строгим правилам оформления и исполнения. Их грамотная подготовка во многом определяет эффективность получения оперативно значимой информации.

4.1. Нормативная основа оформления

Запросы оформляются в виде служебных писем. Согласно **приказу МВД России от 2 сентября 2024 г. № 515 «Об утверждении Инструкции по делопроизводству в органах внутренних дел»**, служебными письмами закрепляются инициативные документы органов внутренних дел.

Ключевая правовая база:

– **ФЗ «О полиции» (ст. 13)** – закрепляет право полиции запрашивать документы, объяснения и справки по уголовным де-

лам, административным материалам и при проверке сообщений о преступлениях;

– **ФЗ «Об оперативно-розыскной деятельности» (ст.ст. 6, 7, 15)** – определяет запрос как разновидность ОРМ «наведение справок» и возлагает обязанность на граждан и организации исполнять законные требования органов, осуществляющих ОРД;

– **ФЗ «О коммерческой тайне» (ст. 6)** и **ФЗ «О банках и банковской деятельности» (ст. 26)** – регулируют порядок предоставления информации, относящейся к охраняемой тайне.

4.2. Структура и содержание официального запроса

Служебное письмо-запрос состоит из двух частей:

1. **Обоснование (мотивировка):**

– ссылки на нормы законодательства (ФЗ «О полиции», ФЗ «Об ОРД», УПК РФ, КоАП РФ);

– функциональная необходимость (например, выявление налоговых преступлений подразделениями ЭБиПК);

– фактические обстоятельства (возбужденное уголовное дело, зарегистрированное сообщение о преступлении, номер КУСП).

2. **Просьба (требование):**

– конкретный перечень запрашиваемых сведений или документов;

– форма их предоставления (на бумажном носителе, в электронном виде, копии);

– срок исполнения.

Ключевой момент – **мотивированность**. Без четкой ссылки на закон и фактические основания запрос может быть признан необоснованным, что создает риск его оспаривания.

4.3. Особенности и проблемы

– **Отсутствие единых стандартов.** Закон прямо не регламентирует структуру запроса, поэтому на практике часто используются смешанные мотивировки (одновременно ссылки на ФЗ «О полиции» и ФЗ «Об ОРД»).

– **Судебная практика.** Суды нередко признают достаточной даже минимальную мотивировку («служебная необходимость»), исходя из принципа законности и обязательности исполнения запросов.

– **Принцип конспирации.** Согласно ФЗ «Об ОРД», органы не обязаны раскрывать в запросе все цели и условия проведения оперативного мероприятия. Это может намеренно скрываться для соблюдения принципов конспирации и негласности.

4.4. Сроки и порядок исполнения

Сроки исполнения прямо законом не закреплены (кроме запросов следователя/дознавателя). На практике применяются:

– **ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»** – общий срок 30 дней;

– **внутренние инструкции МВД России** – конкретный срок указывается в самом запросе.

Формы передачи информации:

1) почтовое отправление;

2) факсимильное сообщение;

3) электронное письмо;

4) личная передача сотруднику полиции.

4.5. Ответственность за неисполнение

– **Статья 19.7 КоАП РФ** – непредставление сведений по запросу полиции: предупреждение или штраф (от 100 до 5000 руб. в зависимости от статуса лица).

– **Статья 17.7 КоАП РФ** – невыполнение законных требований следователя или дознавателя: штраф до 100 000 руб., а для юридических лиц – административное приостановление деятельности до 90 суток.

4.6. Итоговые характеристики

Официальные запросы обладают следующими особенностями:

– они всегда должны быть мотивированными (правовое, функциональное и фактическое обоснование);

– имеют обязательный характер исполнения;

– являются источником документированной информации, которая может использоваться в суде;

– судебная практика трактует их максимально в пользу правоохранительных органов;

– несоблюдение сроков или отказ в предоставлении информации влечет юридическую ответственность.

4.7. Основные проблемы, возникающие при подготовке и направлении запросов

На практике процесс подготовки и направления официальных запросов сталкивается с рядом трудностей.

1. **Ошибки в оформлении документов.** Сотрудники органов внутренних дел нередко допускают неточности при со-

ставлении запросов: отсутствуют обязательные реквизиты, неверно указаны основания, используются неактуальные ссылки на нормативные акты. Это приводит к отказу организаций в предоставлении сведений или к необходимости направлять повторные обращения, что существенно затягивает расследование.

2. **Недостаточная подготовка кадров.** Не все сотрудники владеют знаниями о том, какие именно сведения можно и нужно запрашивать. В результате правоохранительные органы иногда требуют от организаций данные, которые не могут быть предоставлены без решения суда, или формулируют запрос слишком расплывчато.

3. **Ссылки на законодательные ограничения.** Организации, получившие запрос, часто отказывают в предоставлении информации, ссылаясь на режим банковской, коммерческой или налоговой тайны. Однако в соответствии с Федеральным законом «О полиции» и Федеральным законом «Об оперативно-розыскной деятельности» предоставление сведений допускается по мотивированным запросам уполномоченных органов.

4. **Отсутствие единых технических стандартов.** Запросы направляются в различных форматах: почтой, факсом, электронной почтой, через ведомственные системы. Это приводит к несогласованности и увеличивает сроки их обработки.

5. **Несвоевременность ответов.** Организации не всегда соблюдают установленные законом сроки ответа на запросы. Иногда сведения поступают слишком поздно и теряют оперативную ценность.

Наиболее полно типичные ошибки представлены в табл. 4.

Таблица 4

Типовые ошибки при оформлении запросов и их последствия

Ошибка при оформлении запроса	Пример/суть ошибки	Последствия	Рекомендации
Отсутствие ссылки на правовую норму	«Прошу предоставить сведения…» без указания статьи закона	Запрос могут признать необоснованным	Всегда указывать статью, часть, пункт НПА, на основании которых делается запрос
Неполные сведения об адресате	Не указан конкретный орган или подразделение	Задержка или возврат запроса	Указывать точное наименование организации и структурного подразделения
Нет даты и регистрационного номера	Запрос оформлен без даты и исходящего номера	Потеря юридической силы документа	Всегда ставить дату и номер регистрации документа
Некорректное указание должности и Ф. И. О.	Ошибки в должности адресата или Ф. И. О.	Формальный отказ в ответе	Проверять реквизиты по официальным источникам
Нарушение официально-делового стиля	Разговорные формулировки, сокращения без расшифровки	Уменьшение авторитета документа, риск отказа	Использовать единый официальный стиль, раскрывать сокращения при первом упоминании
Отсутствие подписи и печати	Запрос без подписи должностного лица и печати	Юридическая ничтожность документа	Подписывать руководителем/уполномоченным лицом, заверять печатью
Несоблюдение формата и структуры	Отсутствие шапки, обращения, основной части или заключения	Документ возвращается без рассмотрения	Соблюдать стандартную структуру служебных писем
Прикладываются неподтвержденные копии	Приложения без заверения	Их могут не принять	Заверять приложения печатью и подписью
Отсутствие контактных данных отправителя	Нет адреса/телефона для обратной связи	Затруднена коммуникация	Включать контакты для ответа и уточнений
Ошибки в ссылках на НПА	Упоминание утраченных силу законов (например, приказ МВД России № 615, заменен на № 515)	Признание запроса юридически некорректным	Проверять актуальность нормативных актов и использовать действующие редакции

Таким образом, официальные запросы правоохранительных органов – это один из ключевых инструментов получения оперативно значимой информации. От качества их подготовки и своевременности исполнения зависят эффективность расследования преступлений и уровень раскрываемости дел. Проблемы подготовки и направления запросов обусловлены как человеческим фактором (ошибки сотрудников, недостаточная квалификация), так и объективными обстоятельствами (отсутствие единых стандартов, задержки со стороны организаций). Для повышения эффективности необходимо совершенствовать нормативную базу, обучать сотрудников правильному оформлению запросов и развивать технические средства взаимодействия между ведомствами.

Для повышения эффективности необходимо:

– совершенствовать нормативную правовую базу, уточняя перечень обязательных для предоставления сведений;

– закреплять единые стандарты оформления запросов (включая унифицированные электронные формы);

– развивать технические средства обмена информацией и внедрять единую платформу для взаимодействия ведомств;

– повышать уровень подготовки сотрудников, формируя у них практические навыки правильного составления запросов.

Законодательная база (ФЗ «О полиции», ФЗ «Об оперативно-розыскной деятельности», УПК РФ, приказ МВД России № 515) предоставляет достаточные полномочия для эффективного получения данных. Однако их практическая реализация требует системной доработки и организационной дисциплины.

Для студентов и будущих специалистов важно понимать, что умение грамотно составлять запросы – это не только юридиче-

ский навык, но и элемент профессиональной культуры сотрудника органов внутренних дел. Правильно оформленный запрос способен существенно ускорить расследование, а неверно составленный – затянуть процесс и снизить доверие граждан к правоохранительной системе.

Учебно-методический раздел к главе 6

Цели изучения темы

1. Освоить базовые понятия и правовые основы оформления официальных запросов.

2. Понять роль запросов в раскрытии и расследовании преступлений.

3. Научиться составлять корректные запросы в государственные органы и организации.

4. Получить опыт выявления и исправления ошибок.

5. Развить критическое мышление в оценке баланса «права на информацию ↔ право на неприкосновенность частной жизни».

Вопросы для семинарского занятия

Теоретические вопросы

1. Какие виды запросов применяются в правоохранительной деятельности?

2. Что обязательно должно содержаться в запросе?

3. Каковы отличия национальных и международных запросов?

Практические вопросы

1. Составьте идеальный запрос в банк о движении денежных средств.
2. Подготовьте текст запроса оператору связи о детализации звонков.
3. Разработайте проект межведомственного запроса в Роскомнадзор.

Проблемные вопросы

1. Что произойдет, если сослаться на утративший силу приказ?
2. Какие риски несет неправильный адресат?
3. Может ли организация отказать в предоставлении данных?

Дискуссионные вопросы

1. Должны ли правоохранительные органы иметь упрощенный доступ к персональным данным?
2. Где проходит грань между безопасностью и правами человека?
3. Что важнее: эффективность раскрытия преступлений или защита частной жизни?

Варианты практических заданий

1. Редактор ошибок: получите задание с испорченным запросом и исправьте все ошибки.
2. Кейс «Неверный адресат». В группу направлен запрос не по компетенции. Определите последствия и разработайте алгоритм предотвращения.

3. Международный вызов. Подготовьте проект запроса в Meta (Facebook), учтите юрисдикцию и международные конвенции.

4. Памятка сотруднику. Составьте 10 правил оформления запросов.

Учебные ситуации

1. Ошибочный запрос. Следователь направил запрос с указанием приказа МВД России № 615 (утратил силу). Определите, на какой НПА нужно сослаться (актуальный приказ № 515), и разработайте меры профилактики ошибок.

2. Отказ в предоставлении данных. Оператор связи вернул запрос с мотивировкой «отсутствие процессуальных оснований». Укажите, какие статьи УПК РФ должны были быть использованы.

3. Международный запрос». Российским правоохранительным органам нужно получить данные из США. Опишите процедуру: от Минюста России через MLA (Mutual Legal Assistance) до компании.

Библиографический список к главе 6

Нормативные правовые акты

1. Федеральный закон от 12 агуста 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 04.09.2025).

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». – https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 04.09.2025).

3. Уголовный кодекс Российской Федерации : УК : Федеральный закон № 63-ФЗ : принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 04.09.2025).

4. Уголовно-процессуальный кодекс Российской Федерации : УПК : Федеральный закон № 174-ФЗ : принят Государственной Думой 22 ноября 2001 г. : одобрен Советом Федерации 5 декабря 2001 г. (ред. от 20.03.2025) // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 04.09.2025).

5. Кодекс Российской Федерации об административных правонарушениях : КоАП : Федеральный закон № 195-ФЗ : принят Государственной Думой 20 декабря 2001 г. : одобрен Советом Федерации 26 декабря 2001 г. (ред. от 07.07.2025) // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 04.09.2025).

6. Указ Президента Российской Федерации от 11 марта 2003 г. № 306 «Вопросы совершенствования государственного управ-

ления в Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_41421/ (дата обращения: 04.09.2025).

7. Указ Президента Российской Федерации от 6 сентября 2008 г. № 1316 «О некоторых вопросах Министерства внутренних дел Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_79834/ (дата обращения: 04.09.2025).

8. Приказ МВД России от 15 сентября 2021 г. № 515 «Об утверждении Инструкции о порядке оформления запросов» // СПП «КонтурНорматив». – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=402593&ysclid=mfcmht9prd646299661 (дата обращения: 24.12.2024).

Учебники, монографии, комментарии

9. Оперативно-розыскная деятельность : учебник для студентов вузов, обучающихся по специальности «Юриспруденция» / под ред. И. А. Климова. – М. : Юнити-Дана, 2014.

10. Федеральный закон «Об оперативно-розыскной деятельности» : научно-практичкский комментарий / под ред. д-ра юрид. наук, проф. А. С. Бахты. Хабаровск : РИО ДВЮИ МВД России, 2013.

11. Баранов, В. В Информационные технологии управления и организация защиты информации : учебник / [В. В. Барановв и др.]. – М. : Академия управления МВД России, 2018.

12. Горошко, И. В. Информационные технологии в науке и образовании : учебное пособие / И. В. Горошко, Б. А. Торопов. – М. : Академия управления МВД России, 2021.

13. Шумилов, А. Ю. Оформление запросов в уголовном процессе / А. Ю. Шумилов. – М. : Юрлитинформ, 2020.

Статьи, сборники

14. Кольцов, Д. В. Запрос как форма реализации оперативно-розыскного мероприятия «Наведение справок» (на примере подразделения ЭБиПК МВД России) / Д. В. Кольцов // Вестник Санкт-Петербургского университета МВД России. – 2018. – № 2 (78). – С. 144–149.

15. Направление запросов при расследовании уголовных дел о преступлениях, совершенных с использованием IT-технологий: организации и располагаемые ими сведения. – М. : Московский университет МВД России имени В. Я. Кикотя, 2022.

16. Иванова, Н. В. Международные запросы о правовой помощи / Н. В. Иванова // Российская юстиция. – 2022. – № 5. – С. 67–74.

Международные документы

17. Конвенция Совета Европы о взаимной правовой помощи по уголовным делам (Страсбург, 1959) // Электронный фонд правовых и нормативно-технических документов [сайт]. – URL: https://docs.cntd.ru/document/1902175?ysclid=mfcmlbb8tx620661064 (дата обращения: 04.10.2024).

18. Interpol. Руководство по международным запросам. –Lyon : Interpol, 2023.

Электронные ресурсы, отчеты

19. Национальный стандарт Российской Федерации. ГОСТ Р 7.0.8–2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_163800/ (дата обращения: 04.09.2025).

20. Национальный стандарт Российской Федерации. ГОСТ Р 6.30–2003 «Организационно-распорядительная документация. Требования к оформлению документов. Методические рекомендации по внедрению» (документ утратил силу) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_112673/ (дата обращения: 04.09.2025).

21. Roskomnadzor. Annual Report on Information Security. 2024. – URL: https://rkn.gov.ru (дата обращения: 04.09.2025).

Глава 7. МЕТОДИКА ВЫЯВЛЕНИЯ И ПРЕСЕЧЕНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБОРОТОМ КУЛЬТУРНЫХ ЦЕННОСТЕЙ В СЕТИ ИНТЕРНЕТ

ВВЕДЕНИЕ

Незаконный оборот культурных ценностей остается одной из серьезных проблем современного общества. По данным международных организаций, объем рынка незаконного оборота антиквариата, произведений искусства и археологических находок занимает третье место среди криминального бизнеса после торговли наркотиками и оружием.

Развитие сети Интернет и цифровых технологий радикально изменило масштабы и формы таких преступлений. Сегодня продажа и покупка предметов, представляющих историческую, художественную или археологическую ценность, часто осуществляется через онлайн-платформы, специализированные сайты и закрытые сообщества в даркнете. Это позволяет злоумышленникам скрывать свою личность, использовать анонимные способы оплаты (в том числе криптовалютой) и обходить традиционные механизмы контроля.

Особенностью преступлений в данной сфере является их международный характер. Культурные ценности незаконно перемещаются через границы, а сделки совершаются между участниками, находящимися в разных странах. В таких условиях борьба с этим видом преступности требует не только национальных, но и международных усилий, включая сотрудничество правоохранительных органов, Интерпола и специализированных организаций, таких как ЮНЕСКО.

В Российской Федерации данная проблема также сохраняет актуальность. Незаконный вывоз предметов искусства, археологии и иконописи наносит ущерб национальному культурному наследию. Одновременно фиксируются случаи обратного ввоза – когда ценности, вывезенные нелегально, возвращаются в страну нелегальными путями. В обоих случаях Интернет выступает как канал коммуникации и инструмент сокрытия следов преступной деятельности.

Поэтому особое значение приобретает разработка и совершенствование методик выявления и пресечения преступлений, связанных с незаконным оборотом культурных ценностей в сети Интернет. Для студентов и будущих специалистов важно понимать не только правовую основу борьбы с этим видом преступности, но и практические аспекты: какие следы оставляют злоумышленники, как использовать цифровые технологии для расследования, какие международные механизмы могут быть задействованы.

§ 1. Нормативно-правовое регулирование охраны культурных ценностей

1.1. Международное правовое регулирование охраны культурных ценностей

Понятие «культурные ценности» закреплено в ряде международных актов. Однако путь к выработке общепризнанного определения был достаточно длительным.

Изначально регулирование вопросов реституции похищенных произведений искусства развивалось в рамках **права войны**. Начиная с конца XIX в. международное право предпринимало попытки выработать правила возврата культурных ценностей

после военных конфликтов. Так, в **Гаагских положениях 1899 и 1907 г.**, **Гаагской конвенции 1907 г.**, а также в «**Пакте Рериха**» 1935 г. акцентировалось внимание на защите культурных объектов в условиях войны, что отражало доминирование военно-правового подхода.

Впервые на международном уровне понятие «культурные ценности» было закреплено в **Гаагской конвенции 1954 г. о защите культурных ценностей в случае вооруженного конфликта**. Согласно ст. 1 Конвенции, к культурным ценностям относятся:

– движимые и недвижимые объекты, имеющие большое значение для культурного наследия народов (памятники, произведения искусства, рукописи и др.);

– здания, предназначенные для хранения культурных ценностей (музеи, библиотеки, архивы);

– центры, содержащие значительное количество культурных ценностей.

Это определение, несмотря на критику за излишнюю широту, стало основой для дальнейшего развития международного регулирования в данной сфере.

Следующим шагом стало принятие в 1970 г. в Париже **Конвенции ЮНЕСКО «О мерах по запрещению и предотвращению незаконного вывоза, ввоза и передачи права собственности на культурные ценности»**. Документ впервые вынес вопросы охраны культурных ценностей за рамки военного права и заложил основы международного сотрудничества в борьбе с их незаконным оборотом.

В 1995 г. в Риме была подписана **Конвенция УНИДРУА «О похищенных или незаконно вывезенных культурных ценностях»**. Она уточнила критерии отнесения объектов к культурным ценностям, включив в их число предметы, име-

ющие значение для археологии, истории, искусства и науки. Конвенция вступила в силу в июле 1998 г. и действует для государств-участников.

Конвенция УНИДРУА рекомендует относить к культурным ценностям, в частности:

1) редкие коллекции и образцы фауны, флоры, минералов, анатомии, объекты палеонтологического интереса;

2) исторические ценности, включая историю наук и технологий, войн и социальной истории, а также жизнь национальных лидеров, мыслителей, ученых, художников и событий национального значения;

3) предметы археологических раскопок (официальных или нелегальных) и археологических открытий;

4) элементы памятников и археологических комплексов;

5) древности старше 100 лет (надписи, монеты, гравюры и др.);

6) объекты этнографического интереса;

7) произведения искусства (картины, скульптуры, оригинальные художественные изделия и конструкции из любых материалов);

8) редкие рукописи, старинные книги, документы и публикации специального характера;

9) почтовые, акцизные и аналогичные марки;

10) архивы (в том числе фото-, кино- и фонодокументы);

11) предметы мебели старше 100 лет, старинные музыкальные инструменты.

При этом окончательное определение категорий культурных ценностей отнесено к компетенции государств-участников, что сохраняет гибкость, но и создает риск правовой неопределенности.

В целом в международных актах понятие «культурные ценности» используется как собирательное. Главным критерием выступает **значимость объекта для наследия народов** – художественная, эстетическая, историческая или эмоциональная цен-

ность. Вопрос разграничения терминов «культурное наследие» и «культурные ценности» остается условным: если наследие охватывает и материальные, и нематериальные формы (языки, традиции, фольклор), то ценности часто имеют оборотоспособный характер и вовлекаются в гражданский оборот.

Эта идея получила развитие в **Конвенции ЮНЕСКО об охране нематериального культурного наследия 2003 г.**, которая впервые сконцентрировала внимание на нематериальных формах культуры:

– устные традиции и выражения, включая язык;
– исполнительские искусства;
– обычаи, обряды и праздники;
– знания и практики, связанные с природой и вселенной;
– традиционные ремесла.

Основная цель документа – защита нематериального культурного наследия и развитие международного сотрудничества в этой сфере. В условиях цифровизации Конвенция приобретает особую значимость: технологии позволяют сохранять традиции, но одновременно создают новые угрозы, например незаконное использование цифровых копий культурных объектов.

Таким образом, международное регулирование постепенно эволюционировало от защиты культурных ценностей в условиях войны к комплексной охране как материального, так и нематериального культурного наследия.

1.2. Российское законодательство в области охраны культурных ценностей

В российском законодательстве понятие «культурные ценности» закреплено в **Основах законодательства Российской Федерации о культуре** (утв. ВС РФ 09.10.1992 № 3612-1; ред.

от 24.06.2025, с изм., вступ. в силу с 01.09.2025) . В соответствии со ст. 3 Основ культурные ценности охватывают как **материальные объекты** (произведения искусства, здания, памятники, территории), так и **нематериальные формы** (традиции, языки, фольклор, знания). Такое понимание соотносится с международным подходом и подчеркивает интеграцию России в глобальную систему охраны культурного наследия.

Закон также оперирует понятием **культурного наследия** как совокупности материальных и духовных ценностей, созданных в прошлом, а также памятников и историко-культурных территорий, и объектов, значимых для сохранения и развития самобытности Российской Федерации и всех ее народов и их вклада в мировую цивилизацию. При этом законодатель устанавливает **общие рамки**, не детализируя критерии значимости. Конкретизация и отбор объектов отнесены к компетенции исполнительной власти, действующей на основании **экспертных заключений**, а при необходимости – на базе судебных решений. Это порождает элемент **правовой неопределенности** на уровне практического применения.

Специальный перечень категорий, относимых к культурным ценностям, приведен в **Законе Российской Федерации от 15 апреля 1993 г. № 4804-1 «О вывозе и ввозе культурных ценностей»** (ред. от 24.07.2023). Согласно ст. 7 к культурным ценностям относятся, в частности:

– редкие рукописи и документальные памятники;

– архивы, включая фото-, фоно-, кино- и видеоархивы;

– уникальные музыкальные инструменты;

– почтовые марки и иные филателистические материалы;

– старинные монеты, ордена, медали;

– редкие коллекции флоры и фауны;

– предметы, представляющие интерес для науки (минералогия, анатомия, палеонтология).

Уголовный кодекс Российской Федерации (ст. 164) предусматривает ответственность за **хищение предметов, имеющих особую ценность**, в качестве специального состава преступления. В судебной практике подчеркивается, что «особая историческая, научная, художественная или культурная ценность» похищенных предметов **устанавливается исключительно на основании экспертизы**; соответствующая позиция отражена в разъяснениях Пленума Верховного Суда Российской Федерации.

Критерии и порядок подтверждения статуса ценности конкретного объекта регламентированы **постановлением Правительства Российской Федерации от 14 сентября 2020 г. № 1425 «Об утверждении Правил проведения экспертизы культурных ценностей, а также критериев отнесения движимых предметов к культурным ценностям…»** (ред. от 06.11.2024). Правила устанавливают признаки (давность изготовления, уникальность, историческая значимость и др.), процедуру экспертизы (по заявлению собственника/организации или по обращению правоохранительных органов / Минкультуры России), а также основания для отнесения к «предметам, имеющим особое историческое, художественное, научное или культурное значение».

В условиях **цифровизации и глобализации**, когда сеть Интернет стала одним из ключевых каналов незаконного оборота культурных ценностей, национальная система нуждается в **актуализации процедур и инструментов учета** (в том числе внедрение защищенных реестров, цифровой маркировки, отслеживаемости). Одновременно возникают риски **незаконного использования цифровых копий** объектов культуры.

Показателен практический пример: в июле 2006 г. при внутренней проверке в Государственном Эрмитаже (г. Санкт-Петербург) выявлено хищение 221 экспоната Русского отдела (в основном эмали XV–XIX вв.) на сумму свыше 5 млн долл.; по материа-

лам оперативно-разыскных мероприятий было установлено, что 77 предметов (около 0,5 млн долл.) сданы в ломбарды и скупки, из них возвращены 35, а судьба остальных до настоящего времени остается неустановленной. Этот кейс демонстрирует важность **инвентаризации, экспертизы, межведомственного обмена данными** и быстрого реагирования.

В целом российская правовая система в сфере охраны культурных ценностей развивается в русле международных стандартов. Проблемными остаются:

– **правовая неопределенность** критериев значимости и особой ценности на уровне практики (решается через экспертизу и ведомственные перечни);

– **адаптация** институтов к цифровым вызовам (цифровые копии, онлайн-оборот, трансграничные сделки). При этом действующая нормативная база обеспечивает юридические инструменты для пресечения незаконного оборота и возврата объектов при надлежащем процессуальном оформлении запросов и экспертиз.

Актуальность НПА

Основы законодательства Российской Федерации о культуре № 3612-1 действуют; последняя редакция – **24 июня 2025 г.** (вступает в силу с 01.09.2025). Источник: СПС «КонсультантПлюс»; Официальный интернет-портал правовой информации.

Закон Российской Федерации от 15 апреля 1993 г. № 4804-1 «О вывозе и ввозе культурных ценностей» действует; изменения от **24 июля 2023 г. № 327-ФЗ** учтены. Источники: «Контур.Норматив»; Право.gov.ru; «Альта-Софт»; Контур.НормативАльта-Софтpravo.gov.ruКНТД.

УК РФ, ст. 164 «Хищение предметов, имеющих особую ценность» действует (с учетом ред. 2003–2011 гг.), санкции актуальны. Источники: СПС «КонсультантПлюс»; НПП «Гарант-сервис».

Постановление Правительства Российской Федерации от 14.09.2020 № 1425 (Правила экспертизы культурных ценностей) действует; актуальная редакция **от 06.11.2024**. Источники: СПС «КонсультантПлюс»; Government.ru; Гарант/Альта. КонсультантПлюсПравительствоРоссииКНТДАльта-Софт.

Позиция Пленума ВС РФ об обязательности экспертизы «особой ценности»: см. разъяснения и практические обзоры (в том числе по постановлению Пленума от **25** апреля **1995 г. № 5**). Источники: СПС «КонсультантПлюс»; аналитические обзоры.

1.3. Правовые механизмы, регламентирующие понятие культурных ценностей в сети Интернет

Интернет как важнейший атрибут современного информационного общества радикально изменил все сферы человеческой жизни: образование, труд, досуг, культурное потребление. Он открыл новые возможности для культурного обмена и творчества, породил сетевую литературу, цифровое искусство, виртуальные музеи и библиотеки. Пользователи получили доступ к культурным ценностям, ранее ограниченным географическими, политическими или экономическими барьерами. Более того, Интернет позволяет самим пользователям участвовать в **создании новых культурных ценностей**.

Наряду с позитивным влиянием сеть стала и каналом распространения деструктивного контента – пропаганды насилия, экстремизма, наркотиков и порнографии. Интернет также используется для незаконного оборота культурных ценностей. В этих условиях необходима **системная государственная стратегия**, объединяющая правовые, организационные, технические, педагогические и социокультурные меры защиты.

Подходы к регулированию Интернета в мировой практике

В научной и правоприменительной практике выделяют три основные модели регулирования:

1. **Стратегия открытости доступа** – минимальное вмешательство государства, упование на саморегуляцию. Пример: либеральная модель США и стран Западной Европы. В России 1990-х гг. попытка подобного подхода привела к негативным последствиям: информационной войне, девальвации традиционных ценностей и росту агрессии.

2. **Стратегия запретов** – жесткая фильтрация и цензура. Характерна для КНР (система «Великий китайский файрвол»), КНДР (отсутствие глобального Интернета), Ирана. Недостаток – ограничение свободы информации и прав граждан.

3. **Комбинированная стратегия** – баланс свободы доступа и правового регулирования. Эта модель реализуется в России: Конституция Российской Федерации гарантирует право на поиск и распространение информации, но государство ограничивает доступ к экстремистскому и вредоносному контенту.

Нормативные правовые акты России

Основу регулирования Интернета составляют федеральные законы от:

– **7 июля 2003 г. № 126-ФЗ «О связи»** (ред. 2024) определяет деятельность операторов связи, включая обеспечение устойчивости и безопасности сетей.

– **27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»** (ред. 2025) – ключевой акт: регулирует оборот информации, вводит блокировку экстремистского и противоправного контента, предусматривает ответственность владельцев ресурсов.

– **29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»** (ред. 2024) закрепляет возрастную маркировку и ограничения доступа к вредным материалам.

– **28 июля 2012 г. № 139-ФЗ «О внесении изменений…»** – учредил **Единый реестр запрещенных сайтов**.

– **2 июля 2013 г. № 187-ФЗ** – защита авторских прав в Интернете (антипиратский закон).

– **5 мая 2014 г. № 97-ФЗ** (закон о блогерах) обязывает популярных авторов (>3000 читателей) соблюдать нормы, аналогичные СМИ.

– **13 июля 2015 г. № 264-ФЗ** (право на забвение) предоставляет гражданам возможность требовать удаления недостоверной информации о себе.

– **6 июля 2016 г. № 374-ФЗ и № 375-ФЗ** (пакет Яровой) регламентируют хранение данных операторов и их передачу органам безопасности.

– **1 мая 2019 г. № 90-ФЗ** (о надежном Рунете) обеспечивает автономность российского сегмента Интернета, включая централизованное управление трафиком и установку технических средств противодействия угрозам.

Эти акты действуют и регулярно актуализируются. Например, в 2022–2024 гг. были внесены изменения, усилившие требования к обработке персональных данных и трансграничной передаче трафика.

Международные примеры

– **США**: Закон COPPA (Children's Online Privacy Protection Act, 1998, ред. 2013) защищает персональные данные детей; DMCA (1998) регулирует защиту авторских прав в цифровой среде.

– **ЕС**: GDPR (2016, применяется с 2018 г.) – единый стандарт защиты персональных данных; директивы о защите авторских прав и борьбе с киберпреступностью.

– **Китай**: система «Великий китайский файрвол» (с 1998 г.) блокирует сайты по ключевым словам и IP-адресам, развивается национальная экосистема цифровых сервисов.

Регулирование Интернета в России развивается по **комбинированной модели**: обеспечивается баланс между свободой доступа и защитой общества от деструктивного контента, при этом уделяется внимание устойчивости и безопасности Рунета. Одновременно актуализируются вопросы защиты культурных ценностей в цифровой среде:

– незаконный оборот объектов искусства;

– цифровое пиратство;

– утечка и подмена цифровых копий.

Для ответа на эти вызовы требуется постоянное совершенствование законодательства и внедрение современных технологий (блокчейн-реестры, цифровая маркировка, искусственный интеллект для мониторинга нарушений).

§ 2. Оборот культурных ценностей в сети Интернет

Цифровые технологии кардинально изменили мир искусства, предоставив художникам и творцам новые инструменты и платформы для самовыражения. Они упростили процесс создания и распространения произведений и сделали искусство более доступным для широкой аудитории, открыв перед авторами новые горизонты и изменив способы создания, распространения и восприятия.

Современные произведения искусства все чаще вовлекают зрителя в процесс восприятия: инсталляции с использованием виртуальной реальности позволяют зрителю стать частью про-

изведения (интерактивное искусство). В среде VR художники создают трехмерные миры, которые можно исследовать, либо дополняют реальный мир цифровыми элементами (AR).

С помощью графических планшетов и специализированного ПО художники свободно экспериментируют со стилями и техниками. Развитие интернета и социальных медиа дало возможность представлять произведения онлайн миллионам людей по всему миру: виртуальные выставки позволяют изучать коллекции, не покидая дома, а профессиональные и любительские платформы помогают находить аудиторию и получать обратную связь.

Сегодня существует множество авторов и проектов, использующих цифровые медиа, например турецкий художник и дизайнер Рефик Анадол, американский художник Кейси Риас, проект Google Arts & Culture, предоставляющий доступ к коллекциям музеев и использующий алгоритмы ИИ для новых художественных интерпретаций.

Цифровые медиа глубоко воздействуют на социокультурную сферу как в мировом масштабе, так и в каждой отдельной стране, в том числе в России. С одной стороны, они делают культурный обмен более доступным и интенсивным, поддерживают культурное разнообразие. С другой стороны, глобальные тренды способны сглаживать различия и унифицировать культурную повестку.

В то же время международное сообщество признает, что незаконная торговля культурными ценностями через Интернет – серьезная и растущая проблема. Она затрагивает как страны происхождения похищенных ценностей, так и государства импорта. В сети продаются самые разные предметы: от подлинных объектов с исторической, художественной или культурной ценностью до подделок и вещей сомнительного происхождения.

Правоохранительные органы России взаимодействуют с Интерполом, Международным советом музеев (ИКОМ) и ЮНЕСКО.

Интерпол играет ключевую роль в обмене информацией между странами: ведет базу данных похищенных культурных ценностей, анализирует тенденции, публикует регулярные подборки разыскиваемых предметов, координирует проверки на границах, в музеях и аукционных домах.

ИКОМ содействует реституции ценностей в страны происхождения: выступает медиатором, помогает заключать двусторонние соглашения, работает в консультационной связке с ЮНЕСКО.

На совещаниях экспертов Интерпола отмечаются проблемы мониторинга интернета: огромный объем лотов, множество платформ в разных странах, отсутствие единого банка данных, высокая скорость онлайн-торгов, транснациональный характер сделок.

Для борьбы с этими вызовами Интерпол и ЮНЕСКО предложили меры предупреждения покупателей о необходимости проверки происхождения предметов, обязанность платформ сообщать о подозрительных сделках, создание международной базы данных и реестра экспертов, обмен информацией между странами, конфискация и возврат законному владельцу.

Эффективной формой взаимодействия является ежегодная операция Pandora, координируемая Интерполом, Европолом и Всемирной таможенной организацией. Так, в ходе этапа 2021 г. были задержаны 52 человека и конфисковано около 9,4 тыс. предметов. С 2016 г. Pandora привела к задержанию более 400 лиц и изъятию свыше 147 тыс. культурных и археологических объектов.

Киберпреступления, создающие угрозу арт-рынку и культурным ценностям, включают: мошенничество (ст. 159 УК РФ), нарушение авторских прав (ст. 146 УК РФ), финансирование терроризма (ст. 205.1 УК РФ), легализацию преступных доходов (ст. ст. 174, 174.1 УК РФ), сбыт имущества, добытого преступным путем (ст. 175 УК РФ), незаконные раскопки и сбыт археологических предметов (ст. 243.2 УК РФ), незаконный оборот порно-

графической продукции (ст.ст. 242, 242.1, 242.2 УК РФ), а также иные преступления (ст.ст. 324, 148, 282 УК РФ).

Таким образом, оборот культурных ценностей в сети требует комплексного подхода, сочетающего открытость доступа с эффективными мерами предотвращения и пресечения правонарушений.

Таблица 5

Основные виды киберпреступлений, связанных с культурными ценностями

Вид киберпреступления	Статья УК РФ	Пример/содержание
Мошенничество	159	Онлайн-аукционы с поддельными работами, ложные атрибуции
Нарушение авторских прав	146	Распространение цифровых копий произведений искусства
Финансирование терроризма	205.1	Продажа культурных ценностей террористами
Легализация доходов	174, 174.1	Отмывание денег через арт-рынок
Скупка краденого	17	Продажа археологических предметов в интернете
Незаконные раскопки	243.2	Сбыт предметов, добытых «черными археологами»
Порнографическая продукция	242, 242.1, 242.2	Интернет-оборот порнографических материалов под видом искусства
Иные составы	324, 148, 282	Незаконный оборот наград, оскорбление религиозных чувств, экстремистские материалы

§ 3. Методика выявления и пресечения преступлений, связанных с незаконным оборотом культурных ценностей в сети Интернет

3.1. Принципы и правовая основа

Цель: обеспечить законное, доказательное и оперативное противодействие онлайн-обороту культурных ценностей (КЦ).

Ключевые НПА РФ: Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»; Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Закон Российской Федерации от 15 апреля 1993 г. № 4804-1 «О вывозе и ввозе культурных ценностей» (ред. с 01.01.2024); Федеральный закон от 25 июня 2002 г. № 73-ФЗ «Об объектах культурного наследия»; постановление Правительства Российской Федерации от 14 сентября 2020 г. № 1425 (Правила экспертизы КЦ).

Международные механизмы: НЦБ Интерпола МВД России, база Stolen Works of Art, мобильное приложение ID-Art, инструменты Европола и Всемирной таможенной организации.

3.2. Этап 0 – подготовка расследования

1. Определение процессуального режима (ОРД или следствие по УПК).

2. Назначение ответственных: оперуполномоченный, аналитик ОСИНТ, эксперт-искусствовед, IT-криминалист, представитель Минкультуры России, контакт в ФТС России.

3. Планирование тактики: перечень запросов и список онлайн-платформ для мониторинга.

4. Соблюдение ограничений: тайна следствия, персональные данные, пропорциональность мер.

3.3. Этап 1 – источники и сбор информации

ГИАЦ МВД России ведет учет похищенных КЦ; Минкультуры России и музеи предоставляют описи фондов.

INTERPOL Stolen Works of Art Database (~57 000 объектов) и приложение ID-Art используются для международных проверок.

Europol/BTO проводят операции Pandora по пресечению контрабанды КЦ.

OSINT: мониторинг аукционов, соцсетей, форумов, блогов, даркнета. Использование стандарта Object ID для описания объектов.

3.4. Этап 2 – мониторинг и аналитика

Карта площадок: открытые, полузакрытые, даркнет.

Инструменты: фиксация веб-страниц (Hunchly), анализ связей (Maltego), поиск по изображению, ID-Art.

Алгоритм подозрительного объявления: нет провенанса (от англ. *provenance* – происхождение; **история владения и перемещений культурной ценности** (картины, скульптуры, артефакта и т. д.) от момента ее создания до настоящего времени), цена занижена, совпадение с ориентировкой, новые аккаунты, криптоплатежи, подозрительные геометки.

3.5. Этап 3 – сохранение цифровых доказательств

Фиксация: скриншоты, HTML-дамп, хеш-суммы.

Привязка ко времени: отметки, нотариальный осмотр сайта.

Цепочка сохранности: журнал действий, контрольные хеши.

Приоритет: сторис и быстро исчезающие лоты.

3.6. Этап 4 – экспертиза и правовая квалификация

Экспертиза по постановлению Правительства Российской Федерации № 1425.

Особая ценность для ст. 164 УК РФ подтверждается экспертизой.

Квалификация: ст. 243.2 УК РФ (незаконные раскопки), ст. 226.1 УК РФ (контрабанда), совокупность со ст.ст. 146, 159, 174, 174.1, 175, 205.1, 242–242.2, 272–273 УК РФ.

3.7. Этап 5 – запросы данных и международное взаимодействие

Внутригосударственные запросы: владельцам платформ и операторам связи.

Международные запросы: через НЦБ Интерпола (Инструкция от 6 октября 2006 г. № 786/310/470/454/333/971).

Структура запроса: адресат, основание, фабула, данные, сроки, контакт, приложения (Object ID).

3.8. Этап 6 – оперативные комбинации и изъятие

Контрольная закупка: фиксация передачи (видео, аудио, метки, хеши).

Изъятие/обыск: ИТ-криминалистика, изъятие предметов с защитой от повреждений.

Таможенный контроль: профили «КЦ-риск», декларации по Закону № 4804-1.

3.9. Этап 7 – возврат и реституция

Подтверждение провенанса через музейные акты и экспертизу.

Координация с Интерполом / иностранными органами.

Практика операций Pandora (совместные группы быстрого реагирования).

3.10. Профилактика и общественное взаимодействие

Обучение сотрудников работе с ID-Art.

Горячие линии и прием сообщений граждан.

Рекомендации рынку: проверка провенанса, использование Object ID, сохранение логов.

3.11. Практические алгоритмы

1. Археология онлайн. Монеты → обратный поиск фото → запрос → контрольная закупка → изъятие → ст. 243.2/175 УК РФ.

2. Икона на зарубежном аукционе. Карточка Object ID → запрос в Интерпол → совпадение с базой → арест лота → реституция.

3. Массовый онлайн-сбыт. Мониторинг каналов → граф связей → выявление «узлов» → одновременные обыски → совокупность статей.

Таблица 6

Сценарии преступлений и статьи УК РФ

Сценарий	Статья УК РФ	Описание
Продажа похищенной иконы через маркетплейс	175, 164	Сбыт заведомо похищенного имущества + хищение культурных ценностей
Онлайн-сбыт археологических предметов	243.2, 175	Незаконные раскопки и сбыт археологических ценностей
Отмывание доходов через онлайн-аукцион	174, 174.1	Легализация преступных доходов
Цифровое пиратство изображений	146	Нарушение авторских прав
Финансирование терроризма через продажу артефактов	205.1	Финансирование террористической деятельности

Учебно-методический раздел к главе 7

Цели изучения темы

1. Изучить международные и российские правовые основы регулирования охраны культурных ценностей.

2. Освоить стратегии регулирования доступа к Интернету и их значение для защиты культурного наследия.

3. Понять влияние цифровых технологий на оборот культурных ценностей, включая новые возможности и угрозы.

4. Научиться анализировать меры, принимаемые Россией и международным сообществом, для борьбы с незаконным оборотом.

5. Освоить современные технологии учета, идентификации и защиты культурных ценностей.

6. Развить навыки критического анализа правоприменительной практики и кейсов международного сотрудничества.

7. Сформировать умение вырабатывать предложения по совершенствованию методик расследования и профилактики.

Вопросы для семинарского занятия

Теоретические вопросы

1. Какие международные конвенции регулируют охрану культурных ценностей? В чем их основные различия?

2. Как определяется понятие «культурные ценности» в российском законодательстве? Какие критерии используются для их идентификации?

3. Какие стратегии регулирования доступа к Интернету существуют в мировой практике? Какая из них, на ваш взгляд, наиболее эффективна и почему?

4. Как цифровые технологии влияют на оборот культурных ценностей? Какие новые возможности и риски они создают?

5. Какие меры принимаются в России для борьбы с незаконным оборотом культурных ценностей через Интернет? Приведите примеры из практики.

6. Какую роль играет международное сотрудничество в борьбе с незаконным оборотом культурных ценностей? Приведите примеры успешных операций (например, операция **Pandora**).

7. Какие современные технологии используются для учета и защиты культурных ценностей? Как они помогают в борьбе с незаконным оборотом?

8. Какие виды киберпреступлений связаны с культурными ценностями? Какие статьи УК РФ применяются для их пресечения?

9. Какие вызовы возникают при регулировании оборота культурных ценностей в условиях цифровизации? Как их можно преодолеть?

10. Какие проблемы возникают при международном розыске культурных ценностей? Как их можно решить?

11. Как общественность может участвовать в борьбе с незаконным оборотом культурных ценностей? Какие инструменты для этого существуют?

Практические задания

1. **Анализ ситуации**: рассмотреть случай возвращения иконы «Спас Вседержитель» или операцию **Pandora**.

Задание: определить меры выявления и пресечения, предложить улучшения.

Групповая стратегия: разделение студентов на команды для разработки стратегии борьбы с незаконным оборотом КЦ в Интернете.

Задание: включить технологии, международное сотрудничество, участие общественности.

2. **Юридический анализ**: работа с УК РФ (например, ст.ст. 159, 164, 205[1]).

Задание: выявить составы преступлений, предложить профилактические меры.

3. **Проектирование базы данных**: создать модель электронной БД для учета КЦ.

Задание: описать структуру, критерии включения объектов, взаимодействие с правоохранительными органами.

Иные формы обучения

– **Мозговой штурм**. Как предотвратить незаконный оборот КЦ в Интернете?

– **Деловая игра**. Роли правоохранителей, таможни, Минкультуры и международных организаций.

– **Ролевая игра**. Симуляция аукциона с выявлением подозрительных сделок.

– **Круглый стол** «Цифровизация и культурное наследие: новые вызовы и возможности».

– **Экспертная дискуссия**. Приглашение специалистов МВД, ФТС, Минкультуры, музейных работников.

– **Решение кейса** «Как вернуть похищенную картину, выставленную на зарубежном аукционе?»

– **Проектная работа**. Разработка системы защиты КЦ в Интернете (анализ проблем, использование технологий – блокчейн, RFID, план межведомственного взаимодействия, вовлечение общества).

Библиографический список к главе 7

Нормативные акты

1. Постановление Пленума Верховного Суда Российской Федерации от 26 апреля 2007 г. № 14 «О практике рассмотрения уголовных дел о хищениях, вымогательстве и незаконном обороте оружия, боеприпасов, взрывчатых веществ и взрывных устройств» // Бюллетень Верховного Суда Российской Федерации. – 2007. – № 7.

Монографии, книги

2. Нешатаева, В. О. Культурные ценности: цена и право / В. О. Нешатаева. – М. : Высшая школа экономики, 2013.

3. Приданов, С. А. Преступления, посягающие на культурные ценности России: квалификация и расследование / С. А. Приданов, С. П. Щерба. – М. : Юрлитинформ, 2002.

Статьи и материалы конференций

4. Белов, В. А. Объект субъективного гражданского права / В. А. Белов // Объекты гражданского оборота. – М. : Юрайт, 2007. – С. 6–77.

5. Алимпиев, Д. С. Особенности расследования преступлений, связанных с незаконным оборотом культурных ценностей в сети Интернет / Д. С. Алимпиев // Вестник криминалистики. – 2023. – № 2. – С. 45–52.

6. Арский, А. А. Информационно-технические аспекты профилактики контрабанды культурных ценностей / А. А. Арский // Маркетинг и логистика. – 2017. – № 4 (12). – С. 5–10.

7. Балашова, К. С. Оценка состояния международного таможенного сотрудничества в России и перспективы его развития / К. С. Балашова, Р. Р. Ахмедзянов // Modern Economy Success. – 2020. – № 3. – С. 86–90.

8. Басалаев, А. Н. Противодействие незаконному обороту культурных ценностей в цифровом пространстве: организационно-правовые аспекты / А. Н. Басалаев // Закон и право. – 2023. – № 5. – С. 21–28.

9. Васильева, А. А. Цифровые следы как источник информации при расследовании преступлений / А. А. Васильева // Информационное общество. – 2023. – № 3. – С. 55–61.

10. Гончарова, А. В. Сравнительный анализ объектов гражданских прав и объектов гражданских правоотношений / А. В. Гончарова // Вестник Волгоградского государственного университета. Серия 5: Юриспруденция. – 2016. – № 4 (33). – С. 18–24.

11. Калинченко, Ю. П. Объект гражданского оборота в Российской Федерации: состояние теории и законодательства / Ю. П. Калинченко // Вестник Московского университета МВД России. – 2018. – № 1. – С. 92–99.

12. Медведева, Н. В. Понятие «культурное наследие» и его правовое значение / Н. В. Медведева, А. С. Стоналова // Материалы Афанасьевских чтений. – 2016. – № 3 (16). – С. 34–39.

13. Русанов, Г. А. Понятие культурных ценностей и критерии их отнесения к объектам охраны / Г. А. Русанов // Российская юстиция. – 2008. – № 4. – С. 18–23.

14. Тришкин, А. С. Безопасность наследия предков / А. С. Тришкин // Полиция России. – 2018. – № 9. – С. 42–47.

Электронные ресурсы и СМИ

15. Хакеры поставили на «Игру престолов» // Коммерсант. 2017. 9 авг. – URL: https://www.kommersant.ru/doc/3387920 (дата обращения: 04.09.2025).

Аналитические обзоры

16. Особенности выявления и пресечения незаконного оборота культурных ценностей в сети Интернет: информационно-аналитический обзор / под ред. В. В. Бычкова. – М. : ГИАЦ МВД России, 2023.

Глава 8. МЕТОДИКА ВЫЯВЛЕНИЯ МЕДИЙНЫХ ИСТОЧНИКОВ, РАСПРОСТРАНЯЮЩИХ ЛОЖНУЮ ИНФОРМАЦИЮ В СЕТИ ИНТЕРНЕТ

ВВЕДЕНИЕ

В современном мире, где информационные технологии развиваются с невероятной скоростью, проблема распространения ложной информации приобретает особую актуальность. Для специалистов в области анализа и защиты информации, в том числе для сотрудников Министерства внутренних дел Российской Федерации, умение **выявлять, анализировать и нейтрализовать недостоверные сведения** становится не только профессиональным навыком, но и одним из ключевых элементов обеспечения информационной безопасности государства и общества.

Медийные источники выполняют двойственную функцию. С одной стороны, они являются важнейшими каналами информирования населения, обеспечивают доступ к актуальным данным, формируют повестку дня. С другой стороны, именно эти источники могут использоваться для **манипуляции общественным мнением, распространения дезинформации и даже координации противоправных действий**.

Сегодня ложная информация способна:

– стать инструментом политического и психологического давления;

– провоцировать массовые беспорядки и социальную напряженность;

– подрывать доверие к государственным институтам;

– использоваться в преступных целях, включая киберпреступность и экстремизм.

В условиях цифровизации необходимо четко понимать:

1. **Природу медийных источников** – их типологию и особенности функционирования.

2. **Методы распространения дезинформации** – от фейковых новостных сайтов и ботоферм до целевых атак в социальных сетях.

3. **Инструменты верификации информации** – фактчекинг, цифровая криминалистика, OSINT (Open Source Intelligence).

4. **Методы противодействия** – организационные, правовые, технические и образовательные меры.

Разработка эффективных методик выявления и пресечения деятельности источников, распространяющих ложную информацию, становится одной из приоритетных задач как для МВД России, так и для международного сообщества.

Эта работа требует комплексного подхода, включающего:

– **правовое регулирование** (Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» и др.);

– **межведомственное взаимодействие** (МВД, ФСБ, Роскомнадзор, прокуратура, суды);

– **технические средства мониторинга** (системы анализа соцсетей, автоматические фильтры, нейросетевые алгоритмы);

– **вовлечение общества** (сотрудничество с НКО, независимыми фактчекерами, образовательные программы по медиаграмотности).

Таким образом, изучение методики выявления медийных источников, распространяющих ложную информацию, имеет не только теоретическое, но и важное прикладное значение: оно помогает формировать у специалистов аналитическое мышле-

ние, умение работать с большими данными и эффективно противостоять современным вызовам информационной безопасности.

§ 1. Источники информации и медийные источники: классификация, свойства и роль в распространении ложной информации

1.1. Понятие «источник информации»

В современном информационном пространстве понятие **«источник информации»** является фундаментальным как для анализа данных, так и для проверки их достоверности и предотвращения распространения ложных сведений.

Под источником информации понимается субъект (человек, организация) или объект (документ, база данных, техническое устройство), из которых поступают сведения, факты, мнения или комментарии. Эти источники служат основой для формирования информационных материалов, принятия решений и проведения аналитических исследований.

Для специалистов в области анализа и защиты информации в частности для сотрудников **Министерства внутренних дел Российской Федерации**, понимание природы источников имеет особое значение. В их профессиональной деятельности источники информации применяются:

– для **сбора оперативных данных**;

– при **проведении расследований**;

– в рамках **мониторинга информационного пространства**, направленного на выявление и нейтрализацию угроз, связанных с распространением дезинформации.

В практике можно выделить несколько основных видов источников информации:

1. **Люди** – очевидцы преступлений, эксперты, информаторы. Их показания могут содержать ценную информацию, однако требуют тщательной проверки на предмет достоверности.

2. **Документы** – официальные отчеты, протоколы, базы данных. Они служат базой для аналитической работы, но могут быть сфальсифицированы или содержать ошибки.

3. **Технические средства** – видеокамеры наблюдения, аудиозаписи, данные с мобильных устройств. Обычно обеспечивают объективность, но возможны технические сбои или умышленное искажение данных.

4. **Интернет-ресурсы** – социальные сети, мессенджеры, блоги, форумы. С одной стороны, они дают быстрый доступ к актуальной информации, с другой – часто становятся каналами распространения ложных данных.

Таким образом, **любой источник информации может содержать искажения или подделку**. Поэтому в работе оперативного сотрудника крайне важна процедура проверки, включающая:

– **верификацию данных** – установление их соответствия фактам, выявление ошибок и противоречий;

– **перекрестную проверку** – сопоставление сведений из нескольких независимых источников;

– **соблюдение законности** при сборе и использовании информации, особенно при обращении к закрытым или конфиденциальным данным.

1.2. Классификация источников информации

Источники информации могут быть классифицированы по различным критериям, что позволяет систематизировать подход к их анализу и оценке достоверности. Рассмотрим основные классификации.

По характеру информации

– **Прямые** – предоставляют сведения из первых рук (очевидцы событий, участники инцидентов, официальные лица). Ценны своей непосредственностью, однако требуют проверки на предмет субъективности и возможного искажения фактов.

– **Косвенные** – передают информацию, полученную от других источников (СМИ, аналитические отчеты, пересказы событий). Они позволяют получить общую картину, но их надежность зависит от достоверности первоисточника.

По степени официальности

– **Официальные** – исходят от государственных органов, правоохранительных структур, международных организаций или корпораций (пресс-релизы, официальные заявления, отчеты). Обычно обладают высоким уровнем доверия, но могут содержать элементы политической или корпоративной ангажированности.

– **Неофициальные** – не связаны с официальными структурами (анонимные информаторы, блоги, социальные сети). Они нередко содержат уникальные сведения, но требуют особенно тщательной проверки.

По доступности информации

– **Открытые** – общедоступные источники (материалы СМИ, интернет-ресурсы, публичные базы данных). Широко применяются в аналитической работе, но данные могут быть неполными или устаревшими.

– **Закрытые** – доступ к ним ограничен (конфиденциальные документы, оперативные данные, персональные интервью). Содержат ценную информацию, однако их использование требует соблюдения правовых и этических норм.

По уровню достоверности

– **Первичные** – предоставляют сведения напрямую, без промежуточных звеньев (протоколы допросов, видеозаписи, оригинальные документы). Считаются наиболее надежными, но также могут содержать ошибки или быть сфальсифицированными.

– **Вторичные** – интерпретируют или перерабатывают данные из первичных источников (новостные статьи, аналитические обзоры, отчеты). Полезны для обобщения информации, но их достоверность зависит от качества анализа и добросовестности авторов.

Таблица 7

Сравнительная характеристика источников информации

Тип источника	Описание	Примеры
Прямые источники	Сведения из первых рук, от самого события или его участника	Свидетель, участник события, официальное заявление
Косвенные источники	Передают информацию, полученную от других источников	СМИ, эксперт, исследовательский отчет
Официальные источники	Представляют государственные органы или организации	Правительственный представитель, пресс-служба
Неофициальные источники	Не связаны с официальными органами, но имеют сведения по теме	Анонимный источник, активист, НКО
Интернет-источники	Доступные через сеть Интернет	Веб-сайт, блог, социальные сети, онлайн-публикации

Свойства надежных источников информации

1. **Независимость** – отсутствие влияния со стороны сторонних лиц или организаций.

2. **Экспертность** – наличие специальных знаний и опыта в определенной области.

3. **Актуальность** – соответствие предоставленных данных современным событиям.

4. **Проверяемость** – возможность подтвердить сведения с помощью других независимых источников.

1.3. Роль медийных источников в распространении ложной информации

Медийные источники играют ключевую роль в современном информационном пространстве: именно через них формируется общественное мнение, задается повестка дня и распространяются как достоверные, так и ложные сведения. Их влияние особенно велико в условиях цифровизации, когда аудитория получает новости не только из традиционных СМИ, но и из онлайн-платформ.

1.4. Основные категории медийных источников

1. Традиционные СМИ

Печатные издания, телевидение, радио.

Отличаются относительно высоким уровнем редакционного контроля, но могут быть ангажированы политически или коммерчески.

В условиях конкуренции иногда допускают публикацию непроверенной информации для повышения рейтингов.

2. Интернет-СМИ и новостные сайты

Онлайн-издания, агрегаторы новостей.

Преимущество – оперативность. Недостаток – частая гонка за сенсацией, что приводит к тиражированию непроверенных фактов.

3. Социальные сети

«ВКонтакте», Telegram, **Facebook**, **X (бывший Twitter)**, **TikTok** и др.

Благодаря мгновенному распространению сообщений и алгоритмам персонализированной ленты становятся основным каналом дезинформации.

Используются для целевых атак: создания фейковых аккаунтов, ботоферм, распространения паники или манипуляции массовым сознанием.

4. Мессенджеры

WhatsApp, **Telegram**, **Signal**, **Viber**.

Обеспечивают закрытые каналы связи, что затрудняет контроль.

Часто используются для координации незаконной деятельности, в том числе распространения ложных слухов.

5. Форумы и блоги

Тематические сообщества, где информация может распространяться стихийно.

Проблема: отсутствие модерации, анонимность и субъективность участников.

6. Автоматизированные системы распространения контента

Ботофермы и сетевые тролли, создающие искусственный информационный поток.

Их задача – усилить эффект дезинформации, создавая иллюзию массовой поддержки или паники.

1.5. Механизмы распространения ложной информации

Вирусный эффект – благодаря лайкам, репостам и комментариям сообщение быстро набирает охват.

Алгоритмы рекомендаций – соцсети и поисковики подталкивают пользователя к просмотру схожего контента, усиливая эффект информационного пузыря.

Использование эмоций – ложные сообщения часто подаются в сенсационной форме, апеллируют к страху, гневу или любопытству.

Мультимедийные фейки – фото- и видеомонтаж, дипфейки, мемы, которые воспринимаются как более убедительные, чем текст.

Примеры влияния

1. Во время чрезвычайных ситуаций (пожары, эпидемии, военные конфликты) дезинформация в соцсетях приводит к панике, распространению слухов и массовым нарушениям порядка.

2. В политической сфере – использование сетевых ботоферм для дискредитации кандидатов или продвижения выгодных нарративов.

3. В экономике – вбросы о банкротстве банков или дефиците товаров провоцируют массовые действия населения.

Таким образом, медийные источники одновременно выступают инструментом **объективного информирования** и каналом **массового распространения дезинформации**. Это обусловливает необходимость разработки методик их постоянного мониторинга, проверки достоверности и контроля за цифровым контентом.

1.6. Виды и форматы медийных источников

1. Традиционные медиа (Mass Media)

Телевидение – сочетает визуальный и аудиальный каналы; обладает высокой силой воздействия.

Радио – оперативное средство информирования, доступное широким слоям населения.

Печатные издания – газеты, журналы, книги; обеспечивают глубину анализа, но уступают в скорости цифровым источникам.

2. Цифровые медиа

Интернет-СМИ (e-media) – новостные порталы и сетевые издания, включая онлайн-версии традиционных СМИ.

Социальные сети (*«ВКонтакте», Facebook, Instagram, X/ Twitter, TikTok*) – платформы для создания и обмена пользовательским контентом.

Блоги и микроблоги – персональные или корпоративные страницы (например, LiveJournal, телеграм-каналы).

Форумы и сообщества – площадки для дискуссий, часто становятся источником непроверенной информации.

Подкасты – аудиопередачи, публикуемые в интернете, альтернатива радио.

Мобильное телевидение – трансляция ТВ на смартфоны через сети 3G/4G/5G.

3. Мультимедиа

Форматы, сочетающие несколько каналов (текст, графика, аудио, видео). Используются для усиления воздействия на аудиторию.

4. Тактические медиа

Малозатратные и технологичные каналы, создаваемые для продвижения определенных идей или политических целей (например, протестные кампании).

5. Новые медиа (New Media)

Виртуальные сообщества и игры – сетевые миры, в которых пользователи взаимодействуют как в реальной среде:

– **Wikis** – коллективные проекты (например, *Wikipedia*), где информация обновляется и дополняется пользователями;

– **VR/AR-платформы** – виртуальная и дополненная реальность, где создаются новые формы культурного контента.

Ключевая особенность: чем новее формат, тем выше скорость распространения информации, но тем ниже степень контроля над ее достоверностью.

§ 2. Нормативные правовые документы, регламентирующие понятие «медийные источники»

В правовой системе России медийные источники информации регулируются целым рядом нормативных актов. Они определяют, что считается открытой информацией, какие ограничения существуют, а также каким образом государство должно обеспечивать гражданам доступ к сведениям.

Понимание правовой базы помогает правильно ориентироваться в информационном пространстве: что можно свободно использовать, а за что можно понести ответственность. Для сотрудников правоохранительных органов знание этих норм – не только теория, но и инструмент работы.

2.1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Это основной документ, задающий правила игры в информационной сфере. Он определяет понятие **открытых источников информации** (ст. 13). Если информация опубликована в Интернете без ограничений, она становится общедоступной. Простой пример: если муниципалитет разместил на своем сайте отчет о расходах бюджета, то любой гражданин имеет право его скачать и использовать, например, для общественного контроля.

2.2. Федеральный закон № 8-ФЗ «Об обеспечении доступа к информации о деятельности органов власти»

Этот закон конкретизирует, какие именно сведения органы власти обязаны публиковать, в какой форме и в какие сроки. Для будущих юристов и аналитиков это важный инструмент – именно на него можно ссылаться при запросе данных у чиновников.

2.3. Постановление Правительства Российской Федерации от 10 июля 2013 г. № 583

Устанавливает правила размещения информации госорганами в открытом доступе. Например, благодаря ему на сайтах министерств мы видим структурированные разделы с документами, статистикой и нормативными актами.

2.4. Приказ Минцифры России от 31 июля 2024 г. № 677

Совсем свежий документ: он утвердил технические и организационные требования к открытым данным. Это уже шаг в сторону цифровизации – теперь государственные органы обязаны публиковать данные в машиночитаемом формате, пригодном для анализа. Это особенно важно для борьбы с фейками: чем прозрачнее государственные данные, тем сложнее манипулировать обществом.

2.5. Закон о СМИ № 2124-1 от 27 декабря 1991 г. (ред. 2024 г.)

Классический закон, регулирующий деятельность средств массовой информации. Здесь закреплено право журналистов со-

бирать сведения, а также ответственность редакций за публикацию недостоверных данных. Например, именно по этому закону можно требовать опровержения, если в газете о вас написали ложь.

2.6. Другие важные федеральные законы

– **№ 98-ФЗ «О коммерческой тайне»** – устанавливает, где заканчивается открытый источник и начинается коммерческая тайна.

– **№ 125-ФЗ «Об архивном деле»** – регулирует доступ к архивам, что важно при исторических расследованиях.

– **№ 152-ФЗ «О персональных данных»** – ключевой закон, ограничивающий публикацию личной информации без согласия гражданина.

– **№ 38-ФЗ «О рекламе»** – регулирует коммуникацию в маркетинге, в том числе онлайн-рекламу.

– **№ 244-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»** – защищает несовершеннолетних от деструктивного контента, особенно в Интернете.

2.7. Международные соглашения

Россия также учитывает международные стандарты. Например, Международный пакт о гражданских и политических правах, Европейская конвенция по правам человека, Заключительный акт СБСЕ, Конвенция СНГ о правах человека.

Все они закрепляют право на свободу слова и доступ к информации, но одновременно подчеркивают: это право может быть ограничено, если затрагивает вопросы национальной безопасности или прав других граждан.

Таким образом, правовая база России в сфере медийных источников построена по принципу открытости с разумными ограничениями. С одной стороны, гражданин имеет право знать и использовать данные, опубликованные государством или СМИ, а с другой – законы защищают частную жизнь, государственные тайны и интересы общества.

Хотя национальное законодательство России (149-ФЗ, 2124-1 и др.) играет ключевую роль в регулировании медийных источников, оно тесно связано с международными обязательствами. Россия как участник ряда международных договоров обязана учитывать их при разработке и применении собственных правовых норм.

1. Международный пакт о гражданских и политических правах (1966 г., ратифицирован СССР в 1973 г.)

– **Статья 19** закрепляет право каждого человека на свободу выражения мнения и право искать, получать и распространять информацию любыми средствами.

Однако это право **может быть ограничено законом**, если речь идет о защите национальной безопасности, общественного порядка, здоровья или нравственности населения, уважении прав и репутации других лиц.

Для медийных источников это значит, что свобода прессы и Интернета не является абсолютной: она всегда уравновешивается обязанностью не причинять вреда.

2. Европейская конвенция о защите прав человека и основных свобод (1950 г.)

– **Статья 10** «Свобода выражения мнения» гарантирует каждому свободу получать и распространять информацию без вмешательства государственных органов.

– Ограничения допускаются лишь в строго определенных случаях: ради национальной безопасности, территориальной целостности, общественного порядка, предотвращения беспорядков или преступлений.

Эта норма активно используется в Европейском суде по правам человека (ЕСПЧ), который рассматривает жалобы на чрезмерные ограничения свободы слова и СМИ.

3. Заключительный акт Совещания по безопасности и сотрудничеству в Европе (Хельсинки, 1975 г.)

– Впервые закрепил взаимосвязь между безопасностью и правами человека, включая свободу информации.

– Государства обязались **обеспечивать более широкий доступ к информации**, включая обмен печатными материалами, трансляциями и культурными программами.

Для современного медийного пространства этот документ интересен тем, что именно он зафиксировал необходимость международного информационного обмена как фактора стабильности.

4. Конвенция СНГ о правах и основных свободах человека (Минск, 1995 г.)

– В значительной степени повторяет положения Европейской конвенции, но адаптирована для постсоветского пространства.

– Гарантирует свободу выражения мнения и доступ к информации, при этом оставляет за государствами-участниками право ограничивать ее в интересах безопасности, морали и защиты прав других лиц.

Для России эта Конвенция важна в контексте взаимодействия с соседними государствами: многие трансграничные информационные потоки (СМИ, соцсети, интернет-ресурсы) действуют именно в пространстве СНГ.

2.8. Другие международные документы

– **Всеобщая декларация прав человека (1948 г., ст. 19)** впервые закрепила право на свободу слова и доступ к информации как универсальное.

– **ЮНЕСКО** принимает декларации и рекомендации, касающиеся свободы интернета, безопасности журналистов и борьбы с дезинформацией.

– **Международный пакт об экономических, социальных и культурных правах (1966 г.)** косвенно затрагивает сферу доступа к информации в связи с правом на образование и участие в культурной жизни.

Таким образом, международные соглашения создают **рамочные стандарты**:

– свобода информации – базовое право человека;

– ограничения возможны только в исключительных случаях;

– государства обязаны развивать открытость данных и защищать журналистов.

Для России это означает необходимость выстраивать баланс. С одной стороны, обеспечивать гражданам доступ к достоверной информации, с другой – блокировать деструктивный контент (экстремизм, наркотики, порнография и т. п.), что напрямую влияет на работу медийных источников в стране.

§ 3. Общие принципы российского законодательства, определяющие порядок формирования и распространения информации

Российское законодательство в сфере информации базируется на фундаментальных принципах, закрепленных в **Конституту-**

ции Российской Федерации от 12 декабря 1993 г. (с последующими изменениями). К ним относятся:

– свобода мысли и слова (ст. 29),

– недопустимость цензуры (ст. 29, ч. 5),

– свобода совести и вероисповедания (ст. 28),

– право на неприкосновенность частной жизни (ст. 23),

– равенство прав и свобод человека и гражданина (ст. 19).

Ключевым актом в сфере средств массовой информации является **Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» (ред. от 23.11.2024)**. Он конкретизирует конституционные нормы, закрепляет свободу СМИ, их права и обязанности, а также ограничения, направленные на защиту интересов общества и государства.

3.1. Свобода средств массовой информации

Статья 29 Конституции Российской Федерации устанавливает: «Каждому гарантируется свобода мысли и слова; каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом».

В развитие этих положений **ст. 1 Закона Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации»** закрепляет:

– СМИ свободны в поиске, получении, производстве и распространении массовой информации;

– учреждение, владение и пользование СМИ не подлежат ограничениям, за исключением случаев, установленных федеральными законами.

Аналогичные правила действуют и для **сетевых изданий**, которые в России с 2014 г. приравнены к СМИ.

3.2. Недопустимость цензуры

Статья 29 (ч. 5) Конституции Российской Федерации: «Гарантируется свобода массовой информации. Цензура запрещается».

Статья 3 Закона Российской Федерации № 2124-1 «О средствах массовой информации» уточняет, что цензурой признается:

– требование государственных органов, должностных лиц или организаций согласовывать материалы до публикации;

– наложение запрета на распространение сообщений или их частей.

Исключение: предварительное согласование материалов внутри редакции (например, с главным редактором) не считается цензурой, так как это часть внутреннего контроля.

Ограничения свободы СМИ допускаются федеральным законодательством, например:

– Федеральный конституционный закон от 30 мая 2001 г. № 3-ФКЗ «О чрезвычайном положении»;

– Федеральный конституционный закон от 30 января 2002 г. № 1-ФКЗ «О военном положении».

3.3. Гарантии против злоупотреблений свободой прессы

Статья 4 Закона Российской Федерации № 2124-1 «О средствах массовой информации» прямо запрещает использовать СМИ для:

– совершения уголовно наказуемых деяний;

– разглашения государственной тайны (см. **Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне»**);

– распространения экстремистских материалов (см. **Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»**);

– пропаганды порнографии, культа насилия или жестокости;

– использования ненормативной лексики.

В **постановлении Пленума Верховного Суда Российской Федерации от 15 июня 2010 г. № 16** (ред. от 2021 г.) разъяснено: при оценке публикаций суд должен учитывать контекст – жанр, стиль, цели автора, общественно-политическую ситуацию. Юмористические и сатирические материалы допускают большую степень преувеличения, но они не должны вводить аудиторию в заблуждение относительно фактов.

3.4. Запреты на распространение отдельных видов информации

Российское законодательство вводит строгие ограничения на публикацию следующих сведений:

– о несовершеннолетних, пострадавших от преступлений (**ст. 4 Закона о СМИ + Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»**);

– о ходе контртеррористических операций (**Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»**);

– о способах изготовления наркотиков и взрывчатых веществ (**Федеральный закон от 8 января 1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах»**).

Пример: в 2022 г. Роскомнадзор заблокировал ряд телеграм-каналов за публикацию инструкций по изготовлению самодельных взрывных устройств.

3.5. Современные тенденции

В последние годы наблюдается усиление государственного контроля за информационным пространством:

– введен **Федеральный закон от 5 мая 2014 г. № 97-ФЗ (о блогерах)** – блогеры с аудиторией более 3 тыс. чел. обязаны соблюдать нормы (как СМИ);

– принят **Федеральный закон от 23 июля 2013 г. № 187-ФЗ «О защите авторских прав в сети Интернет»**;

– действует **Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»**, ограничивающий обработку и распространение информации о частных лицах;

– в 2019 г. вступил в силу **Федеральный закон от 1 мая 2019 г. № 90-ФЗ («О надежном Рунете»)**, закрепивший возможность автономной работы российского сегмента сети.

Эти изменения направлены на защиту общественных интересов и национальной безопасности, но в академической среде часто становятся предметом дискуссий о границах свободы слова.

§ 4. Полномочные государственные органы Российской Федерации в области средств массовой информации: их права и обязанности

Минцифры России (Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации) – ключевой федеральный орган исполнительной власти, который:

– формирует и реализует государственную политику в области информационных технологий, связи, цифровой экономики и массовых коммуникаций;

– разрабатывает стратегии развития цифровой инфраструктуры (интернет, телевидение, радио, телекоммуникации);

– курирует цифровизацию госуслуг, внедрение электронного документооборота и использование IT в экономике;

– участвует в международных проектах в области цифровых технологий;

– разрабатывает нормативные правовые акты и контролирует их исполнение.

Роскомнадзор (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) – федеральный орган, который:

регистрирует средства массовой информации, ведет их государственный реестр;

– выдает лицензии на телерадиовещание;

– контролирует соблюдение законодательства о СМИ и защите персональных данных;

– ведет реестр иностранных агентов среди СМИ;

– имеет полномочия по ограничению доступа к интернет-ресурсам, нарушающим законодательство.

На практике Минцифры отвечает за стратегическое развитие и политику, а Роскомнадзор – за контроль, надзор и практическую реализацию.

Основные направления регулирования

1. Борьба с фейковыми новостями и недостоверной информацией.

– Первые полномочия Роскомнадзора по блокировке сайтов без суда были введены **Федеральным законом от 28 июля 2012 г. № 139-ФЗ** (изменения в Закон № 149-ФЗ «Об информации»).

– С 2019 г. – административная ответственность за распространение фейковых новостей (**Федеральный закон от 18 марта 2019 г. № 31-ФЗ**).

– С 2022 г. – уголовная ответственность за дискредитацию действий Вооруженных Сил Российской Федерации (**Федеральный закон от 4 марта 2022 г. № 32-ФЗ**).

На их основании Роскомнадзор блокировал сайты и СМИ, включая «Медузу», «Дождь», «Эхо Москвы».

2. Ограничения на владение СМИ иностранцами и статус иностранных агентов.

– **Федеральный закон от 14 октября 2014 г. № 305-ФЗ** ограничил участие иностранных инвесторов в российских СМИ максимум 20 %.

– **Федеральный закон от 2 декабря 2019 г. № 426-ФЗ** расширил понятие «иностранного агента», обязав СМИ, получающие иностранное финансирование, маркировать материалы. В 2021 г. «Медуза», «Радио Свобода», «Голос Америки» получили статус иностранного агента.

3. Контроль за интернет-платформами.

– **Федеральный закон от 1 декабря 2020 г. № 481-ФЗ** обязал соцсети с аудиторией более 500 тыс. пользователей удалять запрещенный контент в течение 24 часов. В 2022 г. TikTok был оштрафован за неудаление экстремистских материалов.

Порядок блокировки сайтов

На практике Роскомнадзор действует по упрощенной схеме:

1. Направляет уведомление владельцу сайта с требованием удалить запрещенный контент.

2. Если требование не выполняется – сайт блокируется.

3. **Конституционный Суд Российской Федерации** признал эту процедуру соответствующей Конституции Российской Федерации, указав, что она направлена на защиту национальной безопасности и общественных интересов.

Таким образом, современная тенденция – **усиление роли государства в регулировании информационного пространства**, особенно в части интернет-СМИ. С одной стороны, это повышает уровень информационной безопасности, с другой – вызывает дискуссии о границах свободы слова.

§ 5. Порядок и требования к регистрации средств массовой информации

Регистрация средств массовой информации (СМИ) в Российской Федерации регулируется **Законом Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»** (ред. от 23.11.2024). Контроль за процессом регистрации осуществляет **Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)**.

Учредители СМИ

Согласно ст. 7 Закона о СМИ, учредителями (соучредителями) СМИ могут быть:

– граждане Российской Федерации;

– объединения граждан;

– российские организации (юридические лица);

– государственные органы.

Запреты и ограничения:

– лица младше 18 лет;

– осужденные, отбывающие наказание в местах лишения свободы;

– граждане, признанные судом недееспособными;

– объединения или организации, деятельность которых запрещена (например, признанные экстремистскими);

– иностранные граждане и лица без гражданства, не проживающие постоянно в Российской Федерации.

Пример: в 2021 г. Роскомнадзор отказал в регистрации СМИ, учредителем которого выступал гражданин Украины без постоянного места жительства в России.

Процедура регистрации

1. Учредитель подает заявление о регистрации в Роскомнадзор (или его территориальный орган).

Если СМИ планируется к распространению по всей Российской Федерации или за ее пределами, заявление направляется в федеральный центр;

Если только на уровне субъекта Российской Федерации или муниципалитета – в территориальный орган.

2. Срок рассмотрения – до 30 дней.

3. При положительном решении выдается **свидетельство о регистрации СМИ** (бессрочное).

4. Учредитель обязан начать выпуск в течение 12 месяцев, иначе регистрация аннулируется.

Исключения (ст. 12 Закона о СМИ): регистрация не требуется для:

– официальных изданий органов власти, публикующих законы и нормативные акты;

– печатных изданий с тиражом менее 1000 экз.;

– радио- и телепрограмм, распространяемых по кабелю в пределах учреждения (например, школьное радио);

– аудио- и видеопрограмм с тиражом менее 10 экземпляров.

Пример: в 2023 г. Роскомнадзор подтвердил, что школьные газеты и радиостанции не требуют регистрации, если распространяются только в пределах учебного заведения.

Прекращение или приостановка деятельности СМИ

СМИ может быть прекращено или приостановлено:

– по решению учредителя;

– по решению суда на основании иска Роскомнадзора.

Основания:

– неоднократные нарушения ст. 4 Закона о СМИ (злоупотребление свободой прессы);

– неисполнение предписаний Роскомнадзора;

– нарушение Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности».

Примеры:

– в 2021 г. проект «ОВД-Инфо» был заблокирован за публикации, признанные подстрекательством к митингам;

– в 2022 г. прекращена деятельность телеканала «Дождь» за дискредитацию действий Вооруженных Сил Российской Федерации;

– в том же году деятельность радиостанции «Эхо Москвы» была приостановлена решением суда за распространение экстремистских материалов.

Освобождение СМИ от ответственности

Редакция, главный редактор или журналист могут быть освобождены от ответственности, если информация:

– опубликована в официальных сообщениях госорганов;

– получена от информационных агентств (ТАСС, Интерфакс и др.);

– предоставлена в ответ на официальный запрос;

– исходит из пресс-службы госорганов или организаций;

– является дословным воспроизведением речи должностного лица;

– опубликована в прямом эфире;

– перепечатана из другого СМИ (ответственность несет первоисточник).

Пример: в 2021 г. федеральный телеканал избежал ответственности за цитирование депутата Госдумы: суд установил, что канал дословно воспроизвел речь.

Важно: освобождение не распространяется на случаи искажения данных, публикации экстремистских материалов или информации о несовершеннолетних.

§ 6. Правовой статус блогеров и их ответственность

6.1. Понятие блогера

В современном понимании **блогер** – это физическое или юридическое лицо, которое систематически размещает в сети Интернет публично доступный контент (тексты, фото, видео и др.), предназначенный для неограниченного круга пользователей.

В отличие от журналистов блогеры не всегда связаны редакцией СМИ, но их деятельность регулируется рядом законов, так как она может оказывать значительное влияние на общественное мнение.

С 2014 г. в России действовали так называемые законы о блогерах (Федеральный закон от 05.05.2014 № 97-ФЗ), обязывавшие популярных авторов (с аудиторией свыше 3000 чел. в сутки) регистрироваться в Роскомнадзоре. Впоследствии эти нормы были смягчены, но блогеры по-прежнему подпадают под действие общих правил о распространении информации.

6.2. Регистрация и идентификация

В настоящее время в соответствии с **Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»** блогеры, ведущие публичные страницы, обязаны:

– соблюдать правила, установленные платформами (YouTube, RUTUBE, «ВКонтакте», Telegram, TikTok, Twitch и др.);

– указывать достоверные сведения о себе при регистрации аккаунта (по требованию платформы или Роскомнадзора);

– хранить данные о распространенных публикациях.

Регистрация в Роскомнадзоре обязательна только для владельцев сайтов, которые признаются средствами массовой информации.

6.3. Права блогеров

Блогеры обладают следующими правами:

1. Свободно выражать свое мнение в сети Интернет (ст. 29 Конституции Российской Федерации).

2. Использовать псевдонимы.

3. Размещать рекламу на возмездной основе (при соблюдении требований Федерального закона от 13.03.2006 № 38-ФЗ «О рекламе»).

4. Использовать общедоступную информацию при условии соблюдения авторских прав.

6.4. Обязанности блогеров

Согласно действующему законодательству, блогеры обязаны:

– **проверять достоверность информации** перед ее публикацией (ст. 10.1 Закона о СМИ, применяемая по аналогии);

– **соблюдать авторские права** (Федеральный закон от 18.12.2006 № 230-ФЗ, ст. 1255 ГК РФ);

– **не распространять сведения, ограниченные в доступе**, включая государственную тайну (Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне»), персональные данные (Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»);

– **соблюдать запреты**:

– на распространение экстремистских материалов (Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»);

– на публикацию порнографии и пропаганды наркотиков (ст.ст. 242 и 228 УК РФ);

– на дискредитацию Вооруженных Сил Российской Федерации (ст. 280.3 УК РФ, введена ФЗ № 32-ФЗ от 4 марта 2022 г.).

6.5. Ответственность блогеров

Гражданская ответственность

– За распространение ложных сведений, порочащих честь и достоинство граждан, блогер может быть привлечен к компенсации морального вреда (ст. 152 ГК РФ).

Пример: в 2022 г. блогер был оштрафован судом на 100 тыс. руб. за публикацию ложных сведений о бизнесмене, которые нанесли ущерб его деловой репутации.

Административная ответственность

– статья 13.15 КоАП РФ – злоупотребление свободой массовой информации (штрафы за публикацию фейков);

– статья 20.3.1 КоАП РФ – возбуждение ненависти либо вражды;

– статья 20.33 КоАП РФ – нарушение законодательства об иностранных агентах.

Уголовная ответственность

– статья 128.1 УК РФ – клевета;

– статья 280 УК РФ – публичные призывы к экстремистской деятельности;

– статья 280.3 УК РФ – дискредитация Вооруженных Сил Российской Федерации;

– статья 205.2 УК РФ – оправдание терроризма;

– статья 242.1 УК РФ – оборот материалов с детской порнографией.

Пример: в 2021 г. блогер был осужден условно за публикацию экстремистских материалов в телеграм-канале.

6.6. Ограничения, связанные с несовершеннолетними

Блогерам запрещено публиковать:

– сведения о личности несовершеннолетних потерпевших (Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»);

– материалы, способные причинить вред психическому или нравственному развитию детей.

Пример: в 2021 г. блогер был оштрафован за публикацию видео с участием школьника, приведшее к травле ребенка.

Современный правовой статус блогеров в России базируется на сочетании принципа свободы слова и строгих ограничений, связанных с защитой общественных интересов. Блогеры, как

и журналисты, несут ответственность за достоверность и законность распространяемой информации.

Для минимизации рисков блогерам рекомендуется:

1. Проверять источники перед публикацией.
2. Не использовать материалы без согласия авторов.
3. Консультироваться с юристами по спорным вопросам.
4. Учитывать требования Роскомнадзора и площадок (YouTube, VK, Telegram).

Таблица 8

Правовой режим регулирования СМИ и блогеров в Российской Федерации

Критерий	СМИ	Блогеры
Регистрация	Обязательна в Роскомнадзоре (Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»)	Не требуется, кроме случаев признания сайта/канала СМИ. Ранее действовали «законы о блогерах» (ФЗ № 97-ФЗ от 5 мая 2014 г.), теперь – только учет крупных площадок
Учредитель	Граждане Российской Федерации, юрлица, объединения, госорганы	Любое лицо, ведущее публичный контент. Обязательная идентификация на платформах при монетизации или большой аудитории
Права	Свобода поиска, получения и распространения информации (ст. 29 Конституции Российской Федерации, ст. 1 Закона о СМИ). Возможность аккредитации при госорганах	Свобода выражения мнений (ст. 29 Конституции Российской Федерации). Можно публиковать под псевдонимом, размещать рекламу, использовать общедоступную информацию
Обязанности	Проверка достоверности информации, соблюдение авторских прав, запрет на экстремизм, пропаганду насилия, порнографию (ст. 4 Закона о СМИ)	Те же ограничения: запрет на фейки, экстремизм, нарушение авторских прав, разглашение персональных данных. Дополнительно – маркировка рекламы (ФЗ «О рекламе»)
Ответственность (гражданская)	За клевету, распространение порочащих сведений (ст. 152 ГК РФ)	За клевету, ущерб деловой репутации (ст. 152 ГК РФ)

Окончание табл. 8

Ответственность (административная)	Статья 13.15 КоАП РФ – злоупотребление свободой СМИ; ст. 20.29 КоАП РФ – распространение экстремистских материалов	Статья 13.15 КоАП РФ – фейки; ст. 20.3.1 КоАП РФ – возбуждение ненависти; штрафы за нарушение правил рекламы
Ответственность (уголовная)	Статья 128.1 УК РФ – клевета; ст. 280 УК РФ – призывы к экстремизму; ст. 205.2 УК РФ – оправдание терроризма	Те же статьи УК РФ, плюс ст. 280.3 УК РФ – дискредитация ВС РФ, ст. 242 УК РФ – распространение порнографии
Особые ограничения	Запрет на иностранное владение более 20 % уставного капитала СМИ (ФЗ от 14 октября 2014 г. № 305-ФЗ)	Ограничения на публикацию информации о несовершеннолетних (ФЗ от 29 декабря 2010 г. № 436-ФЗ). Возможность блокировки аккаунтов по требованию Роскомнадзора

§ 7. Методика выявления медийных источников, распространяющих ложную информацию в сети Интернет

Ложная информация – это не только фейки в соцсетях, но и целые кампании, направленные на манипуляцию общественным мнением. Для противодействия необходимо системное и многоуровневое исследование источников.

Методику можно представить в виде **шести шагов**, каждый из которых сопровождается примерами и практическими приемами.

Шаг 1. Проверка источника

Цель – понять, кто распространяет информацию и насколько он заслуживает доверия.

Приемы:

– Сбор метаданных (дата регистрации аккаунта, геолокация, IP-адрес, принадлежность домена).

– Сравнение с белыми списками (официальные СМИ, научные журналы) и черными списками (издания, уличенные в фейках).

– Анализ репутации: был ли источник уличен в публикации ложных материалов ранее?

Пример: анонимный телеграм-канал с десятками тысяч подписчиков, созданный 3 недели назад, публикует эксклюзивные данные о мобилизации – высокий риск фейка.

Шаг 2. Поиск первоисточников

Цель – отделить оригинал от пересказа.

Приемы:

– Проверка ссылок: есть ли в публикации выход на научные статьи, официальные документы или первичные заявления?

– Отслеживание цепочки репостов (OSINT-инструменты: Hoaxy, InVid, CrowdTangle).

– Сравнение дат: если сенсация впервые появляется в малоизвестном блоге, а крупные СМИ молчат – стоит усомниться.

Пример: статья «Ученые доказали, что кофе вызывает рак» без ссылки на журнал или исследование → вероятный фейк.

Шаг 3. Анализ содержания

Цель – выявить маркерные признаки манипуляции.

Красные флаги:

– Заголовки в стиле «СРОЧНО!», «ШОК!», «То, о чем молчат власти!».

– Отсутствие конкретики: «эксперты считают», «источники сообщили».

– Наличие эмоциональной окраски («ужасная правда», «предательство народа»).

Приемы:

– Тон-анализ (Tone Analyzer, TextRazor).

– Сравнение текста с официальными заявлениями.

– Проверка лексического почерка – у сетей ботов набор слов часто повторяется.

Шаг 4. Проверка фактов и деталей

Цель – убедиться, что отдельные элементы новости соответствуют действительности.

Приемы:

– Обратный поиск изображений (Google Images, TinEye, Yandex).

– Геолокация фото (Mapillary, SunCalc, ExifTool).

– Проверка дат через архивы (Wayback Machine).

– Сопоставление фактов: если новость утверждает, что «в Москве прошел митинг на 50 тысяч человек», но фото из Стамбула 2013 г., – это фейк.

Шаг 5. Проверка цитат и экспертов

Цель – выявить искажения или манипуляции авторитетами.

Приемы:

– Поиск оригинала цитаты в базах СМИ и официальных выступлениях.

– Сверка с видеозаписью выступления.

– Проверка эксперта: есть ли у него реальный опыт и публикации, или это мнимый аналитик?

Пример: фраза «В СССР секса нет» в оригинале звучала иначе: «У нас секса нет на телевидении». Контекст кардинально меняет смысл.

Шаг 6. Использование фактчекинговых ресурсов и искусственного интеллекта

Цель – ускорить процесс проверки.

Инструменты:

– Snopes, StopFake, FactCheck.org – англоязычные.

– «Проверено», Fakecheck, «Лентач. Проверка фактов» – российские.

– Deepware Scanner, Hive Moderation – для выявления дипфейков.

– ChatGPT / Bard / Claude – для анализа логических противоречий (но с обязательной перепроверкой).

Креативный прием: формировать цифровое досье на источник: хронология публикаций, стиль, тематика. Так можно отличить случайную ошибку от систематической кампании.

Действия при выявлении ложной информации:

1. Не распространять и не делиться сомнительным материалом.

2. Сообщить о факте фейка администраторам платформы.

3. Передать информацию в Роскомнадзор или Лигу безопасного Интернета.

4. Провести разъяснительную работу в учебных и трудовых коллективах.

Креативный элемент «Фильтрфейка»

Представим методику как **пять фильтров**, через которые должна пройти любая информация:

1. **Источник** – кто сказал?

2. **Первичность** – откуда он это узнал?

3. **Факты** – совпадают ли даты, фото, цифры?

4. **Цитаты** – не вырваны ли слова из контекста?

5. **Технологии** – что скажут фактчекинг и ИИ?

Если новость не прошла хотя бы один фильтр – доверять ей нельзя.

Таблица 9

Методика выявления фейковой информации в сети Интернет

Этап	Действие	Что проверяем	Инструменты/методы
1	Проверка источника	Надежность и репутация СМИ, блогера, телеграм-канала	Проверка данных о СМИ в Роскомнадзоре, поиск публикаций автора в других СМИ
2	Поиск первоисточников	Есть ли ссылки на документы, исследования, официальные заявления	Официальные сайты органов власти, научные журналы, локальные издания
3	Анализ автора	Указан ли автор? Его компетентность и специализация	Поиск по ФИО в интернете, профили в соцсетях, профессиональные биографии
4	Перекрестная проверка	Совпадают ли даты, факты, цитаты у разных источников	Google, Yandex, агрегаторы новостей («Яндекс.Новости», Google News)
5	Проверка отдельных фактов	Имена, географию, даты, статистику	Официальные базы данных (ЕГРЮЛ, «Госстат», «Росстат»), открытые реестры
6	Анализ изображений и видео	Подлинность фото/видео, место и время съемки	Google Images, Yandex.Картинки, TinEye, InVID
7	Проверка цитат	Не искажены ли слова, не вырваны ли из контекста	Поиск цитаты в оригинале, сопоставление с полным текстом или видео
8	Анализ языка	Эмоциональные заголовки, громкие оценки, «сенсации»	Контент-анализ: наличие преувеличений, обилие превосходных степеней
9	Использование фактчекинговых ресурсов	Проверка популярной новости	Snopes, Fakechec, проект «Проверено»
10	Экспертная проверка	Консультация по сложным темам (медицина, финансы, право)	Эксперты, официальные ведомства, отраслевые сообщества

Учебно-методический раздел к главе 8

Цели изучения темы

1. Освоить понятие «медийные источники информации», их классификацию.

2. Изучить признаки и формы ложной информации, используемой в сети Интернет.

3. Научиться применять методику выявления недостоверных сведений (проверка источников, анализ изображений, перекрестная проверка фактов).

4. Развить навыки критического мышления при работе с информацией из открытых источников.

5. Изучить современные технологии проверки достоверности информации (обратный поиск изображений, фактчекинговые платформы, базы данных).

6. Освоить методы правовой оценки деятельности СМИ и блогеров при распространении недостоверных сведений.

7. Сформировать умение предлагать меры по совершенствованию борьбы с дезинформацией на государственном и международном уровнях.

Вопросы для семинарского занятия

Теоретические вопросы

1. Что такое медийные источники информации? Какие их виды вы знаете?

2. Какие нормативные правовые акты Российской Федерации регулируют деятельность СМИ и блогеров?

3. Какие формы и виды ложной информации наиболее распространены в интернете?

4. Каковы этапы методики проверки достоверности информации в сети Интернет?

5. Какие современные инструменты помогают выявлять фейки (Google Images, TinEye, Snopes, Fakecheck)?

6. Почему даже авторитетные СМИ могут становиться источниками ложных сведений?

7. Какую роль играют фактчекинговые ресурсы в противодействии дезинформации?

8. Какую ответственность несут блогеры и журналисты за распространение фейков?

9. Какие риски возникают при усилении контроля государства за информационным пространством?

10. Какие меры можно предложить для повышения медиаграмотности населения?

Варианты практических заданий для студентов

1. Анализ фейковой новости

Найти в соцсетях или мессенджерах пример фейковой публикации.

Проверить: источник, первоисточник, изображения, цитаты.

Подготовить отчет с выводами.

2. Создание фейковой новости (учебный эксперимент)

Разделить студентов на группы. Каждая группа создает фейк с использованием методов искажений (поддельные фото, вырванные цитаты).

Другие группы должны выявить признаки фейка.

3. Проверка источников

Дать студентам список каналов: официальные СМИ, телеграм-каналы, блоги.

Задание: определить уровень достоверности каждого источника.

4. Работа с фактчекинговыми ресурсами

Проверить спорные новости через Snopes, Fakecheck, «Проверено».

Сравнить результаты и обсудить их в группе.

Иные формы обучения

– **Мозговой штурм.** Тема: «Какие методы можно внедрить для борьбы с фейками в России?»

– **Деловая игра «Редакция СМИ».** Студенты играют роли журналистов, редакторов, фактчекеров.

Задача: подготовить материал и проверить его достоверность.

– **Суд над фейком.** Одна группа студентов выступает в роли обвинения, другая – защиты.

Задача: доказать или опровергнуть достоверность новости.

– **Круглый стол** «Свобода слова и контроль информации: где границы?»

– **Ролевая игра «Аукцион».** Студенты моделируют онлайн-аукцион, где появляется сомнительная информация.

Задача: выявить ложные сведения и принять меры.

– **Проектная работа.** Разработка модели национальной системы борьбы с фейками.

Включить: анализ угроз, использование технологий ИИ и блокчейна, участие государства и общества.

Библиографический список к главе 8

Монографии, учебники

1. Браун, М. Методика поиска информации в Интернете / М. Браун. – М. : Новый издательский дом, 2005.

2. Загидуллина, М. В. Панмедиатизация: закат вербальной коммуникации / М. В. Загидуллина. Челябинск : Изд-во ЧелГУ, 2019.

3. Калмыков, А. А. Медиалогия интернета / А. А. Калмыков. – М. : Либроком, 2013.

4. Карпухин, С. В. Регулирование СМИ в России: анализ правового поля и тенденций / С. В. Карпухин. – М., 2019.

5. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. – 5-е изд., перераб. и доп. – М. : Юрайт, 2020.

6. Шилов, А. А. Медийные ресурсы Интернета: проблемы эволюции / А. А. Шилов. – Краснодар : Изд-во КубГУ, 2005.

Статьи

7. Акопов А. И. Электронные сети как новый вид СМИ // Филологический вестник РГУ. – 1998. – № 3. – С. 43–51.

8. Иванов И. И., Петров П. П. Методы выявления и противодействия распространению фейковых новостей в социальных сетях // Информационная безопасность. – 2023. – № 4. – С. 10–18.

9. Каминский В. С. Трансформация общественно-политических воззрений в контексте электорального поведения населения // Проблемы развития территории. – 2019. – № 3. – С. 55–62. – URL: http://pdt.isertran.ru (дата обращения: 04.09.2025).

10. Козлов К. К., Морозов М. М. Анализ алгоритмов распространения фейковых новостей // Информационное общество. – 2023. – № 3. – С. 25–32.

11. Николаев Н. Н., Васильев В. В. Цифровая криминалистика: выявление источников дезинформации // Компьютерная криминалистика. – 2024. – № 1. – С. 77–84.

12. Раскладкина М. К. Сетевая пресса как объект коммуникативных исследований // Теория коммуникации & прикладная коммуникация : сб. науч. трудов / под ред. И. Н. Розиной. – Ростов н/Д. : ИУБиП, 2002. – Вып. 1. – С. 223-224.

13. Самосват О. И. Лайк в социальных сетях как показатель социального одобрения // Казанский педагогический журнал. – 2015. – № 6. – С. 148–150.

14. Сидорова А. А. Правовое регулирование противодействия фейковым новостям в России // Государство и право. – 2024. – № 2. – С. 19–25.

15. Шарипов Л. З. Проблемы правового регулирования средств массовой информации в России // NovaUm. – 2020. – Вып. 25. 16.05.2020.

Электронные ресурсы

16. Рожкова? М. А. «Общедоступная информация», «открытые данные» и «персональные данные, разрешенные субъектом для распространения» – что это такое и как они между собой связаны? / М. А. Рожкова // Закон.ру. – 2021. – 13 января. – URL: https://zakon.ru/blog/2021/1/13/obschedostupnaya_informaciya_otkrytye_dannye_i_pe (дата обращения: 04.09.2025).

Глава 9. МЕТОДИКА ВЫЯВЛЕНИЯ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С РАСПРОСТРАНЕНИЕМ ПРОТИВОПРАВНОГО КОНТЕНТА В СЕТИ ИНТЕРНЕТ

ВВЕДЕНИЕ

Современное общество невозможно представить без информационно-телекоммуникационной сети Интернет, которая стала неотъемлемой частью повседневной жизни. Однако наряду с огромными возможностями, которые предоставляет глобальная сеть, она также стала площадкой для распространения противоправного контента, представляющего серьезную угрозу для безопасности личности, общества и государства.

Сегодня в Интернете активно распространяются материалы экстремистского характера, пропаганда наркотиков, мошеннические схемы, контент, связанный с эксплуатацией детей, и другие виды противоправной информации. Это требует от правоохранительных органов не только оперативного реагирования, но и владения современными методиками выявления, анализа и пресечения таких преступлений.

Согласно данным отчета Global Digital за 2023 г.[1], более **66 %** всех жителей нашей планеты пользуются интернетом. За 2023 г. аудитория интернета выросла на **97 млн** новых пользователей, а их общее число составляет **5,35 млрд чел**. В России этот показатель составляет 73,3 %, что делает нашу страну одной из самых активных в цифровом пространстве.

[1] URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2024-v-mire-i-v-rossii/?utm_referrer=https%3a%2f%2fyandex.ru%2f#3.

В 2024 г., согласно исследованиям, общее время, проведенное пользователями в социальных сетях, достигло колоссальной цифры – **500 млн лет!** Вдумайтесь: время существования человечества (7–8 млн лет) по сравнению с этим – мгновение. Это время было потрачено на поиск информации, общение, потребление новостей и развлекательного контента. Такой масштаб цифровой активности подчеркивает не только огромную роль социальных сетей в современной жизни, но и необходимость тщательного контроля их содержания, чтобы минимизировать риски, связанные с распространением противоправного контента. Ведь за кажущейся безобидностью этих действий скрываются серьезные риски: противоправный контент маскируется под легальные материалы, что затрудняет его выявление и блокировку.

Для борьбы с противоправным контентом необходимо знать и владеть основными понятиями, связанными с контентом в сети Интернет, его формами и видами, с методиками выявления и раскрытия преступлений, связанных с распространением противоправной информации, а также нормативную базу, регулирующую эту сферу.

§ 1. Формы и виды контента в сети Интернет

Объяснить, что такое контент, простыми словами непросто, поскольку у этого термина существует множество трактовок.

В общепринятом понимании контент – это любая информация, которую человек способен воспринять визуально, аудиально или текстуально. В широком смысле он существовал задолго до цифровой эпохи: книги, газеты, радио- и телепередачи также являются формами контента.

В современном понимании термин «контент» чаще всего связан именно с цифровой средой – информацией, размещенной

и потребляемой через Интернет: тексты, изображения, аудио, видео и мультимедиа.

Сегодня цифровой контент окружает каждого:

– посты и публикации в социальных сетях,

– новостные статьи и аналитика,

– видеоролики и прямые трансляции на YouTube, RuTube или Twitch,

– подкасты и аудиокниги,

– рекламные баннеры, презентации и инфографика.

Важная особенность цифровой эпохи – двойственная роль пользователей: каждый человек является не только потребителем, но и создателем контента. Это формирует крайне динамичную и разнообразную цифровую среду, где информация мгновенно распространяется и меняется, а вместе с этим растут и риски появления противоправного или деструктивного контента.

Таким образом, под контентом в сети Интернет следует понимать любую совокупность текстовой, визуальной, аудиальной или смешанной информации, созданной и распространяемой в цифровом формате, которая формирует современное медиапространство и оказывает прямое влияние на общественное сознание, поведение и безопасность.

1.1. Классификация контента

Несмотря на условность и неоднозначность термина «контент», его можно систематизировать по ряду критериев. Такая классификация помогает лучше понимать природу информации, особенности ее распространения, а также облегчает выявление противоправного контента.

1. По форме подачи информации:

– **текстовый** – статьи, посты, комментарии, книги, новости;

– **графический** – фотографии, иллюстрации, инфографика, мемы;

– **видео** – фильмы, ролики, сторис, трансляции;

– **аудио** – музыка, подкасты, аудиокниги, голосовые сообщения;

– **мультимедийный** – сочетание нескольких форм (например, статья с фото и видео).

2. По содержанию:

– **информационный** – новости, сводки, аналитика;

– **познавательный (обучающий)** – инструкции, лекции, курсы;

– **развлекательный** – юмористические ролики, мемы, игры;

– **коммерческий** – реклама, продающие тексты, промоакции;

– **интерактивный** – опросы, квизы, голосования.

3. По площадкам размещения:

– социальные сети (ВКонтакте, Instagram, TikTok, X);

– видеохостинги (YouTube, RuTube, Vimeo);

– блоги и сайты (корпоративные и персональные);

– мессенджеры (Telegram, WhatsApp, Viber);

– специализированные платформы (форумы, vc.ru и др.).

4. По назначению:

– **информационный** – донесение фактов;

– **рекламный** – продвижение товаров и услуг;

– **сервисный** – уведомления, инструкции;

– **вирусный** – рассчитанный на быстрое распространение;

– **репутационный** – отзывы, кейсы, рекомендации.

5. По степени уникальности:

– **авторский** – оригинальный материал, созданный с нуля;

– **рерайт** – переработанный текст;

– **копипаст** – дословное копирование;

– **перевод** – адаптация с другого языка.

6. По степени эксклюзивности:

– **эксклюзивный** – рассчитанный на конкретную аудиторию;

– **массовый** – доступный широкой публике.

7. Современные тенденции в создании контента:

– использование **искусственного интеллекта** (нейросети, генераторы текста и изображений);

– рост популярности **коротких вертикальных видео** (Reels, TikTok);

– распространение **подкастов** и аудиоконтента;

– вовлечение аудитории через **интерактивность** (опросы, комментарии, челленджи);

– популяризация **искреннего и живого контента** (реальные истории, признания, ошибки).

Для правоохранительных органов понимание классификации контента имеет практическое значение:

– по форме подачи можно определить методы маскировки противоправного материала (например, скрытые надписи на изображениях);

– по содержанию – выявить тематику и цель публикации (экстремизм, мошенничество, пропаганда наркотиков);

– по площадке – локализовать аудиторию и разработать стратегию мониторинга;

– по уникальности – отличить подлинные материалы от копий, вбросов и клонов.

Таблица 10

Формы и виды контента в сети Интернет

Критерий	Вид контента	Примеры	Преимущества	Недостатки/риски
Форма подачи	Текстовый	Статьи, блоги, посты, новости	Доступность, простота создания	Легко подделать или исказить
	Графический	Фото, инфографика, мемы	Визуальная наглядность	Фейковые изображения, монтаж
	Видео	Ролики, трансляции, фильмы	Высокая вовлеченность аудитории	Подделка (deepfake), манипуляции
	Аудио	Подкасты, аудиокниги, музыка	Удобство восприятия (на ходу)	Сложно проверить достоверность
	Мультимедийный	Статьи с фото и видео, лонгриды	Комплексное воздействие	Требует больше ресурсов для проверки
Содержание	Информационный	Новости, отчеты, сводки	Оперативность	Возможные фейки под видом новостей
	Познавательный	Лекции, инструкции, обучающие видео	Польза для аудитории	Риск распространения ложных знаний
	Развлекательный	Мемы, шутки, игры	Вирусный эффект, вовлеченность	Часто используется для маскировки фейков
	Коммерческий	Реклама, промо-ролики, продающие тексты	Стимулирует продажи	Скрытая реклама, мошенничество
	Интерактивный	Тесты, опросы, голосования	Активное вовлечение	Возможна манипуляция результатами

Окончание табл. 10

Площадка	Социальные сети	VK, Instagra, TikTok, X (Twitter)	Широкий охват	Быстрый разгон фейков
	Видеохостинги	YouTube, RuTube, Vimeo	Визуальное воздействие	Сложно контролировать объем контента
	Блоги/сайты	«Яндекс.Дзен», VC.ru, личные сайты	Экспертность, нишевая аудитория	Слабая модерация, низкая проверяемость
	Мессенджеры	Telegram, WhatsApp, Viber	Высокая скорость распространения	Анонимность, трудность контроля
	Тематические форумы	Профессиональные площадки, сообщества	Целевая аудитория	Легко распространять дезинформацию
Назначение	Вирусный	Челленджи, флешмоб, мемы	Быстрое распространение	Высокая вероятность манипуляций
	Репутационный	Отзывы, кейсы, рекомендации	Доверие к источнику	Заказные отзывы, черный PR
Уникальность	Авторский	Оригинальные статьи, уникальные фото	Ценность, доверие	Требует усилий, времени
	Рерайт	Переработанный материал	Доступность	Потеря смысла, искажение фактов
	Копипаст	Прямое копирование	Скорость	Плагиат, дезинформация
	Перевод	Адаптация с иностранного источника	Расширение аудитории	Риск неточного перевода
Эксклюзивность	Эксклюзивный	Контент для конкретной аудитории	Высокий уровень доверия	Ограниченный охват
	Массовый	Новости, вирусные видео	Широкий охват	Низкая достоверность, шум

1.2. Противоправный контент в сети Интернет: сущность и виды

Противоправный контент – это информация, распространение которой в сети Интернет нарушает законодательство Российской Федерации и международные нормы. Ключевая его особенность заключается в том, что он может маскироваться под легальные материалы, распространяться через разные каналы и быстро адаптироваться к мерам блокировки.

1.3. Виды и формы противоправного (деструктивного) контента в сети Интернет

В современном цифровом обществе понятие *«противоправный контент»* стало привычным, но в научной и правоприменительной практике до сих пор нет единого определения. Чаще всего под ним понимают **информацию в сети Интернет, которая нарушает законодательство, угрожает общественной безопасности или оказывает негативное влияние на пользователей**.

В международной практике применяются разные термины: «вредоносный контент», «социально опасный контент», «деструктивная информация», что создает правовую неопределенность и затрудняет единый подход к классификации.

На основании российского законодательства, анализа практики Роскомнадзора, Лиги безопасного интернета и зарубежного опыта можно выделить **четыре ключевые категории противоправного контента**:

1.3.1. Запрещенный контент

Материалы, распространение которых **жестко запрещено законом**.

– сексуализация несовершеннолетних (детская порнография, эксплуатация образов детей);

– насилие над людьми и животными (сцены пыток, жестокости);

– самоповреждение и суицидальный контент;

– киберунижение и травля (доксинг, публикация интимных фото без согласия);

– оккультные услуги, связанные с нанесением вреда жизни и здоровью;

– подрыв норм поведения (девиации, асоциальные модели);

– распространение ложных сведений о пользе алкоголя, наркотиков и табака.

Пример: в 2024 г. Роскомнадзор заблокировал ряд телеграм-каналов, публиковавших инструкции по изготовлению взрывчатых веществ и пропаганду насилия.

1.3.2. Ограниченный к распространению контент

Материалы, доступ к которым может быть **ограничен из-за риска для психики и морали**:

– сцены насилия и антиобщественных действий;

– чрезмерное использование нецензурной лексики;

– шок-контент (кадры катастроф, травм, жестокости).

Пример: YouTube неоднократно подвергался критике за запоздалое удаление роликов с издевательствами над животными.

1.3.3. Контент, вовлекающий в противоправную деятельность

Информация, которая побуждает пользователя к совершению преступлений:

– экстремизм и терроризм (призывы к насилию, оправдание терроризма);

– инструкции по совершению преступлений (хакерство, взломы, изготовление оружия);

– мошенничество (финансовые пирамиды, фишинг, поддельные вакансии).

Пример: в 2024 г. Лига безопасного интернета выявила видеоролики с инструкциями по изготовлению коктейлей Молотова, что привело к их судебной блокировке.

1.3.4. Контент, нарушающий нормы морали и нравственности

Материалы, формирующие искаженные ценности и социально опасные практики:

– пропаганда наркотиков, алкоголя, расстройств пищевого поведения;

– кибербуллинг и травля;

– ложные ценности (романтизация асоциального образа жизни, опасных развлечений).

Примеры:

– видео с руфингом и скайуокингом (экстремальные подъемы без страховки);

– контент о диггерстве (нелегальное исследование подземных коммуникаций).

Уязвимые категории граждан

– **Дети**: склонны доверять любым источникам, воспринимать информацию буквально, легко вовлекаются в челленджи и игры.

– **Пожилые люди**: низкий уровень цифровой грамотности делает их уязвимыми для мошенничества и манипуляций.

– **Подростки**: находятся в зоне риска по причине поиска самоидентификации, подвержены трендам.

Пример: в 2022-2023 гг. в TikTok активно распространялись опасные челленджи (Blackout Challenge, Blue Whale), которые побуждали подростков к опасным действиям. Это вызвало рост числа обращений в МВД России и Роскомнадзор.

Современные тенденции регулирования

– **Законодательные инициативы**:

В декабре 2024 г. в Госдуму Российской Федерации внесен законопроект о *маркировке контента в видеоиграх* (жестокость, насилие, наркотики, ненормативная лексика).

Действует Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Усилен контроль Роскомнадзора за иностранными платформами (TikTok, YouTube, Telegram).

– **Технические меры:** использование систем автоматической фильтрации контента, алгоритмов распознавания изображений и речи, технологий машинного обучения для выявления триггерных слов и подозрительных материалов.

– **Социальные меры**: работа Лиги безопасного интернета, школьных медиаклубов, внедрение курсов по цифровой гигиене и медиаграмотности.

1.4. Проблемы распространения противоправного контента

Распространение противоправного контента в сети Интернет остается одной из наиболее острых проблем современной цифровой среды. Несмотря на активную работу государственных органов и общественных организаций, масштабы угрозы ежегодно растут.

По данным Роскомнадзора за 2024 г.:

– заблокировано более 3,5 тыс. материалов с призывами к массовым беспорядкам (рост в 2,2 раза по сравнению с 2023 г.);

– выявлено и ограничено 33,2 тыс. материалов, вовлекающих несовершеннолетних в противоправные действия (рост в 1,5 раза);

– увеличилось количество блокировок ресурсов с пропагандой наркотиков, азартных игр, а также сайтов, распространяющих мошеннический контент (так называемые фишинговые зеркала).

Однако, по признанию самого ведомства, часть крупных зарубежных площадок игнорирует российское законодательство. Так, еще в 2022 г. Роскомнадзор фиксировал отказ YouTube удалить более **35 тыс. материалов**, признанных нарушающими российские законы. Ситуация сохраняется: в 2024–2025 гг. отдельные иностранные платформы не выполняют требования о блокировке противоправного контента в установленные сроки, что приводит к штрафам и угрозам частичной или полной блокировки.

Три модели регулирования контента в мировой практике:

– **Американский подход** – платформы фактически освобождены от ответственности за пользовательский контент (ориентация на свободу слова, ограничение только по решению суда).

– **Европейский подход** – платформы обязаны удалять противоправный контент, однако его выявление часто возложено на пользователей через систему жалоб (*notice-and-take-down*).

– **Азиатский подход** – государство играет ключевую роль в мониторинге и блокировке деструктивных материалов, нередко в режиме превентивной цензуры.

– **Российская модель** ближе всего к азиатскому подходу, но сочетает его с элементами гражданского контроля.

Помимо Роскомнадзора активное участие в мониторинге принимают общественные организации и профессиональные объединения:

– **Лига безопасного интернета** (поддержка детского и семейного сегмента сети);

– **Group-IB** (анализ киберугроз и финансовых мошеннических схем);

– **Фонд «Дружественный Рунет»** (работа с подростковой аудиторией и образовательные проекты);

– **Российский центр реагирования на компьютерные инциденты (RU-CERT)**.

Основные проблемы в борьбе с противоправным контентом:

– **Технические сложности** – быстрый рост числа ресурсов, зеркал и анонимных каналов в мессенджерах.

– **Юрисдикционные ограничения** – иностранные площадки не всегда подчиняются российскому праву.

– **Размытые границы допустимого** – часть контента находится на грани дозволенного: например, сатирические материалы, мемы, ироничные комментарии или художественные произведения.

– **Социальный фактор** – многие пользователи (особенно подростки) сознательно игнорируют предупреждения о вредности определенных материалов и, наоборот, воспринимают запрет как повышение ценности.

– **Цифровая гигиена** – недостаток навыков критического восприятия информации у населения. По опросам ВЦИОМ (2024), лишь около 52 % россиян уверены, что способны отличить фейковую информацию от достоверной.

Для эффективного противодействия противоправному контенту необходимо сочетание мер: развитие законодательства,

технических инструментов блокировки, просветительских программ по цифровой гигиене и повышение уровня сотрудничества между государством, платформами и обществом.

1.5. Нормативные правовые документы, регламентирующие понятие «противоправный контент» в сети Интернет

В Российской Федерации действует ряд нормативных актов, регулирующих противодействие распространению противоправного контента. Основные:

1. **Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»** (ред. от 04.08.2023) устанавливает правовые основы противодействия экстремизму, включая ответственность за распространение экстремистских материалов в сети Интернет.

2. **Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»** (ред. от 01.05.2024) регулирует порядок ограничения доступа к противоправной информации, механизм блокировки сайтов, а также вводит институт организаторов распространения информации.

3. **Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»** (ред. от 30.12.2023) устанавливает возрастную маркировку информации, запрещает распространение материалов, опасных для несовершеннолетних (насилие, наркотики, порнография, пропаганда самоубийств).

4. **Федеральный закон от 2 декабря 2019 г. № 426-ФЗ** регулирует деятельность СМИ-иноагентов и ограничивает распространение финансируемого из-за рубежа контента.

5. **Федеральный закон от 1 декабря 2020 г. № 481-ФЗ** обязывает владельцев значимых интернет-ресурсов (с аудиторией более 500 тыс. пользователей в сутки) удалять противоправный контент в течение 24 часов.

6. **Федеральный закон от 4 марта 2022 г. № 32-ФЗ** устанавливает уголовную ответственность за дискредитацию действий Вооруженных Сил Российской Федерации.

7. **Федеральный закон от 28 апреля 2023 г. № 127-ФЗ** усиливает меры против фейковой информации о деятельности государственных органов, закрепляет возможность досудебной блокировки деструктивного контента.

Дополнительно применяются:

– **Уголовный кодекс Российской Федерации** (актуальная ред. 2025 г.): ст. 110 (доведение до самоубийства), ст. 146 (нарушение авторских прав), ст. 205.2 (призывы к терроризму), ст. 230 (склонение к употреблению наркотиков), ст.ст. 280–282 (экстремизм), ст. 354.1 (реабилитация нацизма).

– **Кодекс Российской Федерации об административных правонарушениях** (актуальная ред. 2025 г.): ст. 6.13 (пропаганда наркотиков), ст. 13.15 (злоупотребление свободой массовой информации), ст. 13.41 (неудаление запрещенной информации), ст.ст. 20.3 и 20.29 (пропаганда и распространение экстремистских материалов).

Таблица 11

Законодательное урегулирование разных видов деструктивного контента

Виды контента	Законодательная база
Депрессивный/ суицидальный	ФЗ № 436-ФЗ: ст. 5 (для несовершеннолетних); УК РФ: ст.ст. 110, 110.1; КоАП РФ: ст. 13.36
Экстремизм	ФЗ № 114-ФЗ: ст. 8; УК РФ: ст.ст. 280–282.4; КоАП РФ: ст.ст. 13.15, 20.3, 20.29, 20.33

Окончание табл. 11

Терроризм	УК РФ: ст.ст. 205.2, 205.4, 207.1, 208; КоАП РФ: ст. 13.37
Контент о самоубийствах/ «группах смерти»	ФЗ № 436-ФЗ: ст. 5; УК РФ: ст.ст. 110.1, 110.2; КоАП РФ: ст. 13.36
Шок-контент	ФЗ № 436-ФЗ: ст. 5 (ограничения для детей); КоАП РФ: ст. 13.41
Пропаганда наркотиков/ психотропов	ФЗ № 436-ФЗ: ст. 5; УК РФ: ст.ст. 230, 228.1; КоАП РФ: ст. 6.13

В 2024 г. по требованию Роскомнадзора было удалено и заблокировано более **704,8 тыс. интернет-страниц**, из которых 42,6 тыс. содержали экстремистский и террористический контент (ФЗ № 114-ФЗ).

Тогда же выявлено более **33,2 тыс. материалов, опасных для несовершеннолетних** (ФЗ № 436-ФЗ).

В 2025 г. вступили в силу поправки к ФЗ № 149-ФЗ, расширившие понятие информации, подлежащей ограничению: теперь под блокировку подпадают материалы, оправдывающие вандализм, а также деструктивные челленджи в соцсетях.

Для квалификации противоправного контента в сети Интернет применяются нормы как **уголовного**, так и **административного** законодательства. Ниже приведены основные статьи в актуальной редакции на 2025 г.

Уголовный кодекс Российской Федерации

– **Статьи 110, 110.1, 110.2 УК РФ** – доведение до самоубийства, склонение и содействие самоубийству, организация «групп смерти» (до 15 лет лишения свободы).

– **Статья 146 УК РФ** – нарушение авторских и смежных прав (плагиат, незаконное распространение контента).

– **Статья 205.2 УК РФ** – публичные призывы к террористической деятельности, публичное оправдание терроризма.

– **Статьи 207.1, 207.3 УК РФ** – заведомо ложная информация о терактах и действиях госорганов (фейк-ньюс, связанные с ЧС и ВС РФ).

– **Статьи 228.1, 230 УК РФ** – незаконный оборот и пропаганда наркотических средств, склонение к их употреблению.

– **Статьи 280–282.4 УК РФ** – призывы к экстремистской деятельности, возбуждение ненависти или вражды, организация экстремистского сообщества.

– **Статья 354.1 УК РФ** – реабилитация нацизма, распространение ложных сведений о деятельности СССР в годы Второй мировой войны.

Кодекс Российской Федерации об административных правонарушениях

– **Статья 6.13 КоАП РФ** – пропаганда наркотических средств, психотропных веществ.

– **Статья 13.15 КоАП РФ** – злоупотребление свободой массовой информации (штраф за распространение запрещенных материалов в СМИ и интернете).

– **Статья 13.36 КоАП РФ** – распространение информации о способах совершения самоубийства.

– **Статья 13.41 КоАП РФ** – нарушение порядка удаления запрещенной информации владельцем сайта или хостинг-провайдером.

– **Статья 20.3 КоАП РФ** – пропаганда и публичное демонстрирование нацистской и экстремистской символики.

– **Статья 20.29 КоАП РФ** – массовое распространение экстремистских материалов.

– **Статья 20.33 КоАП РФ** – деятельность иностранной или международной НПО, признанной нежелательной в Российской Федерации.

Таблица 12

Сопоставление видов противоправного контента и норм УК РФ и КоАП РФ

Вид противоправного контента	Основные статьи УК РФ	Основные статьи КоАП РФ
Экстремистский контент (призывы, материалы, символика)	280, 280.1, 280.2, 280.3, 280.4, 282, 282.1, 282.2, 282.4	13.15, 20.3, 20.29, 20.33
Террористическая пропаганда и оправдание терроризма	205.2, 207.1, 207.3, 208	13.37
Пропаганда наркотиков и психотропных веществ	228.1, 230	6.13
Самоубийство и склонение к нему («группы смерти», инструкции)	110, 110.1, 110.2	13.36
Деструктивный/шок-контент, травмирующий психику детей	110.2 (при причинении вреда детям)	13.36, 13.15 (в СМИ)
Пропаганда насилия, жестокости, буллинга	110.2, 282 (при наличии признаков возбуждения ненависти)	13.15, 20.3
Реабилитация нацизма	354.1	20.3.1
Фейковые новости, подрывающие общественный порядок	207.1, 207.3	13.15
Нарушение авторских и смежных прав (пиратский контент)	146	7.12
Нарушение неприкосновенности частной жизни (слив персональных данных, фото, переписок)	137	13.11, 13.14

§ 2. Методики выявления и раскрытия преступлений, связанных с распространением противоправного контента в сети Интернет

2.1. Общая характеристика

Распространение противоправного контента в цифровой среде – один из самых сложных вызовов для правоохранительных органов. В отличие от традиционных преступлений **цифровые следы эфемерны**: контент может быть удален в течение секунд, но уже успеет распространиться по сотням ресурсов и мессенджеров. Поэтому методики выявления и раскрытия подобных преступлений строятся на трех ключевых принципах:

– **оперативность** (реагирование в реальном времени);

– **комплексность** (технические, аналитические, правовые инструменты);

– **координация** (межведомственное и международное взаимодействие).

2.2. Основные направления методик

2.2.1. Мониторинг и автоматизированный анализ информации

– Использование систем Big Data и искусственного интеллекта (например, *Аналитическая платформа МВД России*, «Кибердозор»).

– Алгоритмы машинного обучения позволяют выявлять ключевые слова (взрывчатка, легкий заработок, флешмоб смерти), изображения (поиск запрещенных символов, сцен насилия) и паттерны поведения пользователей.

Инструменты:

– **OSINT** (Open Source Intelligence) – анализ открытых источников (форумы, соцсети, даркнет);

– **Image Reverse Search** – обратный поиск изображений (Google Images, TinEye, «Яндекс.Картинки»);

– **Digital Fingerprinting** – цифровые отпечатки файлов, позволяющие отследить копии и их распространение.

Пример: в 2024 г. благодаря системе мониторинга Роскомнадзора удалось выявить телеграм-канал с инструкциями по изготовлению взрывчатки: ИИ проанализировал связанный трафик и сопоставил его с ранее заблокированными сообществами.

2.2.2. Кибероперативная работа («цифровой агент под прикрытием»)

– Создание ловушечных аккаунтов для выявления групп, распространяющих противоправный контент.

– Внедрение сотрудников в закрытые чаты и даркнет-форумы.

– Использование методов **социальной инженерии** для выявления администраторов и активных участников.

Пример: в 2023 г. ФСБ России при участии МВД России провела операцию в даркнете, где выявили 15 администраторов сообществ, пропагандировавших наркотики через онлайн-игры.

2.2.3. Трассировка цифровых следов

– Лог-файлы и метаданные: анализ IP-адресов, cookies, отпечатков браузеров.

– Геолокация по сетевой активности (сравнение времени постинга и активности устройств).

– Анализ криптовалютных транзакций при оплате рекламы деструктивного контента.

Пример: в 2024 г. Следственный комитет раскрыл схему распространения детской порнографии через даркнет, отследив криптовалютные транзакции на биржах Binance и Exmo.

2.2.4. Правовые и процессуальные методики

– Оформление судебных запросов на предоставление данных владельцев аккаунтов (согласно ст. 186.1 УПК РФ – получение компьютерной информации).

– Взаимодействие с Роскомнадзором для оперативной блокировки ресурса.

– Международные запросы через Интерпол и Европол при размещении серверов за рубежом.

Пример: блокировка запрещенных сообществ «группы смерти» в «ВКонтакте» в 2022 г. велась через судебные решения и международные запросы к хостингам.

2.2.5. Экспертно-криминалистический анализ

– Лингвистическая экспертиза: определение признаков экстремизма, призывов к насилию, ксенофобии.

– Психолого-лингвистический анализ материалов, вовлекающих несовершеннолетних.

– Техническая экспертиза: восстановление удаленных данных, анализ скрытых слоев файлов (стеганография).

2.3. Креативные и инновационные подходы

– **Киберпатрули среди граждан** – инициативные группы студентов и активистов, которые фиксируют противоправный контент и передают данные в Роскомнадзор (аналог проекта Cyber Patrol в ЕС).

– **Геймификация мониторинга** – использование игровых приложений для вовлечения добровольцев в выявление подозрительных материалов.

– **Нейросетевые детекторы деструктива** – ИИ-системы, которые анализируют *эмоциональную окраску контента* (например, выявляют призывы к самоубийству в TikTok по депрессивным хэштегам).

– **Digital twin-методика**: создание цифрового двойника подозреваемого на основе его активности в соцсетях для прогнозирования его действий.

2.4. Этапы расследования преступлений

1. Выявление.

Системный мониторинг (ИИ, OSINT, киберпатруль).

Жалобы пользователей.

2. Фиксация доказательств.

Составление протокола осмотра сайта (ст. 164 УПК РФ).

Сохранение цифровых доказательств с помощью хеширования (MD5, SHA256).

3. Идентификация субъекта.

Анализ IP, e-mail, криптовалютных кошельков.

Использование биометрии (голос, лицо в видео).

4. Пресечение.

Оперативная блокировка ресурса.

Изъятие оборудования и арест подозреваемых.

5. Доказывание и квалификация.

Привязка к ст.ст. 205.2, 280, 110 УК РФ и др.

Назначение экспертиз (лингвистической, психолого-криминалистической).

2.5. Образная метафора

– Методики можно представить как **цифровую экологию**.

– Мониторинг – экологическая разведка (отслеживает загрязнение сети).

– Трассировка – анализ ДНК контента (выявляет источник).

– Блокировка – карантин (изолирует зараженные зоны сети).

– Экспертиза – лаборатория (подтверждает токсичность информации).

– Профилактика – вакцинация (создание позитивного контента, просветительские проекты).

§ 3. Пошаговый алгоритм выявления и раскрытия преступлений, связанных с распространением противоправного контента в сети Интернет

Раздел систематизирует комплекс практических приемов работы правоохранительных органов и уполномоченных организаций при обнаружении, квалификации, документировании, блокировании и раскрытии преступлений, осуществляемых посредством распространения противоправной информации в сети Интернет. Методики ориентированы на раннее обнаружение угроз, юридически корректную фиксацию доказательств, эффективное взаимодействие с платформами и оперативное пресечение.

3.1. Операционный конвейер расследования (сквозной алгоритм)

Расследование преступлений, связанных с распространением противоправного контента, строится как последовательный процесс. Он включает ряд взаимосвязанных этапов, каждый

из которых имеет собственные цели, задачи и инструменты.

Этапы можно представить, как «конвейер»:

Подготовка → Обнаружение → Проверка достоверности → Фиксация доказательств → Ограничение доступа → Оперативные мероприятия → Цифровая криминалистика → Аналитика и установление связей → Процессуальные решения → Профилактика.

Таблица 13

Этапы алгоритма

Этап	Цель	Основные действия	Инструменты	Результат
Подготовка	Создать условия для оперативного реагирования	Разработка инструкций, чек-листов, словарей ключевых слов и выражений, назначение ответственных лиц	Ведомственные регламенты, матрицы рисков	Готовность к реагированию
Обнаружение	Выявить противоправный контент на ранних стадиях	Мониторинг открытых источников, настройка оповещений по ключевым словам, прием жалоб от пользователей	Поисковые системы, автоматические боты, «горячие линии»	Сигналы о возможных нарушениях
Проверка и квалификация	Отличить противоправный Контент от допустимого	Проверка достоверности изображений и видео, юридическая оценка, лингвистический анализ	Сервисы обратного поиска изображений, картографические платформы, экспертные методики	Оценка правового статуса материала
Фиксация доказательств	Сохранить данные в неизменном виде	Скриншоты, сохранение страниц в архивах, фиксация метаданных и времени, хеширование файлов	Архиваторы, утилиты сохранения данных	Доказательная база с соблюдением правил хранения
Ограничение доступа	Прекратить распространение незаконных материалов	Уведомление администрации платформ, обращение в надзорные органы, судебные процедуры	Формы уведомлений, государственные реестры, судебные решения	Удаление или блокировка контента

Окончание табл. 13

Оперативные мероприятия	Установить участников и организаторов	Сбор информации, наблюдение, опросы, в рамках закона – оперативные эксперименты	Закон «Об ОРД», ведомственные инструкции	Определение причастных лиц
Цифровая криминалистика	Изъятие и исследование цифровых следов	Копирование носителей, извлечение логов, анализ переписки, исследование криптовалютных транзакций	Программные комплексы цифровой криминалистики	Трассировка действий и финансов
Аналитика и атрибуция	Выявить связи между аккаунтами и событиями	Построение сетевых графов, анализ времени активности, стилистический анализ текстов	Программы для сетевого анализа и статистики	Модель «кто, что, когда, где, каким образом и зачем»
Процессуальные решения	Придать делу юридическую форму	Подготовка экспертиз, уведомлений, ходатайств, обвинительных заключений	Экспертные учреждения, процессуальные формы	Судебное разбирательство
Профилактика	Снизить риск повторных нарушений	Информационные кампании, медиаграмотность, соглашения с платформами	Государственные программы, меморандумы	Снижение количества рецидивов

3.2. Подготовительный этап: инфраструктура и регламенты

На данном этапе создается система, которая позволяет реагировать на угрозы быстро и слаженно:

– формируется список ключевых слов, эвфемизмов и жаргонных выражений, которые чаще всего используются в противоправном контенте;

– составляется карта платформ и сообществ, включая мессенджеры и их зеркала;

– распределяются роли между сотрудниками: кто отслеживает информацию, кто проводит юридическую проверку, кто контактирует с платформами и надзорными органами;

– готовятся шаблоны документов и чек-листы фиксации нарушений.

3.3. Обнаружение: мониторинг открытых источников

Выявление противоправного контента осуществляется с помощью трех каналов:

1. **Автоматические уведомления** – системы поиска реагируют на ключевые слова, хэштеги или характерные фразы.
2. **Жалобы пользователей** – краудсорсинг, когда сами граждане сигнализируют о противоправных публикациях.
3. **Наблюдательные аккаунты** – специально созданные профили, которые встраиваются в группы и сообщества, чтобы фиксировать подозрительную активность.

3.4. Проверка достоверности и правовая квалификация

После выявления контента важно определить, действительно ли он противоправный. Для этого проводятся три вида проверки:

– **Контент**: анализ подлинности изображений, проверка даты и места съемки, установление контекста.

– **Аккаунт**: определение, является ли профиль реальным или созданным для массовой рассылки.

– **Сеть**: анализ координации действий. Если десятки аккаунтов публикуют одно и то же сообщение в одно и то же время, это признак организованной кампании.

Параллельно проводится юридическая оценка: определяется, подпадает ли материал под статьи законодательства об экстремизме, терроризме или вовлечении несовершеннолетних.

3.5. Фиксация цифровых доказательств и обеспечение их подлинности

После выявления противоправного контента необходимо зафиксировать его в таком виде, чтобы собранные материалы могли быть использованы в суде или в ходе следственных действий. Важно не просто сохранить картинку, а обеспечить доказательственную силу.

– Минимальный комплект данных для одного выявленного объекта должен включать:

– **URL-адрес** страницы или публикации;

– **дату и время фиксации** (как в местной зоне, так и по универсальному времени UTC);

– **скриншот** страницы, где виден полный интерфейс и публикация;

– **сохранение исходного кода страницы** (HTML или JSON-дамп) – это помогает доказать, что страница действительно содержала указанный контент;

– **хеш-суммы файлов** (например, SHA-256) – математический способ подтвердить неизменность данных после сохранения;

– **журнал действий** (кто и когда зафиксировал данные);

– **информацию об авторе или аккаунте** (ID-профиля, контактные данные, если доступны);

– **копии уведомлений** в адрес платформы или государственных органов.

Таблица 14

Чек-лист фиксации доказательств

Элемент	Инструменты/формат	Назначение
Скриншот	PNG + отметка времени	Визуальное подтверждение содержания страницы
Исходный код страницы	HTML/JSON	Фиксация внутренней структуры сайта
Медиафайлы	Оригиналы + метаданные	Сохранение следов (EXIF, контейнеры)
Хеш-суммы	SHA-256	Подтверждение подлинности и неизменности
Журнал действий	txt/pdf	Контроль за процессом фиксации
Данные пользователей	ID, ссылки на жалобы	Установление источников и свидетелей
Уведомления	Копии писем и форм	Подтверждение информирования платформ/органов

3.6. Ограничение доступа и блокировка

Когда противоправный контент подтвержден, необходимо прекратить его распространение. Это может происходить разными способами:

– обращение к администрации платформы с требованием удалить материал;

– направление официального уведомления в Роскомнадзор;

– подача иска или судебное решение о блокировке ресурса.

Результат: публикация удаляется или доступ к сайту ограничивается через государственные реестры.

3.7. Оперативно-разыскные мероприятия

На этом этапе правоохранительные органы пытаются установить личности организаторов и участников противоправной деятельности. Используются:

– наблюдение за активностью;

– опросы свидетелей и пользователей;

– оперативные эксперименты (например, контрольная закупка запрещенных материалов в сети).

Результат: появляются конкретные фигуранты, которых можно привлекать к ответственности.

3.8. Цифровая криминалистика

Это работа со всеми следами, которые оставляют преступники в цифровой среде:

– копирование и исследование жестких дисков и мобильных устройств;

– анализ логов и переписки;

– восстановление удаленных файлов;

– изучение криптовалютных транзакций.

Используются специальные операционные системы (например, Kali Linux, CAINE) и утилиты, которые позволяют не повредить оригинальные данные (write-blockers).

Результат: создается своеобразный цифровый портрет действий подозреваемого – где, когда и как он действовал.

3.9. Аналитика и атрибуция

После сбора фактов нужно объединить их в единую картину. Здесь применяются методы:

– построение сетевых графов (кто с кем связан);

– временной анализ (активность в определенные часы или даты);

– стилистический анализ текстов (узнавание авторского стиля).

Результат: формируется модель «кто – что – когда – где – каким способом – с какой целью».

3.10. Процессуальные решения

Материалы передаются в следственные органы, где формируются:

– экспертизы (лингвистические, психологические, компьютерные);

– ходатайства и обвинительные заключения;

– процессуальные документы для суда.

Результат: возбуждается уголовное или административное дело.

3.11. Профилактика и коммуникация

Последний этап направлен на то, чтобы подобные ситуации не повторялись, и включает:

– проведение информационных кампаний;

– обучение медиаграмотности;

– соглашения с платформами об оперативном удалении запрещенной информации.

Результат: снижение риска повторного распространения деструктивного контента и повышение уровня цифровой культуры общества.

§ 4. Методы выявления деструктивных информационных операций на их ранних стадиях в социальных сетях

Согласно Конвенции об обеспечении информационной безопасности ООН, информационная война – это межгосудар-

ственное противоборство в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам. Основным средством ведения таких войн являются информационные операции, которые направлены на достижение информационного превосходства путем воздействия на информационные системы противника и защиты собственных ресурсов. Главными целями любой информационной операции являются:

– максимальный охват аудитории деструктивным контентом;

– вовлечение пользователей в деструктивные события или социальные явления;

– побуждение к практическим действиям, например, участие в протестных акциях.

В качестве объектов воздействия как правило выступают:

– общество в целом (гражданское население, социальные группы, включая силовые структуры);

– государственные, экономические и социальные институты.

Сегодня именно социальные сети и мессенджеры стали основным полем боя в информационных войнах. На рис. 9.4.1 представлена типовая схема активной фазы информационной операции в социальной сети «ВКонтакте», при помощи которой размещение деструктивного контента производится путем публикации постов на сайтах пользователей и их сообществ, либо комментариев под контентом, размещенным другими пользователями.

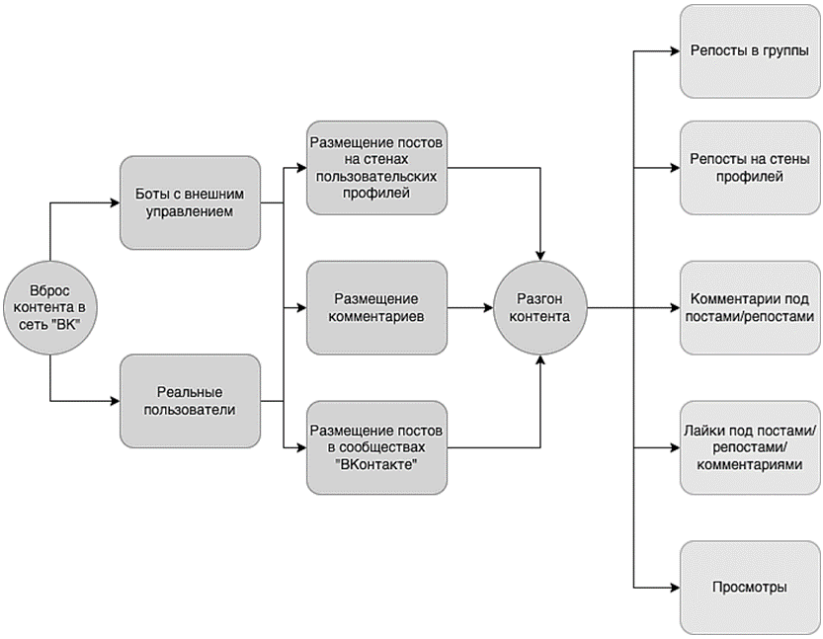


Рис. 9.4.1. Схема активной фазы информационной операции

Для начала процесса распространения целевого деструктивного контента необходимо сформировать в социальной сети первоисточник – пост. Первоисточник может содержать любую информацию (в том числе ссылки на контент, размещенный в других социальных сетях, видеохостингах, сайтах и т. д.). Он может быть размещен как реальным пользователем, так и ботом.

В зависимости от стратегии активной фазы информационной операции первоисточник может быть как открытым (к примеру, ютуб-канал), так и скрытым – первичный пост, как правило, удаляется после начала распространения информации с целью затруднения последующего расследования инцидента.

Кроме того, стратегия активной фазы информационной операции может предполагать наличие множества первоисточников.

Следующим этапом является этап активизации распространения контента. С этой целью используются репосты, комментарии, лайки и просмотры.

Особенностью реализации следующей фазы информационных операций – «**активизации аудитории**» – является применение технологической накрутки показателей контента с целью вывода его в тренды социальной сети. Если это удается, то доверие к нему повышается, и реальные пользователи более активно репостят, комментируют, просматривают и лайкают его, ускоряя распространение информации.

Поскольку типовая информационная операция включает фазу вброса и фазу разгона контента, то **основным элементом противодействия информационным операциям является выявление** информационной операции в фазе вброса контента, что позволяет существенно сократить время реагирования на нее и организовать противодействие ей на ранней стадии, не позволяя противнику достичь своих целей.

Основные признаки информационной операции:

– **рост количества публикаций** с похожим содержанием;

– **высокая частота публикаций** – контент появляется в короткие промежутки времени;

– **короткий временной интервал** между публикациями;

– **стремление к максимальному охвату аудитории** – контент активно распространяется, чтобы привлечь как можно больше пользователей.

Анализируя указанные признаки, можно определить, является ли всплеск активности в сети результатом организованной информационной кампании. Именно выявление этих закономерностей лежит в основе методик выявления информационных операций. Рассмотрим основные из таких методик.

Классический подход. Анализ числа сообщений определенной направленности в заданный промежуток времени позволяет выявить превышение некоего порогового значения, что свидетельствует о возможной информационной операции. Основным недостатком данного метода является эмпирический характер оценки порогового значения, которое зависит от многих факторов.

Для анализа зависимости объемов информационных потоков от времени рассматривается использование временных рядов, корреляционного анализа, анализа Фурье, вейвлет-анализа и фрактального анализа. Подобные подходы отчасти решают задачу выбора пороговых значений, однако имеют общий недостаток – метод требует анализа данных за продолжительный период, что затрудняет выявление операций на ранних стадиях.

Методика нечетких дубликатов. В основу метода заложен тот факт, что выявление информационных операций возможно в момент достижения максимального значения частоты публикаций нечетких дубликатов. В качестве признаков информационных операций используются некоторые метрики центральности и их соотношения для графов, состоящих из сообщений (вершин) и их взаимосвязей (ребер). Однако на выявление информационной операции требуется существенное время, включающее время ее активной фазы, а также время, необходимое на сбор и обработку информации.

Метод массового вброса. В основу метода взят тот факт, что достижение целей информационной операции возможно только в случае обеспечения максимального охвата аудитории в минимальные сроки. Следовательно, при проведении информационной операции должен наблюдаться одновременный массовый вброс целевого контента через множество каналов. При построении временного ряда, соответствующего такому массовому

вбросу, следует ожидать аномально высокую начальную частоту публикации дубликатов. Исходя из такого положения измерение начальной частоты публикации дубликатов и выявление ее аномальных значений позволяет существенно сократить период времени, необходимый для идентификации информационных операций.

Таблица 15

Технические методы

Метод	Суть	Пример применения
Сетевой мониторинг	Отслеживание активности пользователей, анализа частоты публикаций, связей между аккаунтами	Выявление ферм троллей через массовые одинаковые комментарии в Twitter
Автоматизированный контент-анализ	Использование NLP и ИИ для выявления агрессивных слов, триггерных фраз	Определение вбросов о массовых протестах через телеграм-каналы
Ботоводство-детекция	Алгоритмы выявления ботов по скорости постинга, однотипности текстов	Определение скоординированных кампаний в VK
Социально-сетевой анализ (SNA)	Построение графа связей между аккаунтами для выявления координаторов кампании	Анализ сетей влияния вокруг экстремистских сообществ
Анализ нарратива	Поиск повторяющихся сюжетов и ключевых смыслов	Определение ложных нарративов про массовые репрессии в соцсетях
Тренд-анализ	Сравнение скорости распространения информации с нормальными паттернами	Если тема растет экспоненциально за часы – сигнал о возможной операции

Когнитивные методы

Психолингвистический анализ: выявление эмоционально окрашенных слов, призывов к действию.

– **Выявление манипулятивных приемов**: апелляция к страху, стыду, агрессии.

– **Мем-детекция**: отслеживание визуальных мемов, используемых для вброса.

Пример: при кампании по дискредитации органов власти часто используются саркастические мемы. В выявление цепочек мемов помогает распознать раннюю стадию операции.

Социальные методы

– **Краудсорсинг**: вовлечение пользователей в жалобы на деструктивный контент.

– **Цифровые добровольцы**: инициативные группы (например, Лига безопасного интернета).

– **Медиаграмотность**: обучение граждан критическому мышлению.

Комбинированная схема выявления

Мониторинг ключевых слов/хэштегов → Построение сети связей → Сравнение с историческими паттернами → Анализ нарратива → Проверка через фактчекинг → Сигнал в центр мониторинга

Креативные методы

– Использование **ИИ-детекторов эмоций** для выявления панических и агрессивных сообщений.

– Анализ **цифровых следов**: временные паттерны (например, публикации в 03:00 по московскому времени → зарубежные координаторы).

– **Скрытая семантика**: выявление кода и жаргона (например, темные сленговые слова о наркотиках).

– **Симуляция атак**: моделирование вбросов и обучение ИИ выявлять их.

Учебно-методический раздел к главе 9

Цели изучения темы

1. Ознакомить студентов с понятием «контент» и его формами в цифровой среде.

2. Изучить виды противоправного (деструктивного) контента и угрозы, которые он несет обществу.

3. Освоить основные методы выявления и блокировки противоправных материалов в сети Интернет.

4. Понять роль нормативной правовой базы Российской Федерации в регулировании распространения противоправного контента.

5. Изучить алгоритм действий правоохранительных органов при расследовании преступлений, связанных с противоправным контентом.

6. Сформировать представление о современных цифровых инструментах мониторинга и фиксации интернет-материалов.

7. Развить навыки критического анализа информационных потоков и умение отделять деструктивный контент от легального.

8. Воспитать ответственное отношение к цифровой гигиене и безопасности в сети.

Вопросы для семинарского занятия

Теоретические вопросы

1. Что такое «контент» и каковы его основные формы и виды?

2. Какие существуют категории противоправного (деструктивного) контента?

3. В чем заключается опасность распространения деструктивных материалов для общества?

4. Какие проблемы выявления противоправного контента характерны для России и международной практики?

5. Какие нормативные правовые акты регулируют распространение противоправной информации в Российской Федерации?

6. В чем заключаются различия между американским, европейским и азиатским подходами к регулированию цифрового пространства?

7. Каковы этапы операционного конвейера расследования (подготовка, обнаружение, верификация, фиксация доказательств и др.)?

8. Какие цифровые инструменты применяются для мониторинга и выявления деструктивного контента?

9. Каковы принципы фиксации цифровых доказательств и почему важна цепочка хранения?

10. Какие профилактические меры позволяют снизить риски повторного распространения противоправного контента?

Варианты практических заданий

1. **Анализ интернет-материала.** Студентам предлагается выбрать пример публикации в социальных сетях и провести ее проверку: выявить признаки достоверности или деструктивности, указать правовую квалификацию.

2. **Моделирование расследования.** Группы студентов разрабатывают план действий при выявлении противоправного контента: от мониторинга до фиксации доказательств.

3. **Работа с инструментами OSINT.** Используя доступные сервисы (Google Images, Yandex.Картинки, WhoIs, Archive.org),

проверить выбранный материал на подлинность и подготовить отчет.

4. **Юридическая квалификация.** По примерам противоправных материалов определить статьи УК РФ и КоАП РФ, применимые к данному случаю.

5. **Проект «Инфокампания».** Студенты разрабатывают план профилактической кампании по медиаграмотности для молодежи, направленной на снижение воздействия деструктивного контента.

Иные формы обучения

– **Деловая игра** «Цифровой дозор». Студенты делятся на группы (аналитики, юристы, сотрудники МВД России, представители платформ), получают кейс с противоправным контентом и разрабатывают алгоритм его блокировки.

– **Мозговой штурм**: поиск новых способов раннего выявления фейков и деструктивных информационных операций.

– **Ролевая игра** «Суд над контентом». Одна группа выступает обвинением, доказывающим противоправность материала, другая – защитой.

– **Круглый стол**. Обсуждение эффективности действующих законов в сфере борьбы с противоправным контентом.

– **Тренинг по фиксации доказательств**: работа с чек-листами фиксации (скриншоты, дампы HTML, хеш-суммы).

– **Дискуссия** «Где грань между свободой слова и безопасностью общества?»

Библиографический список к главе 9

Нормативные правовые акты

1. Уголовный кодекс Российской Федерации : УК : принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 04.08.2025).

2. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_37867/ (дата обращения: 04.08.2025).

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 04.08.2025).

4. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 04.08.2025).

Монографии, книги, учебные и методические пособия, диссертации

5. Макаренко, С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века / С. И. Макаренко. – СПб. : Наукоемкие технологии, 2017.

6. Методическое пособие по выявлению признаков риска поведения в социальных медиа. – М. : Цифровая гигиена. Молодежь в сети, 2019.

7. Расторгуев, С. П. Информационные операции в сети Интернет / С. П. Расторгуев, М. В. Литвиненко, А. Б. Михайловский ; под ред. А. Б. Михайловского. – М. : АНО ЦСОиП, 2014.

8. Разуваев, Э. В. Правовые средства противостояния информационным войнам : автореф. дис. … канд. юрид. наук / Э. В. Разуваев. – М., 2007.

9. Смирнов, А. А. Формирование системы правового обеспечения информационно-психологической безопасности в Российской Федерации : дис. … д-ра юрид. наук / А. А. Смирнов. – М., 2022.

Статьи

10. Давидюк, Н. В. Интеллектуальный алгоритм идентификации деструктивной информации в тексте / Н. В. Давидюк, В. А. Гостюнина, Д. Р. Байдулова // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2019. – № 2. – С. 29–39.

11. Гайворонская, Я. В. Влияние деструктивного интернет-контента на правосознание молодежи / Я. В. Гайворонская, Ю. И. Каримова // Российский журнал правовых исследований. – 2020. – Т. 7. – № 4. – С. 19–26.

12. Жильцова, О. Н. Формирование контент-плана в социальных сетях / О. Н. Жильцова // Маркетинг и логистика. – 2019. – № 2 (22). – С. 32–37.

13. Минаев, В. А. Выявление информационных операций в социальных сетях на их ранних стадиях / В. А. Минаев, А. Н. Рабчевский, Я. Р. Мустакимова // Информация и безопасность. – 2022. – Т. 25. – № 4. – С. 485–494.

14. Пучинина, М. Ю. Механизм деятельности сторонников деструктивных интернет-сообществ и портрет их типичного участника (на примере «групп смерти» и движения «Колум-

байн») / М. Ю. Пучинина, А. В. Пучинин // Вестник Воронежского института МВД России. – 2021. – № 3. – С. 229–234.

15. Тельбух, В. В. Метод выявления деструктивного контента в информационных Интернет-ресурсах / [В. В. Тельбух и др.] // Известия ТулГУ. Технические науки. – 2023. – Вып. 3. – С. 55–63.

16. Тимофеев, С. В. Выявление и предупреждение преступлений в сети Интернет: проблемы и пути их решения / С. В. Тимофеев, Э. Ю. Пороховой // Вестник Восточно-Сибирского института МВД России. – 2021. – № 4 (99). – С. 220–229.

Электронные и аналитические отчеты

17. Динамика противоправного контента в Рунете за 2021–2024 годы: исследование НЦПТИ / [С. А. Чурилов и др.] // Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет [сайт]. – URL: https://ncpti.su/review/article/44 (дата обращения: 04.08.2025).

Глава 10. МЕТОДИКА ВЫЯВЛЕНИЯ И РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБОРОТОМ ОРУЖИЯ, С ИСПОЛЬЗОВАНИЕМ ОТКРЫТЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ

ВВЕДЕНИЕ

Незаконный оборот оружия представляет собой серьезную угрозу как для национальной безопасности Российской Федерации, так и для мирового сообщества в целом. Глобализация и цифровизация, которые упростили международные торговые и коммуникационные процессы, одновременно создали благоприятные условия для распространения оружия, боеприпасов, взрывчатых и отравляющих веществ, вследствие чего эта проблема затронула практически все регионы мира, включая нашу страну, и требует от правоохранительных органов применения современных методов борьбы с преступностью.

Особую сложность в раскрытии таких преступлений представляет их транснациональный характер и использование преступниками современных технологий. Сегодня незаконный оборот оружия все чаще осуществляется через интернет-платформы, мессенджеры и социальные сети, что требует от специалистов по анализу и защите информации новых подходов и методик.

Незаконный оборот оружия – это не только угроза общественной безопасности, но и вызов правоохранительным органам, требующий от них высокого уровня профессионализма, владения современными технологиями и глубокого понимания правовых норм.

§ 1. Нормативные правовые документы, регламентирующие понятие «оборот оружия» и «незаконный оборот оружия»

Международные правовые акты

Россия участвует в ряде международных соглашений, направленных на предотвращение незаконного оборота оружия, например:

– **Протокол ООН против незаконного изготовления и оборота огнестрельного оружия** (2001 г., к Конвенции ООН против транснациональной организованной преступности), закрепляет меры по лицензированию, маркировке и отслеживанию огнестрельного оружия.

– **Европейская конвенция о контроле за приобретением и хранением огнестрельного оружия частными лицами** (1978) устанавливает стандарты контроля и учета.

Эти акты ратифицированы Россией и применяются как часть национальной системы регулирования.

Федеральное законодательство

Федеральный закон от 13 декабря 1996 г. № 150-ФЗ «Об оружии» (ред. от 04.08.2023) содержит определение термина «оборот оружия», который включает производство, продажу, хранение, ношение, перевозку, использование, ввоз и вывоз оружия. В 2023-2024 гг. в закон внесены изменения, касающиеся:

– усиления контроля за оборотом травматического оружия;

– уточнения правил хранения и транспортировки;

– введения обязательной маркировки при ввозе оружия.

Уголовный кодекс Российской Федерации (гл. 24 «Преступления против общественной безопасности»):

– **статья 222 УК РФ** – незаконные приобретение, хранение, сбыт, перевозка и ношение оружия;

– **статья 222.1 УК РФ** – незаконный оборот взрывчатых веществ и устройств;

– **статья 223 УК РФ** – незаконное изготовление и ремонт оружия, взрывчатых веществ и устройств;

– **статья 224 УК РФ** – небрежное хранение оружия;

– **статья 225 УК РФ** – ненадлежащее исполнение обязанностей по охране оружия и боеприпасов;

– **статьи 226, 226.1 УК РФ** – хищение, вымогательство, контрабанда оружия, боеприпасов и ВВ.

КоАП РФ предусматривает следующую административную ответственность:

– **статья 20.8** – нарушение правил хранения, транспортирования, ношения оружия;

– **статья 20.10** – незаконное изготовление или продажа пневматического оружия;

– **статья 20.12** – незаконная пересылка оружия.

Постановления и подзаконные акты

– **Постановление Правительства Российской Федерации от 21 июля 1998 г. № 814 «О мерах по регулированию оборота гражданского и служебного оружия и патронов к нему»** (ред. от 2024 г.) – ключевой документ, устанавливающий порядок лицензирования, хранения, учета и транспортировки оружия.

– **Постановление Правительства Российской Федерации от 2 ноября 2000 г. № 838** о правилах оборота боевого ручного стрелкового оружия в государственных военизированных организациях.

– **Приказы МВД России** (последние изменения 2023–2024 гг.):

– № 621 от 12 октября 2009 г. («Об утверждении Административного регламента… по контролю за оборотом оружия» ред. 2023 г.);

– № 288 от 29 апреля 2019 г. «Об утверждении правил выдачи лицензий на приобретение оружия».

Судебная практика

– **Постановление Пленума Верховного Суда Российской Федерации от 12 марта 2002 г. № 5** (ред. от 2022 г.) разъясняет понятия «незаконное приобретение», «передача», «сбыт», «хранение», «перевозка», «ношение оружия».

– В 2023–2024 гг. суды активно рассматривали дела по ст.ст. 222 и 223 УК РФ, особенно в части незаконного приобретения оружия через даркнет и пересылки почтовыми отправлениями.

Особенности применения законодательства

– **Добровольная сдача оружия** (ст. 222 УК РФ, примечания) освобождает гражданина от уголовной ответственности.

– Субъект преступления – лицо с 16 лет (по отдельным статьям – с 14 лет).

– Установлена система компенсаций за добровольно сданное оружие (постановления региональных правительств).

На 2025 г. нормативная база оборота оружия в Российской Федерации включает **ФЗ № 150-ФЗ «Об оружии» (ред. 2023–2024 гг.), УК РФ (гл. 24), КоАП РФ (гл. 20), подзаконные акты Правительства и МВД России**. Она продолжает развиваться: в 2024 г. внесены изменения, ужесточающие ответственность за незаконный оборот взрывчатых веществ, а также уточняющие правила оборота травматического и охотничьего оружия.

Таким образом, законодательство обеспечивает комплексное регулирование оборота оружия: от легального приобретения до уголовного преследования за незаконные действия.

Таблица 16

Нормативные правовые акты, регулирующие оборот оружия

Уровень	Документ	Ключевые положения	Актуальность (на 2025 г.)
Международные акты	Протокол ООН против незаконного изготовления и оборота огнестрельного оружия (2001)	Лицензирование, маркировка, отслеживание оборота оружия; международное сотрудничество	Действует, Российская Федерация участвует, используется для гармонизации законодательства
	Европейская конвенция о контроле за приобретением и хранением огнестрельного оружия (1978)	Установлены стандарты контроля, учета и лицензирования оружия	Применяется как часть международных обязательств Российской Федерации
Федеральные законы	ФЗ от 13 декабря 1996 г. № 150-ФЗ «Об оружии» (ред. от 31.07.2025)	Определение оборота оружия (производство, продажа, хранение, транспортировка, использование, ввоз/вывоз). Установлен порядок лицензирования и контроля	Основной закон. Внесены изменения 2023–2024 гг. (усиление контроля за травматическим оружием, уточнение правил хранения и маркировки)
	ФЗ от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»	Используется в случаях оборота оружия, связанного с экстремизмом	Действует, применяется совместно с УК РФ
Уголовный кодекс Российской Федерации	Глава 24 УК РФ (ст.ст. 222–226.1)	Ответственность за незаконные приобретение, хранение, сбыт, перевозку, ношение, изготовление оружия, взрывчатых веществ, а также за хищение и контрабанду	В 2023-2024 гг. внесены изменения (усилены санкции по ст. 222.1, расширены признаки состава преступлений)

Окончание табл. 16

КоАП РФ	Ст.ст. 20.8, 20.10, 20.12 КоАП РФ	Административная ответственность за нарушения правил производства, хранения, перевозки, ношения и пересылки оружия	Действуют, уточнены в 2023 г. (например, по части пересылки и хранения)
Подзаконные акты	Постановление Правительства Российской Федерации от 21 июля 1998 г. № 814 (ред. 2024 г.)	Порядок лицензирования, хранения, учета и транспортировки оружия	Актуализировано в 2024 г. (усилены правила для частных охранных структур)
	Постановление Правительства Российской Федерации от 2 ноября 2000 г. № 838	Правила оборота боевого ручного стрелкового оружия в гос. военизированных организациях	Действует
	Приказ МВД России № 621 от 12.10.2009 (ред. 2023 г.)	Административный регламент по контролю за оборотом оружия	Действует, актуализирован
	Приказ МВД России № 288 от 29.04.2019	Правила выдачи лицензий на приобретение оружия	Действует
Судебные разъяснения	Постановление Пленума ВС РФ от 12 марта 2002 г. № 5 (ред. 2022 г.)	Разъяснение понятий: «незаконное приобретение», «передача», «сбыт», «хранение», «перевозка», «ношение оружия»	Актуально, применяется судами в 2024–2025 гг.

§ 2. Нормативные правовые документы, регламентирующие понятия «оборот оружия» и «незаконный оборот оружия» в сети Интернет

2.1. Понятие «оборот оружия»

Оборот оружия – это установленная законом деятельность по **созданию, передаче и использованию оружия**, которая строго регулируется государством.

В **Федеральном законе от 13 декабря 1996 г. № 150-ФЗ «Об оружии»** (ст. 1) прямо указано, что под оборотом оружия понимаются все стадии жизни оружия, начиная от его производства и заканчивая утилизацией.

К ним относятся:

– производство и ремонт;

– торговля и продажа;

– приобретение и передача;

– хранение и ношение;

– коллекционирование и экспонирование (например, в музеях);

– перевозка и транспортировка;

– использование (в охоте, спорте, самообороне);

– изъятие и уничтожение;

– ввоз и вывоз с территории Российской Федерации.

Другими словами, оборот – это **любое действие с оружием**, которое может совершаться только в рамках закона.

Пример: охотник покупает зарегистрированное ружье в магазине, хранит его в сейфе и использует по правилам охоты – это законный оборот оружия.

2.2. Понятие «незаконный оборот оружия»

Незаконный оборот оружия – это любые действия с оружием, боеприпасами или взрывчатыми веществами, совершенные **без разрешения или с нарушением установленных правил**.

В уголовно-правовом смысле это отражено в **ст.ст. 222–226.1 УК РФ**.

К незаконному обороту относятся:

– **незаконное приобретение** (покупка с рук, через интернет, обмен, получение в дар без лицензии);

– **незаконная передача** (передача другому лицу для временного пользования или хранения без разрешения);

– **незаконный сбыт** (продажа, дарение, обмен, окончательное отчуждение оружия);

– **незаконное хранение** (сокрытие в квартире, тайнике, гараже без регистрации);

– **незаконная перевозка** (транспортировка в машине, поезде, самолете без соответствующих документов);

– **незаконное ношение** (нахождение оружия при себе или в сумке без разрешения);

– **незаконное изготовление или переделка** (например, переделка травматического пистолета в боевой или изготовление самодельного оружия).

*Пример: гражданин заказал через даркнет детали для пистолета и собрал его дома – это **незаконное изготовление и хранение оружия** (ст.ст. 223 и 222 УК РФ).*

Ключевая разница

– **Оборот оружия** – нейтральный термин: это **все действия с оружием**, законные и незаконные.

– **Незаконный оборот оружия** – это только те действия, которые совершаются **в нарушение законодательства** (без лицензии, без регистрации, с преступными целями).

С развитием цифровых технологий оборот оружия получил новое измерение – **виртуальное пространство**, где преступники активно используют анонимность, мессенджеры и криптовалюты для торговли оружием и боеприпасами. В ответ законодательство Российской Федерации было дополнено нормами, прямо учитывающими использование сети Интернет как отягчающего признака.

Федеральные законы

1. Федеральный закон от 13 декабря 1996 г. № 150-ФЗ «Об оружии» (ред. 2023 г.):

– устанавливает порядок законного оборота оружия;

– запрещает незаконные схемы приобретения, сбыта и переделки оружия, в том числе через онлайн-площадки.

2. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»:

– используется при квалификации деяний, когда оборот оружия в сети сопровождается экстремистскими или террористическими призывами.

3. Федеральный закон от 1 июля 2021 г. № 281-ФЗ:

– внес ключевые изменения в УК РФ и УПК РФ;

– в ст.ст. 222, 222.1, 222.2 и 223 УК РФ добавлен новый квалифицирующий признак – использование информационно-телекоммуникационных сетей, включая Интернет;

– наказания ужесточены: например, незаконный сбыт оружия через Интернет карается лишением свободы до 8 лет, а при отягчающих обстоятельствах – свыше 10 лет.

Уголовный кодекс Российской Федерации

– **Статья 222 УК РФ** – незаконное приобретение, хранение, сбыт оружия, в том числе через Интернет.

– **Статья 222.1 УК РФ** – незаконный оборот взрывчатых веществ и устройств, включая виртуальные площадки.

– **Статья 223 УК РФ** – незаконное изготовление или переделка оружия (например, по онлайн-инструкциям).

– **Статья 226.1 УК РФ** – контрабанда оружия, включая пересылку через интернет-магазины и даркнет.

– **Статьи 205.2, 280, 280.1 УК РФ** – квалификация, если оружие используется в террористических или экстремистских целях, а его сбыт координируется в сети.

С 2021 г. **использование сети Интернет признано особо опасным способом** совершения этих преступлений, приравненным по тяжести к сбыту наркотиков онлайн.

Кодекс об административных правонарушениях Российской Федерации

– **Статья 20.8 КоАП РФ** – нарушение правил хранения, перевозки, учета оружия, в том числе с использованием интернет-сервисов.

– **Статья 20.10 КоАП РФ** – незаконная продажа пневматического оружия через сайты или мессенджеры.

– **Статьи 13.15 и 13.41 КоАП РФ** – ответственность СМИ и интернет-ресурсов за публикацию инструкций по переделке оружия или изготовлению взрывчатки.

Судебная практика

Суды активно применяют новые квалифицирующие признаки:

– **2020 г.** – приговор жителю Гусь-Хрустального за покупку деталей оружия через интернет;

– **2021 г.** – в Ярославле гражданин осужден за приобретение и модификацию травматического пистолета через онлайн-площадку;

– **2025 г.** – задержание подростков в Дагестане, которые пытались продать охолощенный пистолет Retey24, переделанный под боевые патроны, через мессенджер.

Международный аспект

– **Протокол ООН против незаконного изготовления и оборота огнестрельного оружия (2001)** обязывает страны бороться с онлайн-каналами сбыта.

– **Будапештская конвенция о киберпреступности (2001)** устанавливает базу для международного сотрудничества в расследовании преступлений, совершаемых через Интернет, включая торговлю оружием.

Таким образом, российское законодательство уже адаптировано к цифровой эпохе: использование Интернета при незаконном обороте оружия выделено как **отдельный квалифицирующий признак**. Но учитывая постоянное развитие даркнета и криптовалют, эксперты считают необходимым дальнейшее совершенствование норм, в частности внедрение систем **онлайн-трассировки сделок** и расширение международного взаимодействия.

§ 3. Незаконный оборот оружия с использованием открытых источников информации

Проблема появления на черном рынке оружия, не состоящего на государственном учете, стоит особенно остро. Это подтверждается рядом громких преступлений, совершенных в последние годы с применением штатных боеприпасов, взрывчатки, пистолетов и автоматов. Среди них: подрыв кафе в Воронеже

(апрель 2024 г.), нападение на сотрудников полиции в Подмосковье, подозреваемым в котором оказался участник наркосети, а также теракт в концертном зале «Крокус».

Правоохранительные органы фиксируют рост организованного незаконного оборота оружия, где действуют устойчивые преступные группы, использующие схожие схемы с наркоторговцами: тайники («закладки), конспирацию, распределение ролей и криптовалютные платежи.

3.1. Источники поступления оружия на черный рынок

На основе анализа оперативных данных можно выделить три основные категории оружия, попадающего в незаконный оборот:

1. **Черные копатели** – находки времен Великой Отечественной войны (винтовки, пистолеты, гранаты, боеприпасы). Часть из них приводится в рабочее состояние.

2. **Переделанное оружие** – изготовленное из газовых, сигнальных, травматических образцов или макетов (например, восстановление боевых свойств газового пистолета или охолощенного оружия).

3. **Оружие из зоны СВО** – основной поток незаконных поставок на конец 2024 г. Схемы предполагают перевозку через Ростовскую область или Крым, а конечным пунктом чаще всего становятся республики Северного Кавказа.

3.2. Организация каналов поставки

– Оружие провозится через блокпосты в разобранном виде.

– Используется система курьеров, когда каждый пассажир автобуса перевозит небольшую часть (например, один ствол или коробку патронов).

– Создаются схроны (тайники), доступ к координатам которых имеют только старшие в группировке.

– Часть поставок прикрывается действующими военными подразделениями.

По своей логистике такие каналы практически идентичны схемам наркотрафика: разветвленные цепочки, разделение функций и минимизация рисков для руководителей.

Кроме того, цены на нелегальном рынке становятся все более доступными, что создает угрозу попадания оружия не только в руки преступных сообществ, но и к обычным гражданам, которые приобретают его на всякий случай.

3.3. Схемы бесконтактного сбыта через интернет

В условиях цифровизации преступные группы активно используют **интернет и анонимные сервисы связи**. Схема обычно выглядит так:

– Размещение объявления о продаже оружия в мессенджерах, на форумах или в даркнете.

– Связь с покупателем через анонимные каналы (Telegram, WhatsApp, Viber и др.).

– Оплата криптовалютой или через электронные переводы без открытия банковского счета.

– Передача координат тайника (закладки) с фото и инструкциями.

Пример: «Нижегородская обл., г. Бор, ул. Кольцова, д. 4. Слева от дома – береза, у ее корней подкоп, в нем сверток».

Подобные схемы позволяют организаторам минимизировать риски: конечные исполнители (курьеры и закладчики) не знают руководителей и часто становятся единственными задержанными.

3.4. Проблемные аспекты

– Значительная часть оружия не числится в российских базах (например, украинские образцы), что осложняет баллистическую экспертизу и пулегильзотеку.

– Зарубежные сервисы мессенджеров и криптовалютные системы не подчиняются российской юрисдикции, что усложняет контроль.

– Растет число покупателей из числа обычных граждан, что увеличивает социальную опасность.

Таким образом, в настоящее время незаконный оборот оружия с использованием открытых источников информации становится **массовым, системным и высокоорганизованным явлением**, а его пресечение требует комплексного подхода: правового, технического и оперативно-разыскного.

§ 4. Торговля оружием в даркнета: методы выявления и противодействия

В XXI в. значительная часть незаконного оборота оружия переместилась в цифровую среду. Особое место занимает так называемый даркнет – сегмент Интернета, доступ к которому осуществляется через специализированные анонимизирующие сети, прежде всего **Tor (The Onion Router)**. В отличие от открытого Интернета, где сайты индексируются поисковыми системами и доступны по стандартным доменам, ресурсы даркнета функционируют на скрытых серверах и имеют адреса вида onion.

Для торговли оружием в даркнете преступники используют комбинацию трех ключевых технологий:

1) **анонимизирующие сети (Tor)** – позволяют скрывать IP-адреса и обеспечивают доступ к невидимым сайтам;

2) **криптографические протоколы** – симметричное и асимметричное шифрование применяются для защиты переписки;

3) **криптовалюты (Bitcoin и аналоги)** – позволяют проводить транзакции без привязки к личности.

Схема функционирования незаконной торговли оружием в даркнете

1. **Создание торговой площадки.** Продавец договаривается с администрацией даркнет-форума или маркетплейса о размещении объявлений.

2. **Размещение информации.** В объявлении указываются характеристики оружия, цена, фотографии, способы связи и **публичный ключ** для шифрования.

3. **Переговоры и согласование условий.** Общение ведется через зашифрованные каналы, недоступные для прослушивания.

4. **Участие гаранта.** Для снижения риска мошенничества в сделку вовлекается посредник – гарант. Покупатель переводит средства гаранту, который контролирует выполнение условий сделки.

5. **Оплата криптовалютой.** Чаще всего используется **Bitcoin**. Сумма переводится на кошелек гаранта, что делает оплату практически неотслеживаемой традиционными методами.

6. **Передача товара (закладка).** Продавец оставляет оружие в условленном месте (клад) и сообщает покупателю координаты.

7. **Финализация сделки.** После подтверждения получения товара гарант перечисляет деньги продавцу, удерживая комиссию (3–7 %).

Основные риски для участников

1. **Мошенничество** (например, продавец может прислать «воздух»).

2. **Утечка данных** при некачественном шифровании.

3. **Закрытие площадки** и исчезновение администрации с крупными суммами (пример: маркетплейс *Evolution* в 2015 г.).

Методы выявления незаконной торговли оружием

1. **Кибербразведка (OSINT и Darknet Monitoring):**

– использование поисковых систем даркнета (Ahmia, Torch);

– мониторинг маркетплейсов и форумов с ключевыми словами («AK-47», «Makarov», «grenade»).

2. **Инфильтрация сообществ:**

– создание «социальных ловушек» (фальшивых аккаунтов) для сбора информации о продавцах;

– участие в форумах и переписках под видом покупателей.

3. **Анализ блокчейн-транзакций:**

– применение инструментов **Chainalysis, Crystal Blockchain, Elliptic**, позволяющих отследить путь криптовалюты до точек обналичивания.

4. **Криминалистическая атрибуция:**

– сопоставление цифровых следов (метаданные фото, повторяющиеся PGP-ключи, стиль текста);

– выявление связей между аккаунтами через графовый анализ.

Противодействие

1. **Законодательные меры.** Федеральный закон от 1 июля 2021 г. № 281-ФЗ ввел квалифицирующий признак – совершение преступления с использованием сети Интернет. По ст. 222 УК РФ незаконный сбыт оружия через Интернет относится к особо тяжким преступлениям (наказание – до 8 лет лишения свободы, в ряде случаев – свыше 10 лет).

2. **Международное сотрудничество.** Россия участвует в программах Интерпола и ООН по контролю за нелегальным оружием и его цифровыми каналами оборота.

3. **Технические меры:**

– внедрение автоматизированных систем мониторинга даркнета;

– сотрудничество с криптобиржами и финмониторингом (Росфинмониторинг);

– развитие отечественных платформ для анализа блокчейна.

4. **Профилактика:**

– информационные кампании о рисках и наказании;

– стимулирование добровольной сдачи оружия;

– развитие цифровой грамотности, чтобы пользователи могли отличать легальные ресурсы от нелегальных.

§ 5. Методика выявления и раскрытия преступлений, связанных с незаконным оборотом оружия с использованием сети Интернет

5.1. Цели, правовая основа и зоны ответственности

Цель: своевременно обнаруживать, юридически грамотно фиксировать и пресекать интернет-сбыт оружия/боеприпасов/ВВ/ВУ с доведением до процессуального результата.

Правовая основа (базово):

– Федеральный закон № 150-ФЗ «Об оружии» (режим оборота, термины, запреты);

– Федеральный закон № 144-ФЗ «Об оперативно-розыскной деятельности» (основания, виды ОРМ, пределы вмешательства);

– Федеральный закон № 149-ФЗ «Об информации…» (ограничение доступа, взаимодействие с платформами);

– Федеральный закон № 115-ФЗ (ПОД/ФТ: финансовая разведка, мониторинг операций);

– УК РФ (ст.ст. 222, 222.1, 222.2, 223, 226.1 и квалифицирующий признак «с использованием ИКТ»);

– УПК РФ (процессуальные основания изъятий, экспертиз, международных запросов).

Роли: аналитик (OSINT/мониторинг), оперативный сотрудник (ОРД), следователь (процесс), криминалист (цифровая и баллистическая экспертизы), специалист по блокчейн-трассировке, юрист (квалификация, санкции суда), связной по платформам/Роскомнадзору/Интерполу.

5.2. Сквозной алгоритм (от сигнала до профилактики)

Таблица 17

Алгоритм профилактики

Этап	Вопрос	Что делаем	Выход
1. Подготовка	Готовы ли мы реагировать «здесь и сейчас»?	SOP, чек-листы, шаблоны запросов/уведомлений, словарь триггеров, таблица контактных точек (РКН, платформы, провайдеры, ЭЦП)	Организационная готовность
2. Обнаружение	Где первые следы?	Непрерывный мониторинг (поверхностная сеть, форумы, маркетплейсы, Telegram/мессенджеры, даркнет), поступающие жалобы	Сырой сигнал/инцидент
3. Верификация и квалификация	Это про оружие и это незаконно?	Проверка подлинности (описания/фото/видео), оценка по 150-ФЗ/УК РФ, отделение копии/муляжи/охолощенки от боевого	Предварительная правовая оценка

Окончание табл. 17

4. Фиксация доказательств	Как это сохранить, чтобы выдержало суд?	Скриншоты+штамп времени, дамп HTML/JSON, выгрузка медиа с метаданными, хеш-суммы, журнал действий, архивирование	Доказательственный пакет с цепочкой хранения
5. Ограничение распространения	Как быстро прекратить доступ?	Уведомление платформы, направление в РКН/прокуратуру, судебная блокировка/ограничение	Удаление/блокировка
6. ОРМ	Кто за этим стоит?	Наблюдение, опросы, проверочная закупка в рамках закона, контрольная поставка/пересылка, ИКТ-ОРМ	Идентификация фигурантов
7. Цифровая криминалистика	Где цифровые следы?	Изъятие устройств, форензика, сетевые логи, данные провайдеров, профили мессенджеров	Трассировка действий
8. Финансы/крипто	Как проходят деньги?	Росфинмониторинг, платежные системы, блокчейн-аналитика, запросы к обменникам/биржам	Связка «аккаунт – кошелек – человек»
9. Аналитика и атрибуция	Как связаны аккаунты/люди/события?	Соцсетевой анализ, хронология, геосопоставление, баллистика	Модель дела («кто – что – где – когда – как – зачем»)
10. Процесс	Как довести до приговора?	Экспертизы, уведомления, задержания, обыски, предъявление обвинения	Процессуальный результат
11. Профилактика	Как снизить риск рецидива?	Инфокампании, взаимодействие с платформами, черные списки торговцев, контрольные закупки	Снижение инцидентности

5.3. Обнаружение (мониторинг) и ранняя фильтрация

5.3.1. Карта мониторинга

– **Поверхностная сеть:** доски объявлений, региональные форумы, барахолки, соцсети и группы (продам/обменяю), маркетплейсы.

– **Полузакрытые среды:** телеграм-каналы/чаты, тематические сообщества в VK/форумы с допуском.

– **Даркнет (Tor):** маркетплейсы, форумы, эскроу-сервисы.

– **Сопутствующие цепочки:** мастера по переделке/охолощению, инструкции, поставки комплектующих, логистика/закладки.

5.3.2. Триггеры (якорные признаки) для первичного отбора

– **Лексика:** «ствол», «ствол рабочий», «без доков», «переход на боевые», «комплект», «в наличии цинк», «АПС/ТТ/ПМ», «сувенир/муляж» при явной боевой геометрии.

– **Визуальные признаки:** серийные/клейма, следы снятия маркировки, патроны военного образца, фото «комплекта» (оружие+патроны+магазины).

– **Финансы/логистика:** криптовалюты/эскроу, «гарант», «закладка», «оплата через…», «только личка/мессенджер», сомнительные «пункты отправки».

5.3.3.Матрица первичного риска (триаж)

Таблица 18

Матрица первичного риска

Признак	Низкий	Средний	Высокий
Тип предмета	Пневматика/ муляж	Охолощенное/ сигнальное с сомнениями	Явные боевые образцы/ВВ/ВУ
Документы	Есть, проверяемые	Заявлены, но не подтверждены	«Без доков»/«нашел»
Платеж	безнал/нал	ЭПС без KYC	Крипто+эскроу
Локация	Магазин/тир	Частные лица	Маршруты «по СЗФО/ ЮФО/Кавказ/ с приграничьем»
Коммуникация	Открытая	Только личка	Только Tor/PGP/ эскроу

Комбинация ≥ 2 высоких признаков → немедленная верификация и фиксация.

5.4. Верификация и правовая квалификация

1. Контент-проверка:

– сопоставление фото с открытыми каталогами/базами (модель/калибр);

– анализ EXIF/видеокадров (если доступны);

– выявление красных флагов: боеприпасы, патроны, магазины, признаки боевых ЗИП.

2. Аккаунт-проверка:

– органический/неорганический профиль (дата, связи, активность);

– копипаст по тексту/фото в других местах;

– связь с мастерами/гарантами.

3. Юридическая оценка:

– **ст.ст. 222, 222.1, 223, 226.1 УК РФ** по предмету и фазе деяния;

– квалифицирующий признак **«с использованием ИКТ»**;

– при наличии – **признаки группы/организованной группы**, вовлечение несовершеннолетних, контрабанды.

Результат: решение о запуске фиксации и ОРМ/процессуальных действий или о прекращении (если предмет легален).

5.5. Фиксация цифровых доказательств (чек-лист)

Таблица 19

Фиксация цифровых доказательств

Элемент	Чем фиксируем	Почему это важно
URL + дата/время (локально и UTC)	Журнал фиксации, тайм-штамп	Привязка ко времени/ юрисдикции
Скриншот страницы	PNG/PDF целиком	Визуальная привязка контента

Окончание табл. 19

Исходный код	Сохранение HTML/ JSON	Доказательство содержимого под капотом
Медиа	Оригинальные файлы (без перекодирования)	Сохранение exif/ контейнера
Хеш-суммы	SHA-256 всех файлов	Неизменность артефактов
Данные профиля	ID, описания, контакты	Идентификация субъекта
Свидетельские данные	Номера жалоб/ обращений	Независимое подтверждение
Уведомления	Копии обращений на платформы/в РКН/ прокуратуру	Демонстрация добросовестных действий

Все помещается в структурированный пакет дела, цепочка хранения документируется (кто / что / когда / как сохранил).

5.6. Ограничение распространения: тактика быстрого реагирования

– **Линия 1:** уведомление платформы / администратора сообщества по их форме (с приложением правовой квалификации и артефактов).

– **Линия 2:** направление материалов в Роскомнадзор/прокуратуру (№ 149-ФЗ, основания ограничения доступа).

– **Линия 3:** судебное решение о блокировке/удалении (если требуется принудительный характер).

– **Линия 4 (параллельно):** ОРМ и форензика для установления фигурантов – блокировка не должна спугнуть приоритетную разработку.

5.7. ОРМ и контрольные действия в цифровой среде

– **Проверочная закупка / контрольная поставка** – строго в рамках 144-ФЗ и внутриведомственных регламентов; документируется «от и до».

– **Внедрение / работа под легендой** – с оценкой рисков и правовой защиты сотрудников.

– **Перехват на логистике** – закладки, курьеры, пункты выдачи; взаимодействие с почтовыми/курьерскими операторами по закону.

– **Дистанционные ИКТ-мероприятия** – получение компьютерной информации, снятие информации с технических каналов связи – при наличии оснований и санкций.

5.8. Цифровая криминалистика и сетевые следы

– **Идентификаторы:** IP (сессии, провайдер, время), при возможности – **MAC** (локальные сети/изъятые устройства), отпечатки браузера/клиента.

– **NAT/VPN/Tor:** учитывается сложность привязки. Компенсации: временная корреляция, провайдерские логи, поведенческие паттерны, анализ выходных узлов Tor, сопоставление с чистыми сессиями фигуранта.

– **Изъятие и исследование:** живой ответ (live-response) при обыске, затем полный образ носителей (forensic image), поиск артефактов мессенджеров, кошельков, PGP-ключей, эскроу-аккаунтов, файлов-инструкций, истории переделок.

5.9. Финансовая и криптовалютная составляющая

– **Традиционные ЭПС/банки:** запросы в платежные системы, **Росфинмониторинг** (115-ФЗ), построение графов переводов, идентификация звеньев обналичивания.

– **Криптовалюты:**

– первичная атрибуция по адресам из переписки/квитанций;

– кластеризация и маркировка (биржи, миксеры, P2P-сервисы);

– **триаж трансакций**: крупные входы/выходы, быстрые сквозные переводы, контакт с сервисами, имеющими KYC;

– запросы в обменники/биржи (особенно при фиат-выводе).

Цель: связать платеж с человеком (момент KYC/вывода, пересечение с офлайном).

Таблица 20

Триаж крипто-операций

Признак	Риск
Ввод с биржи → один хоп → эскроу	Высокий
Регулярные мелкие транши с P2P	Средний
Вывод на биржу с KYC	Шанс на deanonymization

5.10. Атрибуция и аналитическая сборка дела

– **Соцсетевой анализ**: связи между аккаунтами, гарантами, мастерами, каналами логистики; роли в группе.

– **Хронология:** от первых постов/переписок до транзакций/закладок/изъятий.

– **География:** места фото, маршруты отправки, окна активности по часовым поясам.

– **Баллистика и криминалистика:** связывание изъятого оружия/боеприпасов с преступлениями, выявление переделок, происхождения деталей.

5.11. Процессуальные решения и экспертизы

Экспертизы: баллистическая, трасологическая, компьютерно-техническая (аппаратная/программная/информационная/сетевая), лингвистическая (смысл переписки/намерения).

Процесс: ходатайства об обысках/выемках, задержания, предъявление обвинения, обеспечение доказательств, воз-

можные международные запросы (по действующим каналам МВД России/Интерпола/двусторонним соглашениям).

Фокус: сохранность цепочки хранения, воспроизводимость экспертиз, корректная квалификация (включая признак ИКТ и организованную группу).

5.12. Профилактика и устойчивое подавление каналов

– **Техническое:** соглашения с платформами о быстрых треках блокирования и выдачи данных по законным запросам, фильтры на оружейные маркеры, автоматизированная аналитика.

– **Организационное:** межведомственная группа (МВД России – РКН – Росфинмониторинг – таможня – почтовые операторы), регулярные контрольные закупки.

– **Общественное:** горячие линии, анонимные формы сообщений, кампании медиаграмотности (как распознать незаконные предложения).

– **Отраслевое:** работа с обменниками/биржами (KYC, флаги подозрительных паттернов), магазинами реплик/охолощенки (разъяснения, комплаенс).

5.13. Три практических плейбука

А. Телеграм-канал «продам/обменяю».

1. Мониторинг → верификация по триаж-матрице → фиксация.

2. Одновременные запросы: платформе (удаление/данные админа), провайдеру (IP-сессии), ЭПС/крипто.

3. ОРМ (проверочная закупка/контрольная поставка) → задержание при передаче/закладке.

В. Даркнет-маркет с эскроу.

1. Профиль продавца (история сделок/PGP/адреса), фиксация витрин и переписки.

2. Эскроу-адреса → блокчейн-трассировка → точки KYC.

3. Совместные действия с правообладателями/хостерами/правоохранением (по действующим каналам) → снятие площадки/арест админов, параллельно – разработка продавцов.

С. Мастер по переделке (офлайн-цех).

1. Отработка клиентов/чатов → заказные цепочки.

2. Обыски, изъятия станков/деталей/ТТК, экспертиза переделок.

3. Квалификация по ст. 223 УК РФ (+ группа/доход/ИКТ).

5.14. Ключевые риски и способы их снижения

– **Преждевременная блокировка** (срыв разработки) → план двух дорожек: фиксация/ОРМ до уведомления платформ.

– **Шифрование/анонимизация** → комбинирование источников: время/место, финансы, поведенческие маркеры, ошибки **OPSEC** (операционной безопасности) → мелкие проколы: логин в другой сервис с тем же ником, случайное использование реального IP, публикация фото с метаданными, личные детали в сообщениях («у меня сегодня снег», «иду на пары» и т. п.).

– **Рассеивание ответственности (курьеры/закладчики)** → доведение до организаторов: финансы, управление каналами, складские адреса, гаранты.

– **Международные элементы** → раннее подключение международных каналов, заморозка на биржах в момент вывода.

Таблица 21

Приложение А

Мини-таблица: какие данные у кого запрашивать (по закону)

Контрагент	Тип данных	Основание
Платформа/ мессенджер	Регистрационные атрибуты, IP-сессии, логи доступа, данные администрирования канала	149-ФЗ, процессуальные нормы, запрос правоохранительных органов
Провайдер связи	Сведения о соединениях/сессиях, учетные данные абонента	126-ФЗ «О связи», процессуальные нормы
ЭПС/банк	Сведения об операциях/связанных счетах	115-ФЗ, процессуальные нормы
Биржа/ обменник	KYC, история по адресам, ордера	Законодательство юрисдикции биржи, международные запросы

Приложение В

Чек-лист следователя/оперативника на стол

1. **Сигнал/линк** → фиксация по чек-листу.
2. **Правовая оценка** (150-ФЗ, УК РФ, признак ИКТ).
3. **Решение о блокировке** (согласованное с планом ОРМ).
4. **Комплект запросов**: платформа/провайдер/ЭПС/биржа.
5. **ОРМ-план**: закупка/закладка/логистика/задержание.
6. **Форензика**: изъятие устройств, образы, пароли/ключи, кошельки.
7. **Экспертизы**: баллистика, КТЭ, лингвистика.
8. **Финансы/крипто**: граф переводов, точки KYC/обнал.
9. **Атрибуция**: SNA-граф, хронология, география.
10. **Процесс/обвинение**: корректная квалификация, доказательственная база.
11. **Профилактика**: информирование, повторные проверки, взаимодействие с платформами.

Библиографический список к главе 10

Нормативные правовые акты

1. Кодекс Российской Федерации об административных правонарушениях : КоАП : принят Государственной Думой 20 декабря 2001 г. : одобрен Советом Федерации 26 декабря 2001 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 04.08.2025).

2. Уголовный кодекс Российской Федерации : УК : принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 04.08.2025).

3. Федеральный закон от 13 декабря 1996 № 150-ФЗ «Об оружии» // Собрание законодательства Российской Федерации. 1996. № 51. Ст. 5681.

Книги, учебники, монографии

4. Беляков, А. А. Современные методы выявления и расследования преступлений в сфере компьютерной информации : монография / А. А. Беляков. – М. : Проспект, 2023.

5. Вехов, В. Б. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебник для вузов / В. Б. Вехов ; отв. ред. С. В. Зуев, В. Б. Вехов. – М. : Юрайт, 2025.

6. Егоров, Н. Н. Криминалистика цифрового следа : учебное пособие / Н. Н. Егоров ; под ред. Н. Н. Егорова. – СПб. : Питер, 2022.

7. Филиппов, А. Г. Актуальные проблемы борьбы с киберпреступностью: сборник научных статей / под ред. А. Г. Филиппова. – М. : Юрлитинформ, 2020.

Диссертации

8. Григорянц, С. А. Незаконный оборот оружия, боеприпасов, взрывчатых веществ и взрывных устройств как объект криминологического исследования : дис. … канд. юрид. наук : 12.00.08 / Григорянц Сергей Анушаванович. – Ростов н/Д.: Ростовский юридический институт МВД России, 2011.

Статьи в журналах

9. Азимов, П. Б. Незаконный оборот оружия в Российской Федерации / П. Б. Азимов // Молодой ученый. – 2020. – № 23 (313). – С. 179–181.

10. Винокуров, А. И. Киберпреступность, связанная с онлайн-торговлей / А. И. Винокуров // Молодой ученый. – 2022. – № 48 (443). – С. 217–219.

11. Загайнова, Ю. В. К вопросу о понятии незаконного оборота оружия / Ю. В. Загайнова // Вестник Восточно-Сибирского института МВД России. – 2012. – № 3 (62). – С. 36–41.

12. Макейкина, Е. В. Проблемы противодействия незаконному обороту оружия на современном этапе / Е. В. Макейкина // Актуальные вопросы юриспруденции : сборник статей. – Пенза, 2020. – С. 130–132.

13. Степаненко, Д. А. О некоторых аспектах расследования преступлений в сфере компьютерной информации / Д. А. Степаненко // Вестник Восточно-Сибирского института МВД России. – 2024. – № 3.

14. Грибунов, О. П. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / О. П. Грибунов, Э. В. Лантух, В. С. Ишигеев // Всероссийский криминологический журнал. – 2020. – Т. 14. – № 6. – С. 882–890.

Материалы конференций и сборников

15. Жубрин, Р. В. Некоторые проблемы противодействия незаконному обороту оружия / Р. В. Жубрин // Противодействие незаконному обороту оружия в России : сборник материалов круглого стола (Москва, 25 сентября 2019 г.). – М. : Университет прокуратуры Российской Федерации, 2020. – С. 53–61.

СМИ и интернет-ресурсы

16. Фалалеев, М. Ищите ствол в Сети / М. Фалалеев // Российская газета. – 2019. – 25 дек.

Глава 11. МЕТОДЫ И СРЕДСТВА ОПРЕДЕЛЕНИЯ КОНФИГУРАЦИИ СЕТИ. ПЕРЕХВАТ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО СЕТИ. МОНИТОРИНГ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

ВВЕДЕНИЕ

Современные информационные технологии (ИТ) стремительно развиваются, что приводит к значительным изменениям в подходах к построению и управлению информационно-телекоммуникационными сетями (ИТКС). Сегодня мы наблюдаем активную интеграцию сетей связи с компьютерными системами, а также появление сложных распределенных сетей, которые охватывают такие направления, как интернет вещей (IoT), умные города, умные дома и умные производства.

Эти технологии, основанные на концепции «Индустрия 4.0», используют стек протоколов TCP/IP и сети нового поколения (NGN), что делает их гибкими и масштабируемыми, но одновременно и более уязвимыми к угрозам.

Одной из ключевых задач в таких сетях является обеспечение их функциональной надежности и безопасности. Современные ИТКС представляют собой сложные системы, состоящие из множества элементов: каналов связи, узлов коммутации, серверов и систем управления. Для поддержания их стабильной работы требуется постоянный мониторинг и оперативное управление сетевыми ресурсами. Это особенно важно для сетей, обслуживающих критически важные инфраструктуры (КВИ), такие как энергетика, транспорт или здравоохранение, где сбои могут привести к катастрофическим последствиям.

В этом контексте методы и средства определения конфигурации сети, а также перехвата информации играют важнейшую роль. Они позволяют не только диагностировать текущее состояние сети, но и выявлять потенциальные угрозы, предотвращая атаки и минимизируя риски.

В данном разделе мы рассмотрим, как современные технологии мониторинга и анализа сетевого трафика помогают обеспечивать безопасность и надежность ИТКС, а также какие инструменты и подходы используются для защиты данных от несанкционированного доступа, обсудим, как развитие технологий «Индустрии 4.0» и интернета вещей влияет на требования к сетевой безопасности и какие вызовы это создает для специалистов по защите информации.

Понимание этих аспектов позволит не только эффективно управлять сетевыми ресурсами, но и предотвращать потенциальные угрозы, обеспечивая стабильную работу критически важных систем.

§ 1. Общие и основные особенности мониторинга в информационно-телекоммуникационных сетях

1.1. Понятие мониторинга

Мониторинг в информационно-телекоммуникационных сетях (ИТКС) – это **постоянный процесс наблюдения и анализа состояния сети**, который позволяет своевременно выявлять отклонения в ее работе и предотвращать сбои.

Согласно ГОСТ Р 27.102–2021, мониторинг технического состояния (ТС) – это **наблюдение за объектом с целью получения информации о его текущем состоянии и рабочих параметрах**. В применении к ИТКС это означает, что под контролем должны находиться:

– оборудование (маршрутизаторы, коммутаторы, серверы, рабочие станции, точки доступа Wi-Fi);

– каналы связи (их пропускная способность, задержки, потери пакетов);

– сетевой трафик (объемы, направления, подозрительная активность);

– показатели производительности и безопасности.

1.2. Задачи мониторинга

Мониторинг решает одновременно несколько групп задач:

1. Обеспечение бесперебойной работы сети:

– контроль загруженности каналов;

– обнаружение перегрузок и узких мест;

– выявление аппаратных и программных сбоев.

2. Информационная безопасность:

– фиксация попыток несанкционированного доступа;

– выявление аномалий трафика (DDoS-атаки, сканирование портов, подозрительные соединения);

– предупреждение утечек данных.

3. Управление сетью и планирование развития:

– сбор статистики по использованию ресурсов;

– прогнозирование нагрузки;

– принятие решений о модернизации инфраструктуры.

4. Соблюдение нормативных требований. Во многих случаях мониторинг обязателен для организаций. Например, международные стандарты PCI DSS, HIPAA, FISMA, SOX, а также российские нормы в сфере защиты персональных данных и КИИ (критической информационной инфраструктуры) предусматривают обязательное использование мониторинга.

1.3. Преимущества мониторинга

– **Видимость сети**. Администратор получает полную картину работы: от уровня отдельного устройства до глобальных связей между сегментами сети.

– **Предотвращение простоев**. Аварии легче предупредить, чем ликвидировать: система оповещает о сбое до того, как он затронет пользователей.

– **Быстрое устранение проблем**. С помощью сетевых карт и логов можно точно установить, где произошла ошибка.

– **Обнаружение угроз безопасности**. Мониторинг выявляет нетипичные сценарии: слишком частые запросы к серверу, аномальные объемы загрузки данных, подозрительные IP-адреса.

– **Упрощение управления**. Большие сети сложно контролировать вручную; мониторинг автоматизирует сбор данных и сводит их в удобные отчеты.

1.4. Особенности мониторинга гетерогенных ИТКС

Современные ИТКС отличаются **разнородностью**:

– разные операционные системы (Windows, Linux, Cisco IOS и др.);

– разные протоколы связи (Ethernet, Wi-Fi, MPLS, VPN, LTE/5G);

– разные модели безопасности;

– разные принципы администрирования (ведомственные, корпоративные, государственные).

Отсюда возникают ключевые особенности мониторинга:

1. **Децентрализация**. Нет единого центра, контролирующего все; мониторинг строится многоуровневым образом.

2. **Гибкость и адаптивность**. Система должна подстраиваться под динамику нагрузки и архитектуру сети.

3. **Межведомственный характер**. Для государственных сетей мониторинг должен учитывать согласование интересов разных структур.

4. **Сложности математического моделирования**. Невозможно описать такую сеть единой формулой; нужны распределенные методы анализа.

1.5. Виды состояний сети по Международному союзу электросвязи (МСЭ)

В рекомендации М.3703 выделяет следующие состояния сети:

– **U (Неопределенное)** – статус определить невозможно;

– **N (Норма)** – сеть функционирует стабильно;

– **I (Незначительное нарушение)** – небольшие сбои, не влияющие на пользователей;

– **J (Значительное нарушение)** – серьезные проблемы, есть риск перебоев;

– **C (Критическое)** – состояние, близкое к аварии;

– **F (Авария)** – сеть не выполняет свои функции.

– В конечном виде для лица, принимающего решения, остаются два базовых состояния:

– «Норма» (работает);

– «Авария» (не работает).

1.6. Триггерный механизм (метод гистерезиса)

Одной из проблем мониторинга является так называемый **дребезг нуля** – многократная генерация аварийных сигналов при колебаниях параметров около порогового значения.

Метод гистерезиса решает эту проблему:

– задаются два порога – **возрастающий** и **убывающий**;

– событие фиксируется только при переходе через верхний порог;

– новое событие возникает лишь после снижения параметра ниже нижнего порога.

Пример: температура сервера. Если задать пороги 80 °C (верхний) и 70 °C (нижний), система сгенерирует тревогу только при превышении 80 °C и снимет ее, когда температура упадет ниже 70 °C. Это позволяет избежать лишних уведомлений.

1.7. Ключевые метрики и пороговые значения

Чтобы мониторинг был измеримым, заранее фиксируют набор метрик и порогов для тревог.

Сетевые метрики:

– **Доступность (Availability), %** – доля успешных ответов на ping/health-check. Порог: < 99,9 % (критично для ЦОД/КИИ), < 99,5 % (критично для офисной сети).

– **Задержка (Latency), мс** – время туда-обратно (RTT). Порог: LAN < 2–5 мс; WAN внутри региона < 30–40 мс; межрегионально < 80–120 мс.

– **Потери пакетов (Packet Loss), %** – доля потерянных пакетов. Порог: > 0,5 % (для VoIP/видео уже заметно), > 2% (критично).

– **Джиттер (Jitter), мс** – разброс задержек. Порог: > 20–30 мс (для голоса/видео – проблема).

– **Загрузка интерфейса, %** – текущая утилизация порта/канала. Порог: устойчиво > 80–85 % (нужна разгрузка/апгрейд).

– **Ошибки/дропа на интерфейсах** – CRC, input/output errors. Порог: рост на порядок к базовой линии за интервал наблюдения.

Серверные/прикладные метрики:

– **CPU load, %** – > 85–90 % устойчиво → признак узкого места / «утечки».

– **RAM, % свободно** – < 10–15 % длительно → риск свопинга/тормозов.

– **Диск (IOPS/Latency)** – рост задержек чтения/записи > 10–15 мс на SSD и > 20–30 мс на HDD.

– **Время ответа сервиса (APM), мс** – SLO/SLA-пороги (например, p95 <300 мс).

– **Ошибки приложений (error rate)** – рост 4xx/5xx, исключений.

Безопасность:

– **Аномальные аутентификации** – частые неудачные логины, входы из необычных стран/ASN.

– **Сканирование портов / подозрительные соединения** – всплески SYN/UDP, рост talkers.

– **Объемы исходящего трафика** – ночные пики, нетипичные направления (эксфильтрация).

Практика: пороги задают двухступенчато – предупреждение (warning) и авария (critical) + гистерезис. Базовую линию (baseline) считают за 2–4 недели нормальной работы.

1.8. Архитектуры систем мониторинга

Агентская модель. На узлы ставят агенты (Zabbix Agent, WMI/Telegraf), которые собирают метрики и шлют на сервер. Плюсы: детально, безопасные pull/push-каналы, низкая зависимость от SNMP. Минусы: управление агентами, обновления.

Безагентная (SNMP/ICMP/HTTP-checks). Опрос по стандартным протоколам. Плюсы: быстро стартовать, минимум

вмешательства. Минусы: меньше глубины; зависит от настроек SNMP/ACL.

Гибридная (рекомендуется для гетерогенных ИТКС). Комбинация: SNMP + агенты + NetFlow/sFlow + syslog/SIEM.

Централизованная vs распределенная.

– Централизованная – один / пара ЦУ (head-end), удобно управлять, риск единой точки отказа.

– Распределенная – региональные/ведомственные коллекторы, локальная корреляция, агрегация в центр (подходит межведомственным сетям и КИИ).

Хранилище и визуализация TSDB (Prometheus, InfluxDB), поисковый стек (ELK/Opensearch), графики (Grafana), SIEM (QRadar/ArcSight/Splunk).

1.9. Жизненный цикл инцидента (ITIL-совместимо)

1. **Обнаружение** (alert по порогу/корреляции/сигнатуре).
2. **Регистрация** (тикет, приоритет P1–P4, SLA).
3. **Классификация и маршрутизация** (сеть/ сервер/безопасность).
4. **Диагностика** (проверки, трассировки, лог-анализ, гипотеза).
5. **Эскалация** (если требуется – к L2/L3/вендору).
6. **Восстановление** (обходной путь/фикс/rollback).
7. **Закрытие** (верификация нормальной работы).
8. **Post-Incident Review** (урок, корректировка порогов, знаниевая база).

§ 2. Характеристики, виды и формы мониторинга в информационно-телекоммуникационных сетях

2.1. Активный и пассивный мониторинг

Активный мониторинг – это когда в сеть специально вбрасываются тестовые пакеты или запросы.

– Пример: пинг до сервера или имитация обращения клиента к веб-приложению.

– Плюсы: можно заранее проверить доступность и скорость ответа.

– Минусы: дополнительные пакеты нагружают сеть, а иногда сам тест становится шумом.

Пассивный мониторинг – это когда мы только наблюдаем, не вмешиваясь в трафик.

– Пример: считывание статистики с портов коммутатора или анализ уже прошедших пакетов.

– Плюсы: никак не влияет на работу сети.

– Минусы: глазами пользователя не всегда видно, жив ли сервис.

Активный мониторинг похож на контрольный звонок врачу: «Алло, слышите меня?», а пассивный – на медицинский анализ крови: он ничего не меняет, но дает картину состояния.

2.2. Основные формы дублирования трафика

Мониторинг невозможен без копии трафика. Для этого используют:

1. **Зеркалирование портов (SPAN-порт).** Коммутатор дублирует весь трафик с выбранного порта на зеркальный.

Простой метод, встроен почти в каждое оборудование.

Минус: при большом трафике могут теряться пакеты.

2. **TAP-устройства (Test Access Port).** Физически врезаются в линию, создавая разветвление.

Пассивные – простые, надежные, не требуют питания (но ограничены скоростью).

Активные – работают на гигабитах и выше, но добавляют микрозадержку.

3. **NIC в режиме мониторинга (inline-мост).** Компьютер с двумя сетевыми картами ставится в разрыв линии.

Позволяет гибко анализировать, фильтровать трафик.

Минус: если компьютер выйдет из строя, сеть прервется.

4. **NIC с функцией обхода (bypass).** Даже при сбое питания сохраняется прямое соединение.

Повышает надежность, но привязывает устройство к месту установки.

2.3. Методы анализа трафика

1. **Захват пакетов (Packet Capture).**

Используются программы (Wireshark, tcpdump).

Можно анализировать в реальном времени или сохранять PCAP-файлы.

Часто применяется для расследования инцидентов.

2. **Глубокая инспекция пакетов (Deep Packet Inspection, DPI).**

Изучает не только заголовки, но и содержимое.

Два подхода:

Сопоставление с шаблонами – ищем конкретные последовательности (сигнатуры).

Анализ на основе событий – пакеты превращаются в «события», которые анализируются скриптами.

Применяется в системах IDS/IPS (обнаружение/предотвращение вторжений).

3. **Анализ потоков (Flow Monitoring).**

RFC 7011: поток = все пакеты с одинаковыми IP-адресами источника и назначения, портами и протоколом за определенный период.

Методы: NetFlow, sFlow, IPFIX.

Плюсы: меньше нагрузка, чем при DPI; не нарушает приватность, так как данные пользователей не сохраняются.

Минус: нет глубины содержания – видны только «кто, куда и сколько».

Таблица 22

Сравнительные характеристики методов

Метод	Что видно	Преимущества	Ограничения
SPAN-порт	Все пакеты с конкретного порта	Простота	Потери при высокой нагрузке
TAP	Трафик линии	Надежность, полная копия	Дорого, нужна установка
NIC inline	Трафик линии	Гибкость анализа	Риск прерывания
Capture (PCAP)	Полный пакет	Детальный анализ	Огромные объемы данных
DPI	Заголовки + содержимое	Обнаружение атак, фильтрация	Высокая нагрузка на систему
Flow	Только заголовки	Быстро, экономично	Нет содержания, только метаданные

2.5. Живой пример

Представим: в офисе сотрудники жалуются, что интернет тормозит.

– **Пассивный мониторинг через NetFlow** показывает: 70 % трафика уходит на один IP в Азии.

– **Захват пакетов** подтверждает: это не бизнес-приложение, а торрент.

– **Решение:** включить DPI и заблокировать по сигнатуре.

2.6. Выводы

– Мониторинг сети всегда начинается с **копирования трафика**, а дальше – выбор метода анализа.

– **Пакетный анализ (PCAP, DPI)** нужен для глубокой экспертизы.

– **Поточный анализ (Flow)** удобен для постоянного мониторинга и выявления аномалий.

– **Активный мониторинг** помогает увидеть глазами пользователя.

– В реальных сетях почти всегда комбинируют методы: Flow для широкой картины + DPI/PCAP для точечной диагностики.

§ 3. Технологии мониторинга в информационно-телекоммуникационных сетях

Современные сети – это сложные и разветвленные структуры, объединяющие десятки и сотни устройств, серверов и каналов связи. Их стабильная работа напрямую зависит от качества мониторинга. Однако универсального инструмента (на все случаи жизни) не существует. Каждая система имеет свои сильные стороны и ограничения. Чтобы лучше разобраться, рассмотрим несколько популярных решений, применяемых в IT-инфраструктурах.

Таблица 23

Сравнение базовых возможностей систем

Система	Особенности	Приеимущества	Недостатки
SCOM	Корпоративный продукт Microsoft, интегрированный с Windows-инфраструктурой и виртуализацией	Высокая производительность, удобная визуализация, поддержка PowerShell, интеграция с другими продуктами Microsoft	Ограниченная поддержка не-Windows систем, высокая стоимость, сложность настройки
Zabbix	Бесплатное решение с открытым кодом, поддерживающее распределенный мониторинг	Автоматическое обнаружение устройств, гибкая настройка, поддержка разных ОС	Сложная конфигурация, необходимость агентов, слабая интеграция с AD
Nagios	Классика open-source мониторинга, основанная на плагинах	Простая архитектура расширений, гибкость, поддержка удаленного мониторинга	Ограниченный функционал «из коробки», необходимость плагинов, проблемы с Windows
Cacti	Простое приложение для визуализации метрик с использованием RRDtool	Удобные графики, быстрый запуск, поддержка MySQL+PHP	Ограниченные возможности при сложных метриках, падение производительности в больших сетях
OSS	Решения для операторов связи (HP OpenView, Huawei U2000 и др.)	Централизованное управление сетью, высокий уровень защиты, интеграция с оборудованием	Очень дорогие, требуют большой команды специалистов
SRE / SLA	Современный подход, ориентированный на качество услуг и доступность сервисов	Контроль метрик SLA (SLI, SLO, RPO, RTO), снижение простоев, ориентация на бизнес-результат	Сложность внедрения, требует изменения организационных процессов

SCOM (System Center Operations) Manager можно сравнить с «центральным пультом управления» для больших компаний. Он особенно эффективен там, где уже развернута Windows-ин-

фраструктура и Microsoft-сервисы. Преимущество – интеграция с виртуальными машинами и облаками, но цена и сложность настройки делают его решением для крупных организаций.

Zabbix – «швейцарский нож» среди бесплатных систем мониторинга. Он подходит как для бизнеса, так и для госструктур. Его любят за универсальность и поддержку разных платформ. Но нужно помнить: новичкам Zabbix кажется слишком сложным, интерфейс перегружен настройками.

Nagios называют конструктором: возможности напрямую зависят от набора установленных плагинов. Если правильно собрать систему, она будет надежным инструментом для администрирования. Но «из коробки» Nagios простоват, и без расширений пользоваться им неудобно.

Cacti отлично справляется с визуализацией. Если нужно просто построить графики нагрузки на процессор, память или канал связи, он идеален. Однако для анализа атак или сложных аномалий его возможностей недостаточно.

OSS-системы – это уже тяжелая артиллерия. Они используются в телекоммуникационных компаниях и государственных структурах для тотального контроля над сетью. Их главный плюс – централизованность и высокая защита. Но стоимость и требования к персоналу делают их недоступными для малого бизнеса.

SRE и **SLA**-мониторинг – эти технологии фокусируются не на «железе», а на качестве предоставляемых услуг. В центре внимания – пользователь. Важны не сами устройства, а то, насколько стабильно клиент получает доступ к интернету, сервису или приложению. Такой подход постепенно вытесняет классические методы, особенно в компаниях, где все оценивается через призму бизнес-результата.

Таблица 24

Сравнение расширенных параметров

Система	Масштабируемость	Стоимость	Простота внедрения	Уровень безопасности
SCOM	Очень высокая (ЦОД, корпорации)	$$$ (дорого)	Низкая (сложная настройка)	Высокий
Zabbix	Высокая (1000+ узлов)	$ (бесплатно)	Средняя (много параметров)	Средний
Nagios	Средняя (зависит от плагинов)	$ (бесплатно)	Средняя (нужна практика)	Средний
Cacti	Средняя (для малых и средних сетей)	$ (бесплатно)	Высокая (быстрый старт)	Низкий
OSS	Очень высокая (на уровне операторов)	$$$$ (очень дорого)	Низкая (нужна команда)	Очень высокий
SRE / SLA	Гибкая (зависит от архитектуры)	$$–$$$	Низкая (меняет процессы)	Высокий

Итог: каждая система по-своему уникальна. SCOM больше подходит для крупных корпораций с Windows-инфраструктурой, Zabbix универсален и подходит для гибкого распределенного мониторинга, Nagios считается конструктором благодаря плагинам, Cacti отлично визуализирует метрики, OSS-системы применяются телекоммуникационными компаниями, а SRE/SLA делают акцент на качестве услуг.

Выбор системы мониторинга зависит от задач и масштаба организации. Для малого бизнеса подойдут простые решения вроде Cacti, для среднего бизнеса – Zabbix и Nagios, а для крупных корпораций – SCOM или OSS. Современный тренд все больше смещается в сторону SLA-ориентированных технологий, где главным показателем является не работа оборудования, а качество предоставляемой услуги.

§ 4. Методики мониторинга (пошагово, как делать)

4.1. Базовая проверка доступности (ICMP + маршрут)

Цель: быстро понять, жив ли узел и где обрыв.

Шаги:

1. ping <адрес> – 5–10 эхо-запросов, фиксируем RTT/потери.
2. traceroute/tracert – выявить, на каком хопе сбой/рост задержки.
3. Проверить ARP/MAC-таблицу на ближнем коммутаторе (MAC-флап/петля).
4. Снять интерфейсную статистику (show interfaces): errors/drops/CRC.
5. Сверить с картой сети/резервным маршрутом (ECMP/HSRP/VRRP).

Результат: локализован участок и тип сбоя (канал/петля/деградация).

4.2. SNMP-опрос оборудования

Цель: видеть здоровье портов/температуры/вентиляторов/питания.

Шаги:

1. Включить SNMPv3 (аутентификация/шифрование), ограничить ACL.
2. На сервере мониторинга задать шаблоны устройств (OID, опрос 30–60 с).
3. Визуализировать загрузку портов, ошибки, температуру, PSU/FAN статус.
4. Пороги: порт > 85 % 10 мин – warning; > 95 % 5 мин – critical.

5. Настроить оповещения и авто-тикеты.

Результат: превентивно видим перегрузки и умирающее «железо».

4.3. Анализ трафика потоков (NetFlow/sFlow/IPFIX)

Цель: кто/куда/сколько и чем нагружает сеть; выявить аномалии/утечки. **Шаги**:

1. Включить экспорт NetFlow/sFlow на граничных/ядро-устройствах на коллектор.

2. Настроить агрегацию потоков по 5-tuple (src/dst IP/port, протокол).

3. Завести базовые отчеты: Top talkers, Top destinations, приложения, ASN.

4. Пороги/правила: ночной исходящий пик> базовой линии ×2 – alert; новые внешние подсети – наблюдение; всплеск 443/QUIC – проверка.

5. Коррелировать с пользовательскими событиями (SIEM).

Результат: быстро находим «прожорливые» узлы и возможные каналы утечки.

4.4. Лог-мониторинг и корреляция (SIEM)

Цель: видеть скрытые инциденты и цепочки событий.

Шаги:

1. Централизовать логи: syslog из сетевого оборудования, Windows Event, Linux journald, прокси/веб-серверы, VPN, IAM.

2. Нормализовать (CEF/LEEF), обогащать (GeoIP, каталоги пользователей).

3. Правила корреляции:

– ≥ 5 неудачных логинов за 2 минуты + вход – риск брутфорса;

– смена привилегий + большой исходящий трафик – риск эксфильтрации;

– массовые 404/500 + аномальный POST – попытка эксплуатации.

4. Настроить реакцию: оповещение, автоблокировка учетки/адреса (где допустимо).

5. Еженедельно – разбор фалс-позитивов и доводка правил.

Результат: сокращение времени обнаружения инцидентов (MTTD).

4.5. APM и синтетические проверки сервисов

Цель: убедиться, что для пользователя все работает быстро.

Шаги:

1. Задать критические сценарии: логин, поиск, оплата, загрузка отчета.

2. Настроить синтетические транзакции (каждые 5–10 мин, из разных точек).

3. Собрать трассировки (Distributed Tracing) – где теряется время: фронт/бэкенд/БД.

4. Пороги: p95 ответа сценария < 300–500 мс; rate ошибок < 1–2 %.

5. При деградации – авто-тикет с прикрепленной трассой/логами.

Результат: проблемы ловятся до жалоб пользователей.

4.6. SLA/SLO и отчетность

Цель: фиксировать качество услуги и выполнять регуляторные/договорные требования.

Шаги:

1. Описать SLO (цели) и SLA (обязательства) по сервисам: доступность, время реакции.

2. Считать аптайм по календарям бизнес-времени, учитывать плановые окна.

3. Строить ежемесячные отчеты: аптайм, MTTR/MTTD, инциденты по причинам.

4. Ретроспектива: что улучшили, какие пороги/правила скорректированы.

Результат: управляемый сервис с прозрачными метриками.

4.7. Пример: как это выглядит на практике

Симптом: утром пользователи жалуются: «почта и CRM открываются медленно».

Действия:

1. Дашборд «Здоровье сервисов»: p95 ответа CRM ↑ с 250 до 1200 мс; email IMAP/SMTP – в норме, но веб-доступ OWA медленнее.

2. NetFlow: ночной исходящий трафик из сегмента CRM-DB вырос ×3, активные соединения к внешнему S3-провайдеру.

3. APM-трасса: задержка на запросах к БД, очереди диска ↑.

4. SNMP: у сторедж-массива выросла латентность диска, одновременно бэкап-джоб оверран до рабочего времени.

5. Решение: сдвинуть окно резервного копирования, включить QoS/IO-throttling для бэкапа.

6. Контроль: метрики вернулись к baseline; отчет, корректировка расписания, правило в мониторинге – алерт при перекрытии бэкапа и бизнес-часов.

Вывод: проблема была не в сети, а в конкуренции за дисковую подсистему; комплексный мониторинг позволил это быстро доказать.

4.8. Настройка SPAN-порта (зеркалирование трафика)

Цель: Получить копию трафика с выбранного порта коммутатора для анализа.

Шаги:

1. Определить порт коммутатора, к которому подключено устройство (например, сервер).
2. Подключить анализатор (ноутбук с Wireshark) к свободному порту коммутатора.
3. Войти в настройки коммутатора (обычно через CLI или web-интерфейс).
4. Указать, какой порт будет зеркалироваться (source), и какой порт будет получать копию (destination).
5. Запустить Wireshark на ноутбуке и проверить, идут ли пакеты.
6. При необходимости ограничить зеркалирование (например, только входящий или исходящий трафик).

Результат: поток пакетов в реальном времени доступен для анализа.

4.9. Использование TAP-устройства

Цель: Получить независимую копию трафика без нагрузки на коммутатор.

Шаги:

1. Установить TAP в разрыв линии (между сервером и коммутатором).
2. Подключить ноутбук с анализатором к TAP-порту.
3. Запустить программу анализа (Wireshark или tcpdump).
4. Проверить, что виден весь трафик обоих направлений.
5. Зафиксировать данные (например, сохранить PCAP-файл).

Результат: полный трафик линии, включая служебные пакеты, доступен для детального изучения.

4.10. Захват пакетов в Wireshark

Цель: Изучить содержимое пакетов и выявить аномалии.

Шаги:

1. Установить Wireshark (бесплатно, доступно на Windows/Linux).

2. Запустить программу, выбрать нужный сетевой интерфейс.

3. Нажать Start Capture и наблюдать за потоками пакетов.

4. Использовать фильтры (например, ip.addr == 192.168.1.5 или tcp.port == 80).

5. Найти подозрительные пакеты (например, большое число SYN-запросов → возможная атака).

6. Сохранить захваченные данные в формате PCAP для последующего анализа.

Результат: полная картина сетевого трафика, вплоть до содержания пакетов.

4.11. Использование NetFlow / sFlow (поточный мониторинг)

Цель: Получить статистику по потокам данных без глубокого анализа пакетов.

Шаги:

1. Убедиться, что маршрутизатор или коммутатор поддерживает NetFlow (или sFlow).

2. Включить экспорт NetFlow на устройстве (например, Cisco: ip flow-export destination 192.168.1.10 2055).

3. Установить на отдельный сервер анализатор NetFlow (например, nfdump или ntopng).

4. Настроить прием данных на этом сервере.

5. В интерфейсе анализатора посмотреть статистику:

– кто потребляет больше всего трафика;

– какие IP-адреса общаются чаще всего;

– какие протоколы занимают полосу.

Результат: видимость сетевых потоков: кто, куда и сколько.

4.12. DPI-анализ (глубокая инспекция пакетов)

Цель: Обнаружить вредоносную активность (вирусы, запрещенные протоколы, нелегальный контент).

Шаги:

1. Развернуть систему IDS/IPS (например, Suricata или Snort).

2. Настроить источник трафика (SPAN-порт, TAP или зеркалирование).

3. Подключить систему IDS к этому трафику.

4. Включить правила анализа (сигнатуры).

5. Система автоматически выделит:

– подозрительные соединения;

– попытки сканирования портов;

– вредоносные файлы.

6. Настроить отчеты и уведомления (email, syslog).

Результат: автоматическое выявление угроз в сетевом трафике.

4.13. Активный мониторинг (имитация работы пользователя)

Цель: Проверить доступность и скорость работы сервисов.

Шаги:

1. Установить специализированную систему (например, Zabbix, Nagios или PRTG).

2. Настроить пинги до ключевых серверов и маршрутизаторов.

3. Настроить проверки:

– HTTP (работает ли сайт);

– SMTP (отправляется ли почта);

– DNS (корректно ли разрешаются имена).

4. Задать пороги (например, задержка > 200 мс – тревога).

5. Настроить оповещения (email, Telegram-бот).

Результат: администратор получает сигнал о проблеме раньше, чем пользователи.

Примерная ситуация «Подозрительный трафик в сети университета»

В университете работает компьютерная сеть:

– есть сервер с базой данных студентов;

– несколько десятков компьютеров в аудиториях;

– Wi-Fi для преподавателей и студентов;

– маршрутизатор, через который сеть выходит в интернет.

Один из сотрудников IT-службы заметил, что вечером нагрузка на интернет-канал остается очень высокой, хотя занятия уже закончились и компьютеры должны быть выключены.

Этапы мониторинга и расследования

Этап 1. Подготовка

IT-служба использует систему мониторинга **Zabbix** и настроила сбор данных о трафике через протокол **NetFlow** на маршрутизаторе.

– Это значит, что каждый пакет данных (как письмо в конверте) фиксируется: откуда, куда и сколько.

– Для удобства настроены оповещения: если нагрузка превышает 80 % канала, приходит уведомление администратору.

Этап 2. Обнаружение

Администратор вечером получает уведомление: «Загрузка интернет-канала 90 %».

Он открывает панель мониторинга и видит:

– с одного компьютера в аудитории № 305 идет большой поток данных;

– нагрузка сохраняется уже более 2 часов.

Этап 3. Верификация

С помощью системы **Wireshark** администратор подключается к зеркальному порту коммутатора и анализирует пакеты.

– Он замечает, что трафик идtt на зарубежные IP-адреса, которые связаны с облачным хранилищем.

– Формат файлов – архивы .rar и .zip.

– Это указывает на возможную **утечку данных** или использование компьютера для теневой деятельности.

Этап 4. Фиксация доказательств

Чтобы bct выглядело как доказательство:

1. Сохраняются логи маршрутизатора.
2. Делается дамп пакетов (Wireshark → .pcap файл).
3. Все файлы подписываются электронной подписью и фиксируются контрольными суммами (SHA-256), чтобы их нельзя было подделать.

Этап 5. Ограничение доступа

Администратор временно отключает проблемный компьютер от сети, чтобы прекратить передачу данных.

Этап 6. Расследование

После отключения выясняется:

– компьютер принадлежит студенту, который остался в аудитории и установил нелицензионное ПО для майнинга криптовалюты;

– программа использовала ресурсы сети для передачи результатов на сервер за границей.

Этап 7. Профилактика

На все компьютеры ставят обновленный антивирус.

Усиливают политику доступа (только администратор может устанавливать программы).

На маршрутизаторе добавляют фильтры для блокировки подозрительных IP-адресов.

Итог

Благодаря системному мониторингу удалось:

– выявить подозрительный трафик;

– вовремя пресечь его;

– зафиксировать доказательства;

– предотвратить возможную утечку данных.

Учебно-методический раздел к главе 11

Цели изучения темы

– Освоить понятие «сетевая конфигурация» и уяснить роль конфигурации в администрировании и безопасности ИТКС.

– Изучить основные методы определения конфигурации сети (ручные, автоматизированные, с применением специализированных утилит).

– Ознакомиться с современными средствами мониторинга сетей (SCOM, Zabbix, Nagios, Cacti и др.).

– Разобрать практику перехвата сетевого трафика (пакетный анализ, DPI, NetFlow).

– Научиться применять базовые методики выявления аномалий и подозрительной активности в сетях.

– Сформировать навыки фиксации цифровых доказательств при анализе сетевых инцидентов.

– Развить умение сопоставлять данные мониторинга и результаты анализа конфигурации для выстраивания целостной картины сетевой безопасности.

Вопросы для семинарского занятия

1. Что понимается под конфигурацией сети? Каковы ее основные элементы?

2. Какие существуют методы определения конфигурации сети?

3. В чем разница между активным и пассивным мониторингом?

4. Какие протоколы чаще всего используются для мониторинга (SNMP, NetFlow, sFlow)?

5. Каковы особенности систем SCOM, Zabbix, Nagios и Cacti?

6. В чем преимущества и недостатки OSS- и SLA-мониторинга?

7. Что такое перехват информации в сети? Какие его методы применяются в учебных и практических целях?

8. Как работает технология Deep Packet Inspection (DPI)?

9. Каковы этические и правовые аспекты применения мониторинга и перехвата?

10. Как связаны задачи мониторинга с обеспечением информационной безопасности?

Варианты практических заданий для студентов

1. Анализ конфигурации сети

– С помощью утилит ipconfig, ifconfig, tracert, nmap составить карту учебной сети.

– Построить схему соединений (топологию).

– Определить узкие места и потенциальные точки атаки.

2. Мониторинг трафика

– Настроить Zabbix/Nagios или аналог.

– Снять показатели загрузки одного из интерфейсов.

– Построить график изменения параметров.

3. Перехват пакетов

– С помощью Wireshark или tcpdump зафиксировать сетевой трафик.

– Отфильтровать пакеты по IP/протоколу.

– Определить: какие сервисы используются, какие порты задействованы.

4. Выявление инцидента

– Получить учебные данные (например, всплеск трафика на неизвестный IP).

– Пошагово определить источник, зафиксировать активность, предложить меры реагирования.

5. Сравнительный анализ систем мониторинга

– Разделить студентов на группы, каждой группе дать систему (SCOM, Zabbix, Nagios, Cacti).

– Составить таблицу «Плюсы/Минусы/Область применения».

– Представить результаты в формате мини-доклада.

Иные формы обучения

Лабораторная работа «Основы мониторинга в информационно-телекоммуникационных сетях»

Цель: научиться использовать простейшие методы мониторинга сети на примере домашнего Wi-Fi роутера и ноутбука.

Оборудование и ПО:

– Wi-Fi роутер (любой, даже домашний);

– Ноутбук или ПК с выходом в интернет.

Программы:

– командная строка (Windows CMD или Linux Terminal);

– Wireshark (бесплатно, скачать с официального сайта);

– браузер (для проверки доступа к сайтам).

Этап 1. Проверка доступности сети (пинг)

Шаги:

1. Откройте командную строку (Win + R → cmd).
2. Введите команду: ping ya.ru.
3. Посмотрите результат:

– время отклика (например, 25 мс);

– потери пакетов (если 0% – это хорошо).

Что это показывает? Если сайт отвечает быстро, значит, интернет-соединение работает нормально. Если время ответа большое (200–300 мс) или есть потери, значит, где-т. е. перегрузка или сбой.

Этап 2. Трассировка маршрута (tracert)

Шаги:

1. Введите команду: tracert ya.ru.
2. На экране появится список узлов, через которые идет трафик.

Что это показывает? Маршрут пакета до сервера. Если связь обрывается на каком-то узле, значит, проблема именно там.

Этап 3. Проверка пропускной способности (speedtest)

Шаги:

1. Перейдите на сайт speedtest.net.
2. Запустите тест.
3. Запишите результаты: скорость загрузки, скорость отдачи, задержка.

Что это показывает? Фактическую скорость интернета и качество соединения.

Этап 4. Захват пакетов в Wireshark

Шаги:

1. Запустите Wireshark.
2. Выберите интерфейс Wi-Fi или Ethernet.
3. Нажмите Start Capture.
4. Откройте любой сайт в браузере.

5. Остановите захват и найдите пакеты, где в колонке Protocol указано HTTP или TLS.

Что это показывает? Каждое соединение – это десятки пакетов. Вы увидите, как «разговаривают» ваш компьютер и сайт.

Этап 5. Фильтрация трафика

Шаги:

1. В Wireshark в строке фильтра введите: ip.addr == 8.8.8.8 (это Google DNS).
2. Наблюдайте только пакеты с этим адресом.

Что это показывает? Фильтры позволяют выделять конкретный поток данных (например, общение с одним сервером).

Этап 6. Анализ потоков (NetFlow-аналог)

Если Wireshark кажется слишком сложным, можно использовать встроенные средства Windows:

Шаги:

1. Введите команду: netstat.
2. Посмотрите список подключений: IP-адреса, порты, состояния соединений.

Что это показывает? С какими серверами общается ваш компьютер прямо сейчас.

Этап 7. Визуализация

Для закрепления можно построить простую схему (даже вручную в тетради):

– Мой ноутбук → Роутер → Интернет-провайдер → Сервер Яндекс.

– Подписать: где проверяли пинг, где делали трассировку, где ловили пакеты.

Итог

Выполнив эти шаги вы:

– освоите **базовые команды сетевой диагностики** (ping, tracert, netstat);

– поймете, как работает **захват пакетов** (Wireshark);

– сможете **выявить простейшие проблемы** (например, слабый сигнал Wi-Fi или перегруженный канал);

– научитесь связывать теорию (каналы, пакеты, маршрутизация) с практикой.

Библиографический список к главе 11

Нормативные правовые акты

1. Национальный стандарт Российской Федерации. ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения: национальный стандарт Российской Федерации». – М. : Стандартинформ, 2021.

Книги, учебники

2. Инфокоммуникационные сети : энциклопедия / [П. А. Будко и др.]. Кн. 4. Гетерогенные сети связи: принципы построения, методы синтеза, эффективность, цена, качество / под ред. проф. В. И. Мирошникова. – М. : Наука, 2020.

3. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб. : Питер, 2021.

4. Скиба, В. Ю. Методы и средства защиты информации в компьютерных сетях : учебное пособие / В. Ю. Скиба. – СПб. : Лань, 2020.

5. Шаньгин, В. С. Защита информации в компьютерных системах и сетях / В. С. Шаньгин. – 2-е изд. – М. : Инфра-М, 2021.

Статьи

6. Аллакин, В. В. Общий подход к построению перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей / В. В. Аллакин, Н. П. Будко, Н. В. Васильев // Системы управления, связи и безопасности. – 2021. – № 4. – С. 125–227.

7. Мониторинг информационно-телекоммуникационных сетей / [Д. А. Груздев и др.] // Труды учебных заведений связи. – 2016. – № 4. – С. 46–50.

8. Клычков, И. А. Способы мониторинга компьютерных сетей / И. А. Клычков // Молодой ученый. – 2024. – № 19 (518). – С. 13–18.

9. Коноваленко, С. А. Анализ систем мониторинга вычислительных сетей / С. А. Коноваленко, И. Д. Королев // Молодой ученый. – 2016. – № 23 (127). – С. 66–73.

10. Коцыняк, М. А. Методика оценки устойчивости интегрированной информационно-телекоммуникационной сети в условиях компьютерных атак / М. А. Коцыняк, О. С. Лаута, С. А. Осадчий // Информация и космос. – 2014. – № 2. – С. 38–41.

11. Стародубцев, Ю. И. Проблема формирования системы показателей для оценки защищенности информационно-телекоммуникационных сетей / Ю. И. Стародубцев, А. А. Евграфов, Е. В. Сухорукова // Проблемы экономики и управления в торговле и промышленности. – 2014. – № 3. – С. 80–86.

12. Сторожук, М. Использование систем мониторинга сетей для обеспечения работы критически важных приложений / М. Сторожук // Первая миля. – 2021. – № 1. – С. 40–44.

13. Применение мониторинга для обеспечения безопасности информационных систем / [С. С. Черненко и др.] // Современные проблемы науки и образования. – 2014. – № 4. – С. 209–221.

Электронные ресурсы

14. Как работает мониторинг компьютерных сетей. – URL: https://net-admin.ru/stati/kak-rabotaet-monitoring-kompyuternykh-setey/ (дата обращения: 21.05.2024).

15. Методы мониторинга и обеспечения безопасности для поддержания работоспособности корпоративной сети. – URL: https://www.securitylab.ru/analytics/301808.php (дата обращения: 21.05.2024).

16. Средства мониторинга и анализа. – URL: https://spravochnick.ru/informatika/sredstva_monitoringa_i_analiza_lokalnyh_setey/ (дата обращения: 21.05.2024).

Глава 12. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

ВВЕДЕНИЕ

Представьте: вам в мессенджер приходит сообщение от друга: *«Срочно! Помоги, переведи 5000 рублей, завтра верну».* Что вы сделаете? Большинство даже не задумываются – помогают. А потом выясняется, что друг ничего не писал. Его аккаунт взломали, а деньги ушли мошенникам.

Это и есть **социальная инженерия** – когда обман строится не на взломе компьютеров, а на умении манипулировать человеком.

Сегодня информацию часто называют «новой нефтью». Она действительно стала самым ценным ресурсом. Компании тратят миллионы на защиту серверов, государство строит сложные системы кибербезопасности. Но есть одно слабое место, обойти которое легче всего, – **сам человек**.

Какие бы современные средства защиты мы ни придумали – антивирусы, шифрование, пароли по SMS, токены или биометрию, – все это можно обойти, если человек сам, по незнанию или доверчивости, откроет дверь злоумышленникам.

Почему это работает?

Социальная инженерия опирается на слабости, знакомые каждому из нас.

– **Доверчивость:** мы привыкли верить официальным письмам и звонкам.

– **Желание помочь:** мошенники часто изображают просьбу о помощи.

– **Страх**: «Ваш счет заблокирован», «Вы обвиняетесь в нарушении закона».

– **Любопытство**: «Смотри фото, где ты отмечен».

– **Жадность или выгода**: «Вы выиграли приз, получите бонус».

Человек реагирует быстрее, чем успевает включить логику. И этим пользуются атакующие.

Реальные истории

История знает немало случаев, когда доверие оказалось сильнее любой защиты.

– **Фрэнк Абигнейл** (фильм *«Поймай меня, если сможешь»*): за 5 лет обманул банки на миллионы долларов, притворяясь пилотом и врачом.

– **Компания Ubiquiti Networks**: сотрудники перевели 40 млн долл. по письму, пришедшему «от руководства».

– **Карлос Фломенбаум**: украл алмазы на 28 млн долл., просто завоевав доверие персонала банка.

– **Виктор Люстиг**: легендарный мошенник, который дважды (!) продал Эйфелеву башню.

Обратите внимание: в этих историях не использовались суперкомпьютеры, вирусы или сложные программы. Все строилось на психологии, манипуляциях и доверии.

Социальная инженерия в цифровом мире

Сегодня она стала еще опаснее, потому что переместилась в Интернет:

– **Фишинг** – поддельные письма и сайты банков.

– **Вишинг** – звонки «из службы безопасности».

– **Смишинг** – SMS с вредоносными ссылками.

– **Социальные сети и мессенджеры** – рассылки от «друзей» или «коллег».

– **Многоступенчатые атаки** – письмо + звонок + фальшивый сайт.

Социальный инженер действует так, чтобы вы сами сделали нужный шаг: кликнули на ссылку, открыли вложение, сообщили данные карты.

Таким образом, социальная инженерия – это не просто обман. Это целая наука на стыке **психологии, социологии и информационных технологий**. Она постоянно развивается. И пока техника становится все совершеннее, **человек остается самым уязвимым звеном**.

§ 1. Нормативные правовые документы, определяющие понятие «социальная инженерия»

Когда мы слышим словосочетание *«социальная инженерия»*, у многих оно ассоциируется с современными кибератаками. Но на самом деле история этого явления уходит в глубокую древность.

Еще в Древней Греции и Риме искусные ораторы умели убеждать, манипулировать, склонять людей к нужному решению. Это была социальная инженерия своего времени. Правда, больше похожая на искусство речи, чем на преступление.

В XX в. термин «социальная инженерия» вошел в научный и политический обиход. Тогда он означал методы управления обществом. Но уже после Второй мировой войны оттенок изменился. Слово стало ассоциироваться с манипуляциями и обманом.

В 1970-е гг. появились первые синжеры – телефонные мошенники. Они звонили людям и, играя на страхах или доверии, вытягивали конфиденциальные данные. С появлением компьютеров они переквалифицировались в **социальных хакеров**. Так социальная инженерия оказалась плотно связанной с киберпреступностью.

Терминология и ключевые фигуры

– Впервые термин «социальная инженерия» ввел американский юрист и социолог **Роско Паунд**. Для него социальная инженерия была инструментом права: помогать юристам решать общественные задачи.

– Настоящую популярность понятию принес **Кевин Митник** – легендарный хакер, а затем консультант по безопасности. Его книги «Искусство обмана» и «Искусство вторжения» до сих пор считаются классикой: там подробно разобрано, как манипулировать человеческим фактором.

– В России термин стали использовать ученые и криминалисты:

– П. В. Ревенков и А. А. Бердюгин трактуют социальную инженерию как **способ хищения конфиденциальной информации**.

– В. С. Овчинский называет ее одним из самых опасных векторов атак на данные.

До сих пор нет единого юридического определения социальной инженерии. В уголовных делах мы встречаем формулировки вроде *«психологические приемы общения»* или *«наступательная тактика»*. Это создает трудности для следователей и судов.

В России понятие «социальная инженерия» постепенно закрепляется в официальных документах.

– Впервые оно появилось в **«Основных направлениях развития финансового рынка Российской Федерации» (2022–2024 гг.)**, где под ним понималось введение в заблуждение ради получения доступа к информации или деньгам.

– Затем термин вошел в документы Банка России: *«Основные направления развития информационной безопасности кредитно-финансовой сферы на 2023–2025 гг.»* (утверждены 22.05.2023): *«Основные направления развития финансового рын-*

ка Российской Федерации на 2024–2026 гг.».

Почему это важно? Потому что именно Центробанк фиксирует реальную угрозу. По его данным:

– в 2017 г. – 75 % всех кибермошенничеств строились на социальной инженерии;

– в 2019 г. – уже 89 %;

– в 2020 г. – 90 %;

– в 2024 г. доля выросла: **две трети всех IT-преступлений – это именно атаки с применением социальной инженерии**.

В ответ на рост угроз начали внедряться законодательные инициативы:

1. **Период охлаждения** (вступает в силу с 1 сентября 2025 г.). Если человек оформляет кредит от 50 до 200 тыс. руб., деньги переводятся только через 4 часа. Если сумма больше 200 тыс., ожидание – 48 часов. Идея проста: дать жертве время опомниться и отказаться от кредита, навязанного мошенниками.

2. **Сервис «второй руки»** (планируется к запуску в 2025 г.).

Клиент может назначить доверенное лицо, которое получит уведомление о крупном переводе.

Особенно актуально для пожилых людей, которых часто обманывают.

3. **Самозапрет на кредиты** (введен 1 марта 2025 г.).

Любой гражданин может подать заявку, чтобы банки не выдавали ему кредиты без его личного согласия.

За первые 10 дней этой опцией уже воспользовались 5 млн человек.

Вывод. Законодательство постепенно догоняет реальность. Но мошенники изощряются быстрее, чем появляются новые законы. Поэтому одного периода охлаждения и сервиса «второй руки» мало. Необходим **комплексный подход**:

– совершенствование НПА;

– внедрение технологических решений;

– повышение киберграмотности населения.

И пока в системе остается слабое звено – человек, социальная инженерия будет оставаться одной из главных угроз безопасности.

§ 2. Характеристики и особенности социальной инженерии, ее формы и методы

Когда мы слышим про социальную инженерию, то часто представляем звонки «сотрудников банка» или письма с фишинговыми ссылками. Но на самом деле все глубже. Чтобы понять, как она работает, важно рассмотреть **характеристики, формы и методы** этого явления.

2.1. Основные характеристики социальной инженерии

Социальная инженерия отличается от других видов преступлений, прежде всего, тем, что в ее центре стоит **человек**, а не техника. Вместо того чтобы взламывать сложные системы безопасности, мошенники взламывают психику.

Ключевые черты социальной инженерии:

– **Обход критического мышления.** Влияние идет не на логику, а на эмоции. Жертву пугают, торопят, льстят или вводят в стресс.

– **Простота и эффективность.** Зачем ломать дорогую защиту сервера, если нужные данные можно выпросить у человека за 5 минут?

– **Низкий риск для преступника.** В отличие от технического взлома социальные атаки трудно доказать и расследовать.

– **Адаптивность.** Социальные инженеры легко подстраи-

ваются под новые условия: меняют легенды, маскируются под тренды и события (например, пандемия или СВО).

– **Эмоциональное давление.** Главный инструмент – вывести жертву из равновесия и заставить действовать автоматически.

2.2. Цели и объекты социальной инженерии

Цели:

1. Завоевать доверие.
2. Получить доступ к конфиденциальным данным.
3. Вынудить жертву совершить нужные действия (перевод денег, ввод пароля, открытие файла).

Объекты атак:

– люди с личными качествами – доверчивостью, отзывчивостью, страхами;

– работники компаний, особенно те, кто имеет доступ к информации или финансам;

– все мы: пользователи банковских приложений, соцсетей, госуслуг.

2.3. Факторы, повышающие эффективность атак

Социальные инженеры знают: лучше всего жертва ведется, когда **не успевает подумать**.

Они используют:

– **время суток:** чаще звонят ночью или поздно вечером, когда человек уязвим;

– **срочность:** «У вас 10 минут, иначе деньги уйдут навсегда»;

– **ссылку на авторитет:** «Говорит полковник ФСБ», «… служба безопасности Центробанка»;

– **сильные эмоции:** страх, радость («вы выиграли»), тревога («с вашими близкими что-то случилось»).

2.4. Трехзвенная структура преступлений

Социальная инженерия редко бывает экспромтом. Обычно это:

1. **Подготовка.** Сбор информации (анкеты, соцсети, звонки).

2. **Атака.** Вывод жертвы в стресс и получение нужных данных или действий.

3. **Сокрытие.** Уход от ответственности: смена номеров, подставные лица, обналичивание средств.

Пример: мошенники заранее знают, как зовут родственников жертвы, их возраст, место работы, учебы и т. п., используют это для правдоподобной легенды.

2.5. Формы социальной инженерии

OSINT (разведка по **открытым источникам)**

Суть. Сбор фактов о человеке/организации из открытых ресурсов: соцсети, сайты компаний, госреестры, конференционные программы, вакансии, отзывы, рекламные каталоги.

Зачем это злоумышленнику. Подготовить правдоподобный предлог: знать, как зовут HR-директора, какие VPN и почтовый домен у компании, где офис, какой стек технологий.

Типовой сценарий. В LinkedIn видят, что вы ищете работу → HR присылает оффер «мечты» → «для оформления» просит сканы паспорта и ИНН → данные уходят в кредитные схемы.

Как защититься.

– Минимизируйте избыточную открытость: скрывайте дату рождения/телефон/адрес.

– Проверяйте цифровой след: что о вас видно без логина.

– С критикой относитесь к просьбам предоставлять сканы различных документов под видом «оформления» до подписания договора лично.

Фишинг (e-mail, массовый)

Суть. Массовая рассылка писем со ссылками/вложениями: ведут на поддельные страницы или ставят вредоносы.

Сценарий. «Ваши Госуслуги заблокированы, перейдите по ссылке». Переход → ввод логина/пароля → код из SMS → утечка.

Как защититься.

– Не жмите на ссылки из писем «с тревогой/срочностью». Открывайте сайт вручную из закладок.

– Смотрите на домен: подмена букв, лишние поддомены – красный флаг.

– Включайте 2FA (TOTP/апп-генератор, а не только SMS).

Целевой фишинг (spear phishing)

Суть. То же, но персонализировано под конкретного сотрудника: с логотипами партнеров, правильной лексикой, деталями из OSINT.

Сценарий. «Страховая компания» шлет форму «уточнить данные по полису» → клон сайта → кража учетных данных.

Как защититься.

– Политика двух каналов: все важное подтверждаем вторым каналом (звонок/чат в корпоративной системе).

– Почтовая аутентификация на домене: SPF, DKIM, DMARC (для IT-службы).

– Шлюзы web-фильтрации, песочницы вложений (для организаций).

– Регулярные тренировки фишинг-симуляциями.

Вейлинг (whaling)

Суть. Атаки на «больших рыб»: директоров, CFO, бухгалтерию.

Сценарий. Письмо «от генерального» с просьбой «срочно» сделать перевод на «безопасный счет». Потери – миллионы.

Как защититься

– Жесткие **финансовые регламенты**: любой платеж/изменение реквизитов – только после очного или голосового подтверждения *по заранее согласованному номеру*.

– «Двое из трех» на крупные суммы (инициатор/согласующий/плательщик).

– Отдельное обучение топ-менеджмента (кейсы, имитации).

Вишинг (vishing – телефон)

Суть. Звонок с подменой номера, эмоциональное давление («срочно спасаем деньги»).

Сценарий. «СБ банка» сообщает о «мошеннической операции», требует CVV/коды или перевод на «защищенный счет».

Как защититься.

– Никогда не диктуйте коды/пароли/CVV по телефону.

– Завершите разговор и **перезвоните сами** по номеру с карты/сайта банка.

– Используйте антиспам-фильтры звонков на смартфоне.

Смишинг (smishing – SMS/мессенджеры)

Суть. Ссылки в сообщениях: «ваш ящик/доставка/штраф».

Как защититься.

– Не переходите по ссылкам из SMS. Заходите в сервис через приложение/офсайт.

– Удаляйте сомнительные сообщения, включите фильтрацию спама.

Спуфинг (маскарад)

Суть. Подделка «отправителя»: домена, e-mail, телефонного номера, страницы в соцсети.

Сценарий. Фейковый профиль «друга» просит «одолжить на пару дней».

Как защититься.

– Проверка через второй канал: голосом/лично.

– Для IT: строгие DMARC-политики (reject), защита от номерной подмены на АТС.

Обратная социальная инженерия и услуга за услугу (quid pro quo)

Суть. Злоумышленник «помогает» (якобы СБ банка/техподдержка), а потом просит выполнить действия «для защиты/расследования».

Сценарий. «Мы отбили атаку, теперь переведите тестовую сумму для трассировки мошенников» – деньги уходят безвозвратно.

Как защититься.

– Настрой консервативного отказа: никаких переводов для проверки.

– Техподдержка **никогда** не просит пароли/коды и не просит ставить ПО с экрана.

Претекстинг (атакующий сценарий)

Суть. Жизнеспособная легенда + пошаговый сценарий, разбитый на подцели (древо целей).

Сценарий. Продажа на площадке: «покупатель» убеждает продиктовать SMS-код «для перевода» → на деле – привязка вашего мобильного банка на его устройство.

Как защититься.

– Золотое правило: **никому и никогда** не диктовать SMS-коды/пароли.

– Не выполнять непонятные действия с телефоном по чужой просьбе.

– Меняйте пароли регулярно, включайте 2FA.

Бейтинг (приманка, USB/QR)

Суть. «Найдена флешка/QR с чем-то заманчивым» → вредонос.

Современный вариант. USB Rubber Ducky (эмулирует клавиатуру, обходит DLP), QR-наклейки поверх настоящих («оплатите кофе»).

Как защититься.

– Никогда не подключайте чужие носители к корпоративным ПК.

– Проверки только на изолированном песочном компьютере без сети.

– Обучение сотрудников + запрет автозапуска USB, контроль USB в ОС.

Троян во **вложениях**

Суть. Письмо счет/договор/резюме, внутри – скрипт/макрос/эксплойт, крадущий креды.

Как защититься.

– Отключите макросы по умолчанию, используйте защищенный просмотр.

– Песочницы вложений, EDR/NGAV на рабочих станциях.

– Обновления ОС/офиса/плагинов без отставаний.

Scareware (пугалки) и Rogue AV (лже-антивирус)

Суть. «На вашем ПК 785 угроз! Купите срочно защиту» → оплата фейкового ПО → заражение/кража карточных данных.

Как защититься.

– Ставьте **один** лицензионный антивирус, обновляйте его автоматически.

– Блокируйте всплывающие окна в браузере, не скачивайте чистилки со случайных сайтов.

– Письма с вложениями «оплати и спасайся» – удалять без открытия.

Итоговый чек-лист защиты. Для пользователей

– **Берите паузу.** Страх/срочность = почти наверняка обман.

– **Никому** не сообщайте PIN/CVV/пароли/SMS-коды.

– Всегда **перезванивайте сами** по официальному номеру.

– Используйте **2FA** и **уникальные** пароли (менеджер паролей).

– Держите соцсети закрытыми, не светите даты рождения/контакты.

– Не подключайте чужие USB, не сканируйте случайные QR.

Для организаций

– Почтовая защита: **SPF/DKIM/DMARC**, песочницы, web-шлюзы.

– Политики **BEC/вейлинг**: регламенты платежей, «два канала», «двое из трех».

– EDR/NGFW/DLP, запрет автозапуска, контроль USB, патч-менеджмент.

– Обучение и **регулярные фишинг-симуляции** (включая звонки).

– Процедуры реагирования: куда и как сообщать, как быстро блокировать доступы.

2.6. Примеры из практики

Пример 1. Пандемия. Мошенники рассылали письма якобы от ВОЗ с просьбой перечислить деньги «на разработку вакцины». Люди, охваченные страхом, переводили средства.

Пример 2. Отмывание денег. Жертве случайно зачисляют крупную сумму. Потом звонят и просят вернуть деньги. На деле человек становится соучастником отмывания.

Пример 3. Конкурсы в соцсетях Человек выигрывает «приз», его просят оплатить доставку через ссылку. На самом деле это фишинг.

2.7. Психология атаки

Почему люди ведутся? Потому что мозг работает двумя маршрутами:

– **Центральный маршрут.** Логический, медленный. Мы думаем, анализируем.

– **Периферический маршрут.** Быстрый, эмоциональный. Включается при стрессе.

Социальные инженеры делают все, чтобы запустить именно второй маршрут, и человек начинает действовать на автомате.

2.8. Как **распознать атаку**

Признаки:

– Вас торопят («10 минут на решение»).

– Вас пугают («ваш счет заблокирован»).

– Вас вводят в эйфорию («вы выиграли миллион»).

– Ссылаются на авторитет («говорит сотрудник ФСБ»).

2.9. Как **защититься**

– Всегда брать паузу.

– Перезванивать в организацию по официальному номеру.

– Никогда не сообщать личные данные по телефону.

– Относиться критически к «выгодным предложениям» и «срочным угрозам».

Социальная инженерия в современном цифровом обществе представляет собой одну из наиболее коварных и труднообнаруживаемых угроз информационной безопасности. В отличие от технических методов атак, требующих сложного оборудования и специализированных знаний, социальная инженерия эксплуатирует человеческий фактор – доверчивость, эмоциональность, страх или, напротив, желание получить выгоду. Именно поэтому она остается столь результативной: достаточно убедить человека нажать на ссылку, сообщить пароль или передать данные – и даже самые надежные системы защиты оказываются бессильными.

Практика показывает, что социальные инженеры умело сочетают психологические приемы с техническими инструментами – от фишинга и вишинга до использования вредоносного ПО и OSINT-разведки. Каждый год схемы становятся все более изощренными, а их последствия – все опаснее. Мошенники крадут не только деньги, но и персональные данные, корпоративные секреты, подрывают доверие к цифровым сервисам и организациям.

Однако у этой угрозы есть и обратная сторона: зная ее особенности и методы, можно эффективно выстраивать защиту. Главный барьер для социальных инженеров – это осведомленность и критическое мышление пользователей. Чем выше уровень киберграмотности общества, тем меньше шансов у мошенников.

Таким образом, борьба с социальной инженерией – это комплексная задача, требующая взаимодействия государства, бизне-

са и самих граждан. Технические средства защиты могут быть мощными, но именно человек остается самым уязвимым звеном. Только сочетание технологий, права и образования позволит существенно снизить риски и защитить общество от этой стремительно развивающейся формы киберугроз.

Учебно-методический раздел к главе 12

Цели изучения темы

1. Освоить понятие «социальная инженерия» с позиций уголовного и административного права.

2. Изучить основные формы и методы социальной инженерии, применяемые при совершении преступлений.

3. Понять, какие статьи УК РФ и КоАП РФ охватывают данные деяния (мошенничество, неправомерный доступ к информации, кража, вымогательство и др.).

4. Разобрать алгоритмы действий сотрудников правоохранительных органов при выявлении и расследовании преступлений, связанных с социальной инженерией.

5. Освоить методики фиксации доказательств: сохранение переписки, телефонных звонков, финансовых транзакций.

6. Развить умение оценивать уровень киберграмотности граждан и предлагать меры профилактики.

Вопросы для семинарского занятия

Теоретические вопросы

1. Какое определение социальной инженерии закреплено в официальных документах Банка России?

2. Чем отличаются социально-инженерные атаки на граждан от атак на организации?

3. Какие статьи УК РФ применимы при квалификации преступлений, совершенных методами социальной инженерии?

4. Почему в правоприменительной практике до сих пор нет единого подхода к понятию «социальная инженерия»?

5. Какие этапы включает расследование преступлений, связанных с социальной инженерией?

6. В чем сложность доказывания вины мошенников при использовании психологического воздействия?

7. Какие международные практики (например, в ЕС или США) можно заимствовать для противодействия?

8. Каковы основные меры профилактики социальной инженерии на уровне МВД России и Роскомнадзора?

9. Как взаимодействуют между собой Банк России, МВД России и кредитные организации при расследовании киберпреступлений?

10. Какие современные тенденции делают социальную инженерию все более изощренной?

Варианты практических заданий для студентов

1. Анализ инцидента. Разобрать реальное дело (например, звонок от «сотрудника банка»).

Задание: определить состав преступления, квалифицировать действия мошенников по статьям УК РФ, предложить меры расследования.

2. Составление протокола осмотра. Студентам дается сценарий: жертва предъявляет телефон с SMS и звонками от мошенников.

Задание: составить протокол осмотра электронного носителя с фиксацией доказательств.

3. Ролевая игра «Оперативное взаимодействие». Группа студентов делится на «оперативников МВД», «жертву», «социального инженера».

Задача: оперативники должны провести опрос, выявить обстоятельства и зафиксировать первичные данные.

4. Разработка профилактического буклета.

Задание: создать информационную памятку для граждан: «10 правил защиты от мошенников». Обязательное условие – ссылки на статьи УК РФ и рекомендации МВД России.

5. Кейс «Отмывание денег через жертв». Студентам описывается ситуация: жертве случайно перевели крупную сумму, а потом позвонили и попросили вернуть.

Задание: объяснить, почему возврат этих средств делает жертву соучастником преступления, и как правильно действовать.

Иные формы обучения

– **Мозговой штурм** «Как должна быть построена система профилактики социальной инженерии в МВД России?»

– **Деловая игра «Расследование»:** студенты работают как следственная группа, по материалам дела выявляют способы совершения преступления и собирают доказательства.

– **Судебный процесс**: одни студенты играют роль обвинения, другие – защиты. Квалификация: ст. 159 УК РФ («мошенничество»).

– **Круглый стол** «Можно ли ввести в УК РФ отдельную статью за социальную инженерию?»

– **Мини-проект** – разработка модели сотрудничества МВД России, банков и операторов связи для выявления мошенников.

Библиографический список к главе 12

Нормативные правовые акты

1. Уголовный кодекс Российской Федерации : УК : принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 04.08.2025).

2. Кодекс Российской Федерации об административных правонарушениях : КоАП : принят Государственной Думой 20 декабря 2001 г. : одобрен Советом Федерации 26 декабря 2001 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 04.08.2025).

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ч. 1.

4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ч. 1.

Документы Банка России

5. Центральный банк Российской Федерации. Основные направления развития финансового рынка Российской Федерации на 2022–2026 годы. – М., 2022.

6. Центральный банк Российской Федерации. Основные направления развития информационной безопасности кредитно-финансовой сферы на 2023–2025 годы. – М., 2023.

Книги, учебники

7. Горбунов, А. В. Кибербезопасность и социальная инженерия / А. В. Горбунов. – М. : Литрес, 2023.

8. Гордячкова, О. В. Личные финансы и финансовая безопасность : учебное пособие / О. В. Гордячкова. – М. : Мир науки, 2021.

9. Жданов, Ю. Н. Киберполиция XXI века. Международный опыт / Ю. Н. Жданов, В. С. Овчинский ; под ред. С. К. Кузнецова. – М. : Международные отношения, 2020.

10. Кевин, К. Д. Искусство обмана / К. Д. Кевин, Л. С. Вильям. – М., 2004.

11. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. – СПб. : БХВ-Петербург, 2007.

12. Митник, К. Искусство вторжения / К. Митник, У. Саймон. – М. : Литрес, 2022.

13. Митник, К. Искусство обмана / К. Митник, У. Саймон. – М. : Литрес, 2021.

14. Овчинский, В. С. Мафия. Новые мировые тенденции / В. С. Овчинский. – М. : Книжный мир, 2016.

15. Ревенков, П. В. Социальная инженерия: методы и технологии / П. В. Ревенков, А. А. Бердюгин. – М. : Литрес, 2023.

16. Скляров, Д. В. Социальная инженерия: защита и противодействие / Д. В. Скляров. – М. : Литрес, 2022.

Статьи

17. Грызунов, В. В. Особенности применения технологических методов в социальной инженерии / В. В. Грызунов, О. С. Шкреба // Технико-технологические проблемы сервиса. – 2018. – № 4. – С. 90–94.

18. Иванов, И. И. Социальная инженерия в кибербезопасности / И. И. Иванов // Информационная безопасность. – 2024. – № 1. – С. 45–58.

19. Моторина, В. О. Манипуляция обществом методами социальной инженерии / В. О. Моторина, Е. Н. Полякова // Наука и молодежь в XXI веке : сборник научных трудов студентов и молодых ученых. – Курган : Курганский филиал ОУП ВО «АТиСО», 2017. – С. 290–294.

20. Петров, П. П. Фишинг и социальная инженерия: методы и защита / П. П. Петров // Кибербезопасность и защита данных. – 2024. – № 2. – С. 67–82.

21. Сидоров, С. С. Психологические аспекты социальной инженерии / С. С. Сидоров // Психология и кибербезопасность. – 2024. – № 3. – С. 95–110.

22. Созаев, С. С. Социальная инженерия, ее техники и методы противодействия / С. С. Созаев // Вестник науки: международный журнал. – 2020. – № 2 (23). – Т. 1. – С. 85–88.

Глава 13. ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ ПОЛУЧЕНИЯ ОПЕРАТИВНО ЗНАЧИМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

ВВЕДЕНИЕ

На наших глазах информационные технологии кардинально меняют окружающий мир. Цифровая реальность стирает границы между физическим и виртуальным пространством, создавая принципиально новую среду жизни и деятельности, которая радикально отличается от той, что существовала всего 20 лет назад.

Сегодня мы живем в эпоху Интернета всего, где к информационным коммуникациям подключены не только компьютеры и гаджеты, но и бытовая техника, промышленные системы, умные дома и многое другое. Информация перестала быть просто количественной характеристикой – она стала ключевым ресурсом для анализа социально-экономических процессов и основой для принятия решений. В современном мире на первый план выходит человек знающий, понимающий – *homo intelligens.*

Однако прогресс в области информационных технологий не только облегчил жизнь, но и открыл новые возможности для криминальной деятельности. Киберпространство стало ареной для преступлений, которые ранее были просто невозможны. Преступники активно используют такие особенности цифровой среды, как наднациональный характер, анонимность, дистанционность и трансграничность, что требует от правоохранительных органов новых подходов к оперативно-разыскной деятельности, которая теперь немыслима без работы с информационными ресурсами Интернета и другими цифровыми данными.

Однако мало просто уметь выявлять и получать оперативно значимую информацию, используя современные информационно-телекоммуникационные системы и технологии. Чтобы эта информация стала полноценным документом, необходимым для установления всех обстоятельств противоправного деяния, выявления и изобличения преступников, ее нужно грамотно зафиксировать, оформить и представить лицам, принимающим решения.

В этой теме мы обсудим, как обеспечить законность, достоверность и процессуальную значимость таких данных, а также какие нормативные документы регулируют эту деятельность. Но прежде чем перейти к этим вопросам, давайте вспомним ключевые аспекты оперативно-разыскной информации, которые мы уже обсуждали ранее.

§ 1. Оперативно-разыскная информация: сущность и проекции

Оперативно-разыскная информация представляет собой сложный феномен, который можно рассматривать как вектор в трехмерном пространстве, включающем реактивную, ресурсную и фоновую проекции (рис. 13.1).

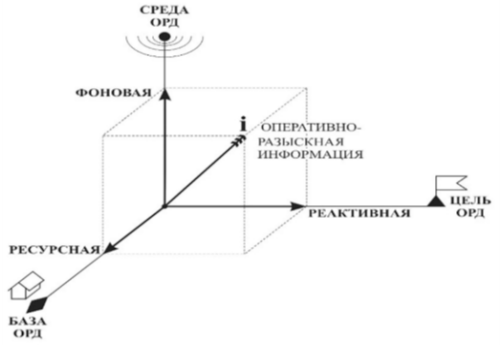


Рис. 13.1. Оперативно-разыскная информация в пространстве ее реактивной, ресурсной и фоновой проекций как цель, база и среда ОРД

Каждая из этих проекций играет самостоятельную и важную роль в системе оперативно-разыскной деятельности (ОРД).

1.1. Реактивная оперативно-разыскная информация

Реактивная информация связана с конкретным преступлением или криминальной ситуацией. Это сведения, которые позволяют действовать здесь и сейчас: сигналы о готовящихся или совершенных преступлениях, данные о подозреваемых лицах, обстоятельства правонарушения.

Пример: сообщение о краже со взломом в магазине, на которое оперативные сотрудники незамедлительно реагируют, выезжая на место происшествия для сбора доказательств.

Такая информация является основой для принятия решений в ОРД. Она позволяет выявлять причинно-следственные связи преступных событий, прогнозировать последствия и оперативно реагировать на угрозы. Добывание реактивной информации – одна из ключевых задач ОРД.

1.2. Ресурсная оперативно-разыскная информация

Ресурсная информация составляет базу оперативно-разыскного процесса. Это накопленные знания и данные, используемые для раскрытия и расследования преступлений, а также профилактики правонарушений.

Пример: сведения из баз данных МВД России о ранее судимых лицах, их связях, местах проживания, характерных привычках. Эти данные позволяют оперативникам выявлять потенциальных участников преступных групп и эффективнее организовывать работу.

Кроме того, ресурсная информация выполняет функцию сохранения и передачи накопленного опыта борьбы с преступностью, являясь фундаментом информационного обеспечения ОРД.

1.3. Фоновая оперативно-разыскная информация

Фоновая информация формирует широкую информационную среду, в которой осуществляется оперативно-разыскной процесс. Это могут быть сообщения СМИ, данные из сетевых коммуникаций, радиоэфира и интернета.

Хотя она не всегда напрямую связана с конкретным преступлением, анализ подобных сведений позволяет выявлять криминальные события и сопутствующие обстоятельства.

Пример: обсуждения в социальных сетях незаконных сделок с наркотиками, оружием или поддельными документами. На первый взгляд, это случайные реплики, но их анализ способен вывести оперативников на реальную преступную деятельность.

Таким образом, для специалистов в сфере анализа и защиты информации понимание всех трех проекций оперативно-разыскной информации имеет принципиальное значение. Умение выделять значимые данные из общего потока и использовать их в ОРД – это ключевая компетенция, позволяющая эффективно противостоять преступности в условиях цифровой трансформации.

§ 2. Оформление оперативно значимой информации

Добыча оперативно значимой информации является лишь первым этапом работы. Основная задача оперативно-разыскной деятельности заключается в выявлении, предупреждении, пресечении и раскрытии преступлений, а также в установлении лиц, причастных к их совершению.

Для этого полученные сведения должны быть не только достоверными и проверенными, но и надлежащим образом оформленными. Только в этом случае они могут быть представлены следственным органам или в суде и приобрести процессуальную силу.

2.1. Нормативные правовые документы, регламентирующие понятие «оформление результатов оперативно значимой информации»

До 1990-х гг. ОРД в нашей стране не имела законодательного закрепления. Она регулировалась подзаконными актами – секретными и совершенно секретными ведомственными документами, доступ к которым был ограничен не только для следователей, но даже для прокуроров и судей.

Ситуация изменилась с принятием **Закона «Об оперативно-розыскной деятельности в Российской Федерации» от 13 марта 1992 г. № 2506-1**, а затем и второго, ныне действующего **Федерального закона «Об оперативно-розыскной деятельности» от 1995 г.** Эти документы впервые определили правовые рамки ОРД: установили виды оперативно-разыскных мероприятий, основания для их проведения, гарантии соблюдения прав и свобод граждан, а также механизмы надзора и контроля за законностью деятельности оперативных органов.

Правовая основа ОРД

Согласно ст. 1 Федерального закона об ОРД оперативно-разыскная деятельность осуществляется посредством проведения конкретных ОРМ. Это обусловливает высокую значимость правового регулирования, так как результаты ОРМ напрямую затрагивают конституционные права граждан.

Нормативная специфика ОРД определяется двумя ключевыми факторами:

1. **Негласный характер деятельности.** Полномочия оперативных подразделений реализуются через тайные действия, которые часто связаны с ограничением конституционных прав (право на неприкосновенность частной жизни, тайну переписки и переговоров и др.). Это требует особой правовой защиты и процессуального контроля.

2. **Использование конфиденциального аппарата.** Значительная часть информации добывается с помощью негласных сотрудников (агентов, информаторов, осведомителей и др.), что также должно находиться в рамках правового регулирования, обеспечивающего баланс между эффективностью работы и защитой прав личности.

Таким образом, специфика нормативного регулирования заключается в том, что многие положения закона носят бланкетный характер и конкретизируются в подзаконных актах, включая секретные документы. Например, ст.ст. 6, 8, 9, 10 и 11 Федерального закона об ОРД требуют детальной разработки в ведомственных инструкциях.

Согласно ч. 1 ст. 4 Федерального закона об ОРД, правовую основу оперативно-разыскной деятельности составляют:

– **Конституция Российской Федерации**, закрепляющая права и свободы граждан и определяющая допустимые пределы их ограничения;

– **Федеральный закон «Об оперативно-розыскной деятельности»**, регулирующий общественные отношения в данной сфере;

– **Уголовно-процессуальный кодекс Российской Федерации**, устанавливающий порядок использования результатов ОРМ в уголовном судопроизводстве;

– **иные федеральные законы**, например «О полиции», «О федеральной службе безопасности», «О связи», «О наркотических средствах и психотропных веществах» и др.;

– **подзаконные акты** (указы Президента Российской Федерации, постановления Правительства Российской Федерации, ведомственные инструкции), определяющие порядок действий конкретных органов – полиции, ФСБ, СВР, Федеральной таможенной службы и др.

Законодательство предоставляет оперативным органам право ограничивать конституционные права граждан в строго определенных случаях. Такое ограничение допускается ч. 3 ст. 55 Конституции Российской Федерации, если оно необходимо для защиты основ конституционного строя, прав и законных интересов граждан, обеспечения обороны и безопасности государства.

Наиболее часто ограничению подвергаются:

– право на неприкосновенность частной жизни, личной и семейной тайны;

– право на неприкосновенность жилища;

– право на тайну переписки, телефонных переговоров и иных сообщений.

Принципы и **задачи ОРД**

Статья 2 Федерального закона об ОРД закрепляет основные **принципы** деятельности:

– **законность** – строгое соблюдение норм права;

– **уважение прав и свобод человека** – ограничение возможно только в рамках закона;

– **конспирация** – применение негласных методов работы;

– **сочетание гласных и негласных методов** – выбор оптимальных средств для достижения целей.

К основным **задачам** ОРД относятся:

– выявление, предупреждение, пресечение и раскрытие преступлений;

– установление лиц, причастных к противоправной деятельности;

– розыск скрывающихся от правосудия;

– добывание информации о событиях, угрожающих государственной, военной, экономической или экологической безопасности.

Эффективность данных мер подтверждается статистикой. Так, только в 2024 г. благодаря сведениям, полученным в ходе негласных ОРМ, удалось предотвратить 190 террористических актов. Среди них – шесть, готовившихся участниками запрещенных в России террористических движений «Маньяки Культ Убийц» и «Колумбайн»[1], которые планировали нападения на учебные заведения и места массового пребывания людей.

2.2. Полномочия и обязанности органов, осуществляющих оперативно-разыскную деятельность

Оперативно-разыскные органы (ОРО) действуют в строгом соответствии с Федеральным законом «Об оперативно-розыскной деятельности». Статья 15 закрепляет **широкие полномочия ОРО**, а ст. 14 – их **основные обязанности**, что обеспечивает баланс между эффективностью борьбы с преступностью и защитой прав граждан.

[1] Признаны террористическими организациями и запрещены на территории Российской Федерации.

Полномочия ОРО (ст. 15 ФЗ «Об ОРД»)

К числу основных полномочий органов, осуществляющих оперативно-разыскную деятельность, относятся:

– проведение ОРМ;

– изъятие документов, предметов и материалов, имеющих значение для предотвращения, пресечения и расследования преступлений;

– приостановление или ограничение оказания услуг связи в случаях, когда это необходимо для предотвращения угрозы жизни, здоровью граждан или безопасности государства.

Эти полномочия носят исключительный характер и реализуются только на законных основаниях, предусмотренных федеральным законодательством.

Обязанности ОРО (ст. 14 ФЗ «Об ОРД»)

Наряду с полномочиями на оперативно-розыскные органы возложен ряд обязанностей, обеспечивающих законность и эффективность их деятельности. Среди них:

– защита конституционных прав и свобод граждан, а также собственности, безопасности общества и государства;

– выполнение поручений дознавателей, следователей и судов, связанных с проведением ОРМ;

– сотрудничество с международными правоохранительными организациями в целях противодействия транснациональной преступности и терроризму;

– соблюдение правил конспирации при проведении оперативной работы;

– обеспечение безопасности собственных сотрудников, а также лиц, оказывающих содействие на конфиденциальной основе;

– организация и проведение сбора данных, необходимых для принятия управленческих и организационных решений, в том числе:

– допуске к сведениям, составляющим государственную тайну;

– праве на выполнение работ, связанных с эксплуатацией объектов повышенной опасности для жизни, здоровья и окружающей среды;

– праве на участие в ОРД либо доступ к материалам, полученным в ее ходе;

– установлении или поддержании сотрудничества с лицами, привлекаемыми к ОРМ;

– по обеспечению собственной безопасности органов, осуществляющих ОРД;

– предоставлении, переоформлении или аннулировании лицензий на частную детективную или охранную деятельность, а также удостоверений частного охранника;

– достоверности сведений, представляемых государственными или муниципальными служащими либо гражданами, претендующими на должность судьи, при наличии официального запроса.

Система полномочий и обязанностей ОРО построена таким образом, чтобы обеспечить гибкость и оперативность их работы, сохраняя при этом контроль над соблюдением прав личности и законности в целом.

2.3. Разграничение оперативно-разыскной деятельности и других видов правоохранительной деятельности

Для правильного процессуального использования результатов ОРД крайне важно не допускать их смешения с иными формами правоохранительной практики. На практике ошибки все же встречаются: нередко порядок проведения и документирования ОРМ отождествляют с процедурой следственных действий, хотя по своей сути это разные виды деятельности.

Следует учитывать, что ОРД и уголовно-процессуальная деятельность осуществляются разными субъектами, которые опираются на разные правовые нормы и в их основе лежат разные методы и средства работы.

Уголовно-процессуальное законодательство действительно предусматривает отдельные основания для проведения ОРМ, но не регулирует порядок их осуществления и фиксации. При этом между оперативными и следственными действиями есть определенное сходство по целям: оба вида направлены на получение информации, способствующей раскрытию преступлений.

Например, оперативный опрос ↔ следственный допрос; оперативное отождествление ↔ следственное опознание; оперативное обследование ↔ следственный осмотр.

Однако отождествлять их недопустимо: оперативные мероприятия решают задачи выявления, пресечения и раскрытия преступлений, а процессуальные действия проводятся в строгих рамках УПК РФ и формируют доказательственную базу для суда.

Кроме того, необходимо разграничивать:

– **ОРД и административно-правовую деятельность**. Результаты ОРМ фиксируются в специальных служебных документах (рапортах, справках, актах), а результаты административной практики – в постановлениях, протоколах и иных процессуальных формах, предусмотренных КоАП РФ;

– **ОРД и частную детективную/охранную деятельность**. ОРД носит исключительно государственно-правовой характер (ФЗ «Об оперативно-розыскной деятельности»), тогда как Закон Российской Федерации от 11 марта 1998 г. № 2487-1 «О частной детективной и охранной деятельности» регулирует негосударственную деятельность, осуществляемую на основании лицензии.

Частные детективы вправе: опрашивать граждан, наводить справки, изучать документы (с согласия владельцев), вести внеш-

нее наблюдение, использовать аудио- и видеозапись (без ущерба для жизни и здоровья граждан).

При этом им строго запрещено выдавать себя за сотрудников правоохранительных органов и проводить ОРМ, относящиеся к исключительной компетенции государственных органов.

Таким образом, современная правовая система России выстроила четкую базу для разграничения различных видов правоохранительной деятельности. Это обеспечивает баланс с одной стороны, – эффективность выявления и пресечения преступлений, с другой – надежную защиту конституционных прав и свобод граждан.

Правовая регламентация (ФЗ «Об ОРД», подзаконные акты, ведомственные инструкции) детально определяет порядок фиксации и оформления результатов оперативно-разыскных мероприятий, что позволяет использовать их как в уголовном процессе, так и в иных правоохранительных целях.

§ 3. Общие и основные требования к оформлению результатов оперативно значимой информации в информационно-телекоммуникационных сетях

Как отмечалось ранее, практически все ОРМ, предусмотренные Федеральным законом «Об оперативно-розыскной деятельности», могут проводиться как в традиционной среде, так и в информационно-телекоммуникационных сетях. **Принципиальное отличие работы в сети Интернет заключается в применении программно-технических средств для получения, обработки и фиксации оперативно значимой информации. Однако все правовые требования, установленные для реальных условий, в равной мере распространяются и на виртуальное пространство**.

Согласно п. 36.1 ст. 5 УПК РФ результаты ОРД представляют собой фактические данные, полученные в установленном порядке, которые указывают на признаки подготавливаемого, совершаемого или совершенного преступления, а также на лиц, причастных к нему. В силу ст. 10 Федерального закона «Об оперативно-разыскной деятельности» такие данные подлежат обязательному документированию.

Формы документирования. Результаты ОРД фиксируются в оперативно-служебных документах (рапортах, справках, актах, отчетах и др.), а также в делах оперативного учета (ДОУ). Дополнительно допускается использование любых материальных носителей: фонограмм, видеозаписей, фотографий, магнитных и лазерных дисков и т. п. Наиболее надежным способом считается **видеофиксация**, которая позволяет отразить не только результат, но и сам процесс проведения ОРМ, обеспечивая тем самым более высокую доказательственную ценность материалов.

Проблема правового регулирования. Законодательство не устанавливает единой формы оперативно-служебных документов. Эти вопросы регулируются ведомственными актами, зачастую секретными или рекомендательного характера. Вследствие этого на практике возникают проблемы:

– несвоевременное составление документов;

– фиксация по памяти, что снижает достоверность;

– отсутствие единообразия и противоречия в правоприменительной практике разных регионов.

Значение результатов ОРД. Результаты ОРМ представляются дознавателю, следователю или в суд и могут быть использованы для:

– возбуждения уголовного дела;

– подготовки и проведения следственных и судебных действий;

– признания доказательствами в уголовном процессе (при соблюдении требований УПК РФ).

Процедура передачи материалов. Передача осуществляется только на основании постановления руководителя оперативного подразделения (или его заместителя), которое подтверждает законность действий и необходимость проверки полученных данных. Процесс включает:

1. Вынесение постановления руководителем подразделения.
2. Оформление сопроводительных документов, подтверждающих законность и содержание материалов.
3. Фактическую передачу материалов (почтой, на́рочным или иным установленным способом).

Ограничения и **гарантии**

– При передаче материалов, связанных с ограничением конституционных прав граждан (например, тайна переписки, телефонных переговоров, неприкосновенность жилища), к ним обязательно прилагаются копии судебных решений, разрешающих проведение ОРМ.

– Следователи и суды **не вправе требовать** предоставления внутренних оперативно-служебных документов (рапортов, инструкций, методик), если это противоречит принципу конспирации.

– Сведения о методах, средствах и лицах, участвующих в ОРМ, составляют государственную тайну. Передача таких материалов возможна только в порядке, установленном законом «О государственной тайне».

Таким образом, оформление результатов ОРД в информационно-телекоммуникационных системах требует строгого соблюдения баланса: с одной стороны, – обеспечение процессуальной

значимости и доказательственной силы материалов, с другой – сохранение конспирации и соблюдение конституционных прав граждан.

Таблица 25

Основные требования к оформлению результатов ОРД

Требование	Содержание
Законность	Документы должны составляться в рамках ФЗ «Об ОРД» и иных нормативных актов
Достоверность	Вся зафиксированная информация должна точно соответствовать реальным фактам
Своевременность	Документы составляются сразу после проведения ОРМ, а не по памяти
Полнота	Указываются все необходимые сведения: кто, где, когда, какие действия проводил
Сохранность	Материалы должны храниться в установленном порядке, исключающем подмену или утрату
Конфиденциальность	Сведения о методах, средствах и лицах-источниках составляют гостайну и защищаются

Комментарий к таблице «Основные требования к оформлению результатов ОРД»

– **Законность** – если документ оформлен с нарушением ФЗ «Об ОРД», его просто отвергнет суд. Например, если оперативник провел обследование жилища без судебного разрешения и оформил акт – такие материалы будут признаны недопустимыми.

– **Достоверность** – ошибка в фамилии, времени или месте проведения ОРМ может поставить под сомнение все дело.

– **Своевременность** – рапорт по памяти через неделю почти всегда вызывает вопросы у прокурора и суда.

– **Полнота** – если не указать, кто именно участвовал в ОРМ или каким прибором велась запись, документ считается пустым.

– **Сохранность** – примеры потери носителей (категорированной флешки) демонстрируют: даже важнейшая информация обесценивается без правильного хранения.

– **Конфиденциальность** – нельзя раскрывать агентурные источники в открытых документах: их данные фиксируются с грифом секретности и передаются особым порядком.

§ 4. Порядок оформления результатов получения оперативно значимой информации в информационно-телекоммуникационных сетях

В большинстве уголовных дел обвинение строится на сведениях, полученных в ходе ОРД. Однако принципиальное значение имеет то, как именно оформлена эта информация и каким образом она передана в уголовное дело. Конституционный Суд Российской Федерации неоднократно подчеркивал: сами по себе результаты ОРМ не являются доказательствами, а лишь информацией, которая может обрести доказательственное значение только после правильного процессуального оформления и приобщения к делу (например, определение Конституционного Суда Российской Федерации от 29 января 2019 г. № 75-О).

Иными словами, добыть сведения – недостаточно; необходимо грамотно оформить их документально. В противном случае данные, даже достоверные, теряют юридическую силу. Практика показывает, что на оформление у оперативного сотрудника уходит порой больше времени, чем на сам процесс добывания информации.

Ключевая мысль: доказательствами по уголовному делу могут быть только те сведения, которые получены и оформлены

в соответствии с Уголовно-процессуальным кодексом Российской Федерации. Все материалы, добытые вне рамок УПК РФ (например, в соответствии с Федеральным законом № 144-ФЗ «Об оперативно-розыскной деятельности» или Федеральным законом «О полиции»), должны пройти установленную законом процедуру передачи и приобщения к делу.

Этапы оформления результатов ОРД

1. **Получение информации.** Например, на сайте «Новости СВО» обнаружены экстремистские призывы. На основании этих данных проводится ОРМ под названием «наведение справок с использованием сети Интернет» (по сути – специальный поисковый запрос).

2. **Документирование основания.** Первичный документ (рапорт, сообщение конфидента и т. п.) должен быть датирован *до проведения ОРМ*. Это подтверждает законность мероприятия и исключает сомнения в его основании.

3. **Оформление результатов.** Выявленные сведения (например, данные об аккаунте с экстремистскими публикациями) фиксируются в документе установленного формата – рапорте, справке или акте. Только после этого информация приобретает статус **результатов ОРД**.

Формы фиксации результатов ОРД

Результаты оформляются в виде:

– рапортов;

– справок;

– актов;

– агентурных сообщений;

– объяснений граждан и иных документов.

При этом важно различать: сами документы лишь фиксируют сведения, но не являются результатами ОРД в чистом виде. **Результаты ОРД** – это фактические данные, которые могут содержаться:

– в оперативно-служебных документах;

– в аудио-, фото- и видеозаписях;

– в сообщениях конфиденциальных источников;

– в показаниях очевидцев и участников мероприятий.

Требования к оформлению

Результаты ОРД признаются таковыми только при условии, что они получены в рамках законных оперативно-разыскных мероприятий. Даже достоверная информация (например, видеозапись преступления) не будет иметь процессуального значения, если не зафиксирована как результат конкретного ОРМ.

С точки зрения прокурорского надзора оперативным сотрудникам не рекомендуется оформлять материалы в виде **протоколов**: этот формат характерен для уголовного и административного процессов. Использование протоколов в ОРД способно вызвать сомнения в законности действий.

Исключение: при проведении гласных ОРМ, связанных с изъятием документов или предметов, протокол обязателен. В таком случае применяются требования ст. 166 УПК РФ: участникам мероприятия разъясняются права, предоставляется возможность вносить замечания, указывается факт применения технических средств. Несоблюдение этих правил делает результаты недопустимыми доказательствами.

Справки и аналитические материалы

При ведении дел оперативного учета допускается составление:

– справок-меморандумов;

– обзорных и аналитических материалов;

– сводок и обобщений.

В них могут содержаться производные сведения, основанные на ранее полученной информации. Однако для придания им юридической силы необходимо приложить все первичные материалы: аудио- и видеозаписи, технические носители и т. п.

Обязательные реквизиты документа

Каждый оперативно-служебный документ должен содержать:

– данные о составителе;

– место, время и дату составления;

– описание проведенных действий;

– сведения о лицах, участвовавших в ОРМ;

– информацию о технических средствах и их использовании;

– подпись должностного лица.

Таким образом, грамотное оформление результатов ОРД – это не формальность, а ключевой этап, определяющий их допустимость в уголовном процессе. Любое нарушение требований к документированию может привести к тому, что ценная информация будет исключена из доказательственной базы.

Таблица 26

Документы ОРД vs Процессуальные документы

Критерий	Документы ОРД	Процессуальные документы
Примеры	Рапорт, справка, акт, агентурное сообщение	Протокол допроса, протокол осмотра, постановление
Правовая база	ФЗ «Об ОРД», ведомственные инструкции	УПК РФ, КоАП РФ
Назначение	Фиксация сведений, добытых в ходе ОРМ	Фиксация процессуальных действий и доказательств
Обязательные реквизиты	Составитель, дата, место, описание действий	Составитель, дата, место, разъяснение прав, подписи участников
Статус в суде	Сами по себе доказательствами не являются	Являются полноценными доказательствами
Форма	Свободная (регламентируется ведомственными актами)	Строго формализованная, закреплена в УПК РФ
Конспирация	Высокая, часто содержит сведения о методах и источниках	Гласность, возможен доступ сторон процесса

Комментарий к таблице «Документы ОРД vs Процессуальные документы»

– **Рапорт ≠ доказательство.** Рапорт сотрудника о том, что «на сайте выявлены экстремистские материалы», – еще не доказательство. Но именно на его основании может быть возбуждено уголовное дело.

– **Протокол = доказательство.** Протокол допроса свидетеля, оформленный по УПК РФ, имеет статус полноценного доказательства в суде.

– **Разница в форме.** Рапорт можно составить в свободной форме («докладываю, что…»), а вот протокол строго фиксируется по требованиям ст.ст. 166–170 УПК РФ: с подписями, разъяснением прав, отметками об использовании техники.

– **Разница в целях.** Документы ОРД нужны для передачи информации от оперативников следователю. Процессуальные документы – уже для юридической упаковки этой информации, чтобы она стала доказательством в суде.

4.1. Типичные ошибки при документировании ОРМ

Несмотря на кажущуюся простоту оформления результатов ОРМ, на практике у оперативных сотрудников часто возникают трудности.

Во-первых, в специальной литературе встречаются разные термины: **«оперативные данные»**, **«оперативная информация»**, **«оперативно значимая информация»**. Они близки по смыслу, но **«результаты ОРД»** – понятие более узкое. Оно относится только к сведениям, полученным оперативно-разыскным путем. В то время как оперативная информация может поступать и из иных источников: от участковых уполномоченных, общественных организаций или даже анонимных заявителей.

Во-вторых, при документировании ОРМ должностные лица оперативно-разыскных органов допускают ряд **типичных ошибок**, которые могут привести к признанию материалов недопустимыми. Среди них:

– **Отсутствие постановления руководителя ОРО** о проведении ОРМ (проверочная закупка, оперативный эксперимент и др.) либо его несвоевременное вынесение или утверждение ненадлежащим должностным лицом.

– **Неверное или неполное указание оснований проведения ОРМ**: в рапортах и постановлениях либо вовсе отсутствует ссылка на основание, либо приводятся сведения, которые не могут рассматриваться в качестве законных.

– **Ошибки в названии мероприятия**: вместо «проверочная закупка» пишут «контрольная покупка», «закупка под контролем» и т. п.; используется неконкретная формулировка «проведенным оперативно-разыскным мероприятием установлено…».

– **Подписи посторонних лиц**: акты и справки подписываются сотрудниками, не имеющими отношения к оперативным подразделениям (например, ППС, ДПС, вневедомственная охрана).

– **Использование понятых «по правилам УПК»**: в оперативных документах отражается участие «понятых» с разъяснением им прав и обязанностей по ст. 60 УПК РФ, что недопустимо, так как ОРД регулируется иным законом.

– **Неправильная процессуальная форма**: по итогам ОРМ, направленных на выявление преступления, составляется протокол об административном правонарушении – что юридически неверно.

– **Неверные ссылки на законы**: при изъятии денег, оружия, наркотиков или техники составляются так называемые акты досмотра, протоколы изъятия со ссылками на ФЗ «О полиции», ФЗ «О наркотических средствах», КоАП РФ или УПК РФ, но без обязательной ссылки на ст. 15 ФЗ «Об ОРД». Это грубое нарушение.

– **Нарушения при изъятии предметов**: изъятые вещи не описываются подробно, не упаковываются должным образом, отсутствуют отметки о пломбировании и сохранности.

Вывод. Эти не просто формальные ошибки. Они могут привести к тому, что собранные материалы будут признаны **недопустимыми доказательствами** и не смогут использоваться в уголовном процессе. Поэтому знание правил документирования и внимательность при их применении – это основа профессиональной работы сотрудника оперативного подразделения.

Таблица 27

Типичные ошибки при документировании ОРМ и их последствия

Ошибка	В чем проявляется	Чем грозит
Нет постановления руководителя ОРО	Постановление о проведении ОРМ не вынесено, вынесено поздно или подписано неуполномоченным лицом	Результаты признаются незаконными, материалы исключаются из уголовного дела
Неправильные или отсутствующие основания	В документах отсутствуют ссылки на основания проведения ОРМ или указаны недостоверные сведения	Нарушение законности, возможность отмены материалов прокурором или судом
Неверное название ОРМ	Проверочная закупка названа контрольной покупкой, используется формулировка «проведенным ОРМ установлено…»	Сомнения в достоверности, риск признания документов ненадлежащими
Подписи посторонних лиц	Акты/справки подписывают сотрудники ППС, ДПС, вневедомственной охраны	Потеря юридической силы документа
Использование понятых по УПК	В оперативных документах указываются «понятые» с разъяснением прав по ст. 60 УПК РФ	Подмена процессуальных действий ОРМ, возможное признание материалов недопустимыми
Протокол вместо рапорта	По результатам ОРМ составляется протокол об административном правонарушении	Документ не соответствует природе ОРМ, риск отказа суда принять материалы
Неверные ссылки на законы	В документах ссылаются на ФЗ «О полиции», КоАП РФ или УПК РФ вместо ст. 15 ФЗ «Об ОРД»	Нарушение правовой основы, возможность исключения результатов из дела
Нарушения при изъятии предметов	Отсутствует описание, упаковка, пломбирование, отметки о сохранности	Утрата вещественных доказательств, невозможность использования в суде

Ошибки в оформлении ОРМ не менее опасны, чем ошибки в самой работе. Даже если удалось получить ценную информацию, ее можно потерять из-за формальных нарушений. Поэтому каждое действие должно быть не только эффективным, но и юридически безупречным.

Памятка как избежать ошибок при документировании ОРМ

1. **Всегда выносите постановление.**

Перед началом ОРМ должно быть постановление руководителя ОРО.

Проверяйте подпись и дату.

2. **Указывайте основания.**

В рапортах и постановлениях обязательно прописывайте, на каком основании проводится ОРМ (ст.ст. 7, 8 ФЗ «Об ОРД»).

3. **Точно называйте ОРМ.**

Используйте формулировки закона: «проверочная закупка», «оперативное наблюдение», «опрос».

Избегайте самодельных названий.

4. **Подписи только сотрудников ОРО.**

Все служебные документы должны быть подписаны уполномоченными оперативными сотрудниками.

5. **Не путайте ОРМ и следственные действия.**

Для ОРМ – рапорт, справка, акт.

Для следственных действий – протокол (УПК РФ).

6. **Правильно ссылайтесь на закон.**

В документах используйте только Федеральный закон «Об ОРД».

Не ссылайтесь на УПК РФ или КоАП РФ, если речь идет об ОРМ.

7. **Корректно оформляйте изъятие предметов.**

Подробное описание, упаковка, пломбы, подписи.

Сохранность и целостность – обязательное условие.

8. **Фиксируйте все своевременно.**

Документ должен быть составлен сразу после проведения ОРМ, а не по памяти.

Даже самая ценная информация теряет юридическую силу, если она неправильно оформлена.

Таблица 28

Типичные ошибки при документировании ОРМ и способы их избежать

Ошибка	Как избежать
Постановление руководителя ОРО о проведении ОРМ не вынесено, вынесено с опозданием или не подписано надлежащим лицом	Всегда оформляйте постановление до начала ОРМ; проверяйте подпись и дату
В документах отсутствуют основания для проведения ОРМ	Четко указывайте основания (ст.ст. 7, 8 ФЗ «Об ОРД»)
Неправильно названы мероприятия («контрольная покупка» вместо «проверочной закупки»)	Используйте официальные формулировки из закона
Документы подписывают сотрудники, не относящиеся к ОРО (ППС, ДПС и т. д.)	Подписи ставят только уполномоченные сотрудники ОРО
Упоминание «понятых» в ОРМ, как при следственных действиях	Не путайте ОРМ с процессуальными действиями УПК РФ
Результаты оформлены протоколом, а не рапортом/справкой	Для ОРМ используйте рапорты, справки, акты; протокол – только для следственных действий
В документах ссылаются на УПК РФ или КоАП РФ вместо ФЗ «Об ОРД»	Ссылайтесь только на Закон «Об ОРД» и ведомственные акты
Изъятые предметы не описаны и не упакованы	Всегда описывайте предметы подробно, упаковывайте, пломбируйте, подписывайте
Документы составлены по памяти через несколько дней	Фиксируйте результаты ОРМ сразу после их проведения

4.2. Представление результатов ОРД

Оперативно значимая информация, полученная в ходе ОРМ с использованием ИТКС, после документального оформления подлежит передаче в органы дознания, следствия, прокурору или в суд.

Порядок представления таких результатов регулируется:

– **статьей 11 Федерального закона «Об оперативно-розыскной деятельности»**;

– **ведомственными нормативными актами**, в том числе Межведомственной инструкцией о порядке представления результатов ОРД.

Формы представления результатов ОРД.

1. **Рапорт об обнаружении признаков преступления** (с приложением оперативных материалов).

2. **Сообщение о результатах ОРД** (служебная форма передачи информации).

В обоих случаях обязательным условием является **вынесение постановления руководителем оперативного подразделения** о представлении результатов ОРД.

4.2.1. Структура постановления (3 части)

1. **Вводная** – наименование документа, дата, место составления, данные руководителя.

2. **Описательная** – сведения о времени, месте и ОРМ, в результате которого получены данные; цель представления (например, возбуждение уголовного дела); данные о санкционировании мероприятия (при необходимости – судебное решение).

3. **Резолютивная** – решение о направлении документов и **перечень всех материалов**, которые передаются.

Постановление оформляется в **двух экземплярах**:

– один передается следователю или дознавателю;

– второй подшивается в дело оперативного учета (ДОУ).

4.2.2. Важное условие допустимости

Результаты ОРД могут использоваться в уголовном процессе **только при наличии постановления о представлении результатов** и его соответствии требованиям ФЗ «Об ОРД». Если

постановление не приобщено к материалам уголовного дела, собранные сведения могут быть признаны недопустимыми доказательствами.

4.2.3. Рапорт об обнаружении признаков преступления

Рапорт составляет оперативный сотрудник и регистрирует его в установленном порядке.

Содержание рапорта:

– изложение сообщения о преступлении;

– источник информации;

– данные составителя (должность, звание, ФИО);

– дата и подпись.

Рапорт является **поводом для возбуждения уголовного дела** и передается для проверки в порядке ст.ст. 144–145 УПК РФ.

Алгоритм составления рапорта:

1. Оперативный сотрудник составляет рапорт.

2. Рапорт регистрируется в КУСП.

3. Начальник органа ОРД передает его вместе с материалами.

4. Выносится постановление с указанием всего передаваемого.

5. Следователь приобщает результаты ОРД к материалам уголовного дела.

Таблица 29

Этапы представления результатов ОРД

Этап	Субъект	Действие	Документ
1	Оперативный сотрудник	Составляет рапорт об обнаружении признаков преступления	**Рапорт**
2	Дежурная часть / подразделение	Регистрирует сообщение в **Книге учета сообщений о преступлениях (КУСП)**	Отметка в КУСП

Окончание табл. 29

3	Начальник органа ОРД	Принимает решение о передаче материалов, утверждает постановление	Постановление о представлении результатов ОРД
4	Начальник органа ОРД	Передает рапорт и все материалы (аудио, видео, фото, справки, акты)	Сопроводительное письмо / перечень приложений
5	Следователь (или дознаватель)	Принимает материалы, проверяет постановление, приобщает к делу	Постановление о приобщении

4.3. Особенности представления результатов ОРД

Представление результатов ОРД в следственные органы, прокурору или в суд имеет ряд особенностей и осуществляется поэтапно:

1. **Рассекречивание сведений.** Если материалы ОРД содержат сведения, составляющие государственную тайну (методы, средства, личности участников ОРМ), принимается решение о возможности рассекречивания. Постановление выносится руководителем оперативного подразделения. В случае невозможности рассекречивания материалы передаются в соответствии с требованиями Закона «О государственной тайне».

2. **Оформление документов.** Передача результатов осуществляется сопроводительным письмом, подписанным руководителем подразделения. В письме перечисляются все документы и предметы, подлежащие передаче, что обеспечивает прозрачность и законность процедуры.

3. **Фактическая передача материалов.** Материалы могут передаваться по почте, с нарочным или иным установленным способом. Обязательным является обеспечение целостности

и сохранности: защита от повреждений, размагничивания, стирания данных.

Для приобщения результатов ОРД к уголовному делу в обязательном порядке представляются:

– постановление о представлении результатов ОРД;

– постановление о проведении ОРМ;

– судебное решение (в случаях ограничения конституционных прав граждан).

Передаваемые материалы должны включать сведения:

– о времени, месте и обстоятельствах изъятия документов или предметов;

– о примененных технических средствах (аудио-, видеозапись, фотосъемка и др.) с указанием их характеристик;

– о способах упаковки и опечатывания изъятых предметов.

Важно: справки-меморандумы с оперативно-разыскной информацией имеют **ориентирующее значение** и не могут служить самостоятельным основанием для возбуждения уголовного дела или проведения процессуальных действий.

Типичные ошибки при представлении результатов ОРД

– **Отсутствие постановления.** При его отсутствии результаты могут быть признаны недопустимыми.

– **Неправильное оформление.** Ошибки в указании оснований проведения ОРМ, некорректные названия мероприятий, искажение данных участников.

– **Нарушение порядка изъятия.** Отсутствие описания предметов, их упаковки и опечатывания.

– **Неправомочность подписантов.** Подписание документов лицами, не уполномоченными на это.

Таким образом, ключевая проблема использования результатов ОРД в уголовном процессе заключается в ошибках оформления. Эти недочеты фиксируются в оперативно-служебных документах, передаются в материалы уголовного дела и могут быть использованы стороной защиты для признания доказательств недопустимыми. В итоге исключаются не только материалы ОРД, но и производные доказательства, полученные в ходе предварительного следствия.

Таблица 30

Этапы представления результатов ОРД и типичные ошибки

Этап	Правильные действия	Типичные ошибки
1. Рассекречивание сведений	Постановление руководителя ОРО о рассекречивании материалов или передача по Закону «О государственной тайне»	Материалы переданы без рассекречивания; отсутствует постановление; сокрытие факта использования негласных методов
2. Сопроводительное письмо	Подписывается руководителем подразделения; подробно указаны документы и предметы	Подписано неправомочным лицом; перечень неполный; ошибки в реквизитах
3. Фактическая передача материалов	Передача по установленному порядку (почтой, нарочным и др.); обеспечена сохранность и целостность	Нарушение упаковки и опечатывания; повреждение носителей; утрата части материалов
4. Приобщение к делу	Материалы приобщаются следователем на основании постановления руководителя ОРО	Приобщение без постановления; справки-меморандумы используются как доказательства; нарушение порядка проверки законности

4.4. Особенности проведения ОРМ в сети Интернет

Проведение ОРМ в сети Интернет имеет ряд принципиальных особенностей, которые отличают их от традиционных форм работы в реальной среде. Интернет – это глобальная децентрали-

зованная инфраструктура, где отсутствуют строгие национальные границы, а информация распространяется мгновенно и может быть удалена в считанные минуты. Все это усложняет задачу правоохранительных органов по фиксации и использованию полученных сведений.

1. Специфика Интернета как объекта ОРД

– **Анонимность и псевдонимность**: преступники используют VPN, TOR, прокси-серверы и анонимайзеры, что затрудняет их идентификацию.

– **Транскордонность**: серверы и аккаунты могут находиться за пределами России, что требует международного сотрудничества (Интерпол, соглашения СНГ, конвенция Будапешта о киберпреступности).

– **Динамичность информации**: цифровые данные легко изменяются и уничтожаются; фиксация в режиме реального времени становится ключевой задачей.

– **Обилие платформ**: социальные сети, мессенджеры, форумы, даркнет-площадки – каждая имеет собственную архитектуру и особенности сбора данных.

2. Виды ОРМ, применяемых в сети Интернет

В соответствии с Федеральным законом «Об оперативно-розыскной деятельности» в виртуальном пространстве чаще всего реализуются:

– **наблюдение (мониторинг)** за веб-ресурсами, чатами, форумами, где могут вестись обсуждения противоправных действий;

– **наведение справок** через поисковые системы и специальные базы данных (WHOIS, реестры IP-адресов и доменов);

– **снятие информации с технических каналов связи** (на основании судебного решения);

– **оперативный эксперимент** (например, имитация покупки наркотических средств на теневой площадке);

– **контроль почтовых отправлений в электронной форме** (переписка, пересылка файлов);

– **оперативное внедрение** – создание подставных аккаунтов, участие в закрытых сообществах для сбора информации.

§ 5. Основные НПА, регулирующие проведение ОРМ в сети Интернет

1. **Конституция Российской Федерации** (принята всенародным голосованием 12 декабря 1993 г., с поправками 2020 г.).

2. **Уголовный кодекс Российской Федерации** от 13 июня 1996 г. № 63-ФЗ (ред. 2024).

3. **Уголовно-процессуальный кодекс Российской Федерации** от 18 декабря 2001 г. № 174-ФЗ (ред. 2024).

4. **Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Обоперативно-розыскной деятельности»** (ред. 2023).

5. **Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Обинформации, информационных технологиях и о защите информации»** (ред. 2024).

6. **Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»** (ред. 2024).

7. **Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»** (ред. 2024).

8. **Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности»** (ред. 2024).

9. **Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»** (ред. 2024).

10. **Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне»** (ред. 2023).

11. **Постановление Правительства Российской Федерации от 31 июля 2014 г. № 759 «Об утверждении Правил вза-**

имодействия операторов связи с органами, осуществляющими оперативно-розыскную деятельность» (с изм. 2022).

12. **Приказ ФСБ России от 19 декабря 2017 г. № 639 «Об утверждении Административного регламента… по реализации требований к СОРМ»**.

13. **Межведомственная инструкция о порядке представления результатов оперативно-розыскной деятельности органам дознания, предварительного следствия и в суд** (утв. совместным приказом Генпрокуратуры Российской Федерации, МВД России, ФСБ России, ФТС России и др. от 17.04.2007 № 89/276/149/59/26/18).

При этом остается проблема: ни один нормативный акт не содержит исчерпывающего порядка проведения ОРМ именно в сети Интернет, что приводит к коллизиям и требует ведомственных инструкций (МВД России, ФСБ России и др.).

Таблица 31

НПА, регулирующие проведение ОРМ в Интернете

Уровень регулирования	Нормативный акт	Содержание и значение
Конституционный	**Конституция Российской Федерации (1993, ред. 2020)**	Закрепляет права и свободы человека и гражданина (тайна переписки, личная жизнь, жилище). Допускает их ограничение только законом для защиты безопасности государства, общества и личности
Уголовный и процессуальный	**УК РФ от 13.06.1996 № 63-ФЗ (ред. 2024)**	Определяет уголовную ответственность за киберпреступления, хищения, терроризм и др.
	УПК РФ от 18 декабря 2001 № 174-ФЗ (ред. 2024)	Регламентирует порядок использования результатов ОРМ в доказывании, закрепляет требования к процессуальным документам

Продолжение табл. 31

Базовый для ОРД	**ФЗ от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»**	Устанавливает виды ОРМ, основания их проведения, порядок документирования и представления результатов
Информационно-правовой	**ФЗ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»**	Регулирует правовой режим информации, порядок доступа к ней, защиту данных в ИТКС
	ФЗ от 7 июля 2003 г. № 126-ФЗ «О связи»	Определяет обязанности операторов связи, в том числе взаимодействие с органами ОРД, порядок хранения данных (СОРМ)
	ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»	Устанавливает правила обработки и защиты персональных данных, используемых в ходе ОРМ
Специальный для служб	**ФЗ от 3 апреля 1995 г. № 40-ФЗ «О ФСБ»**	Закрепляет задачи и полномочия ФСБ России, включая проведение ОРМ в сфере кибербезопасности
	ФЗ от 7 февраля 2011 г. № 3-ФЗ «О полиции»	Определяет полномочия полиции, включая проведение ОРМ и взаимодействие с операторами связи
	ФЗ от 21 июля 1993 г. № 5485-1 «О государственной тайне»	Устанавливает режим секретности в части методов, средств и лиц, участвующих в ОРМ
Подзаконные акты	**Постановление Правительства Российской Федерации от 31 июля 2014 г. № 759**	Утверждает правила взаимодействия операторов связи с органами, осуществляющими ОРД
	Приказ ФСБ России от 19 декабря 2017 г. № 639	Определяет порядок реализации требований к СОРМ (системам оперативно-разыскных мероприятий)

Окончание табл. 31

Межведомственный уровень	**Инструкция о порядке представления результатов ОРД (Приказ Генпрокуратуры России, МВД России, ФСБ России, ФТС России и др. от 17 апреля 2007 г. № 89/276/149/59/26/18)**	Регламентирует порядок оформления и передачи результатов ОРД в органы дознания, следствия и суд

Пример применения НПА: документирование переписки экстремистов в Telegram

1. **Основание для проведения ОРМ.**

ФЗ № 144-ФЗ «Об ОРД», ст.ст. 7, 8 – наличие сведений о подготовке преступления (экстремизм).

Постановление руководителя ОРО о проведении ОРМ («снятие информации из каналов связи» или «оперативный эксперимент»).

2. **Использование средств связи и Интернета.**

ФЗ № 126-ФЗ «О связи» – оператор обязан обеспечить подключение к СОРМ (система оперативно-розыскных мероприятий).

Приказ ФСБ России № 639 (2017) – устанавливает порядок использования СОРМ для перехвата сообщений.

3. **Трудности документирования.**

– **Проблема подлинности**: необходимо обеспечить возможность верификации скриншотов, логов, переписки (цифровая подпись, протоколы хэширования).

– **Формат доказательств**: материалы должны быть представлены в пригодном для судебного рассмотрения виде (электронные носители, заверенные копии).

– **Сохранность**: цифровые файлы подвержены искажению и утрате, поэтому требуется дублирование и хранение на защищенных серверах.

– **Процессуальные риски**: если информация зафиксирована с нарушением закона (например, без постановления суда при съеме данных с трафика), она будет признана недопустимым доказательством.

1. **Практические рекомендации для сотрудников ОРО.**

– Всегда фиксировать дату и время получения информации (например, при скриншотах указывать системное время, URL, идентификаторы страниц).

– Использовать сертифицированные программно-технические средства фиксации (например, ПО для протоколирования сетевого трафика).

– При изъятии цифровых носителей соблюдать правила упаковки, опечатывания и ведения протокола.

– Все сведения оформлять только через предусмотренные законом документы – рапорты, справки, постановления.

– В случае использования международных сервисов – инициировать запросы о правовой помощи через МИД России и Интерпол.

Таким образом, проведение ОРМ в сети Интернет требует сочетания трех факторов: **строгого соблюдения законодательства, владения современными цифровыми технологиями и грамотного документирования каждого действия**. Только так результаты могут быть признаны допустимыми доказательствами в суде.

2. **Фиксация данных ФЗ № 149-ФЗ «Об информации…»** позволяет фиксировать, хранить и использовать данные в рамках законодательства.

ФЗ № 152-ФЗ «О персональных данных» требует соблюдения режима обработки ПДн, чтобы не нарушать права третьих лиц.

3. **Процессуальное оформление.**

ФЗ № 144-ФЗ, ст. 11 – результаты ОРМ фиксируются в рапорте или справке.

УПК РФ, ст.ст. 86, 89 – данные могут использоваться как доказательства только после их проверки и приобщения к делу.

При необходимости прилагается судебное решение (например, ст. 186 УПК РФ – контроль и запись переговоров).

4. **Режим секретности ФЗ № 5485-1 «О государственной тайне»** – сведения о методах фиксации, конфидентах и технических средствах не подлежат раскрытию.

Рассекречивание допускается лишь для представления материалов в суд.

5. **Передача результатов. Инструкция о порядке представления результатов ОРД (2007)** – передача оформляется постановлением руководителя ОРО, в приложении указываются: текст переписки, ID-аккаунтов, дата и время фиксации, технические средства записи.

Передача осуществляется с сопроводительным письмом, материалы подшиваются в дело оперативного учета.

Пример ситуации: в чате Telegram выявлена переписка, где участники обсуждают изготовление взрывных устройств.

– На основании ст. 7 ФЗ «Об ОРД» оперативники инициируют ОРМ «снятие информации из каналов связи».

– С помощью СОРМ фиксируются IP-адреса, даты и содержание переписки.

– Составляется рапорт, прилагаются скриншоты и расшифровки сообщений.

– Материалы направляются в СК России с постановлением руководителя ОРО.

– Суд, опираясь на представленные результаты, выносит решение о проведении обыска и задержания фигурантов.

Учебно-методический раздел к главе 13

Цели изучения темы

1. Освоить понятие «оперативно значимая информация», уяснить роль информации в правоохранительной деятельности.

2. Изучить нормативную правовую базу оформления результатов ОРД с использованием ИТКС.

3. Научиться правильно фиксировать, хранить и оформлять результаты получения информации в цифровой среде.

4. Изучить требования к обеспечению достоверности, законности и процессуальной значимости полученных данных.

5. Развить практические навыки документирования результатов мониторинга, перехвата, анализа трафика и иных способов получения информации в ИТКС.

Теоретические вопросы для обсуждения

1. Что такое оперативно значимая информация в контексте ИТКС?

2. Какие нормативные акты регулируют порядок ее получения и оформления?

3. Чем отличается фиксация цифровых данных от традиционных форм документирования?

4. Какие требования предъявляются к электронным доказательствам в судопроизводстве?

5. Как обеспечить непрерывность цепочки хранения (chain of custody) цифровых данных?

6. Какие технические средства используются для фиксации информации (системы мониторинга, протоколы перехвата, цифровые регистраторы)?

7. Каковы основные ошибки при оформлении материалов и чем они могут повлиять на результаты расследования?

Практическое задание

1. Анализ нормативной базы.

Найдите и изучите статьи ФЗ «Об оперативно-розыскной деятельности» и УПК РФ, касающиеся фиксации информации в цифровой форме.

Подготовьте краткий конспект с выделением ключевых требований.

2. Составление протокола.

На основе смоделированной ситуации (перехват сетевого трафика, выявление подозрительного IP-адреса) составьте протокол получения оперативной информации.

Учтите требования к реквизитам: дата, место, должностное лицо, описание объекта, способ получения, средства фиксации.

3. Практика по цепочке хранения (Chain of Custody).

Разработайте схему передачи цифрового носителя (жесткий диск, флешка, серверные логи) от оперативного сотрудника к экспертному подразделению.

Укажите все необходимые подписи, даты и печати.

4. Кейс-анализ.

Разберите реальный судебный кейс, где цифровые доказательства были признаны недопустимыми из-за нарушений при

оформлении. Укажите, что было сделано неправильно и как нужно было действовать.

Практическое задание «Документирование переписки экстремистов в Telegram»

Оперативное подразделение ФСБ России получило информацию о том, что в одном из телеграм-чатов группа пользователей обсуждает изготовление взрывных устройств и проведение несанкционированной акции.

Необходимо:

1. Выявить признаки преступления.
2. Провести ОРМ.
3. Зафиксировать результаты.
4. Оформить документы так, чтобы они могли быть использованы в уголовном процессе.

Этап 1. Основание для проведения ОРМ

– Проверка информации о признаках преступления (ст. 7 ФЗ № 144-ФЗ «Об ОРД»).

– Постановление руководителя оперативного подразделения о проведении ОРМ «снятие информации из каналов связи».

Задание: назовите правовой документ, который обосновывает проведение ОРМ в данной ситуации.

Этап 2. Сбор и **фиксация информации**

– С помощью СОРМ и программных средств фиксируются:

– участники чата (ID, никнеймы, номера телефонов при наличии);

– дата и время сообщений;

— текст переписки;

— вложения (фото, видео, ссылки).

– Фиксация производится в форме:

— скриншотов (заверенных специалистом);

— протокола технической записи;

— приложенных носителей (диски, флешки).

Задание: какие носители информации допустимо использовать при документировании ОРД?

Этап 3. Документирование результатов

Составляются:

– **Рапорт** сотрудника о выявлении признаков преступления.

– **Справка** о проведенном ОРМ с указанием:

— основания (постановление руководителя);

— даты и времени фиксации;

— технических средств (например, ПО для анализа Telegram, сервер СОРМ);

— приложенных материалов (распечатки сообщений, видеофиксация).

Задание: какие обязательные реквизиты должны быть в рапорте (назовите не менее трех)?

Этап 4. Представление материалов

– Руководитель ОРО выносит **постановление о представлении результатов ОРД**.

– Материалы передаются в СК России для возбуждения уголовного дела (ст.ст. 144-145 УПК РФ).

– Если в ходе ОРМ ограничивались конституционные права (перехват сообщений), прилагается судебное решение.

Задание: что произойдет, если постановление о представлении результатов ОРД не будет приобщено к делу?

Этап 5. Использование в **уголовном процессе**

– Следователь проверяет законность и достоверность материалов.

– При положительной проверке результаты ОРД приобщаются к делу как доказательства.

– На их основании суд может санкционировать обыск, арест фигурантов или иные процессуальные действия.

Задание: почему справка-меморандум не может быть основанием для возбуждения уголовного дела?

Необходимо составить **рапорта**, указав:

– дату и место;

– основание для ОРМ;

– краткое содержание переписки;

– выявленные признаки преступления;

– список приложений (распечатки, диски, фото).

Библиографический список к главе 13

Нормативные правовые акты

1. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // СПС «КонсультантПлюс». – URL: мhttps://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 04.09.2025).

2. Уголовно-процессуальный кодекс Российской Федерации : УПК : Федеральный закон № 174-ФЗ : принят Государственной Думой 22 ноября 2001 г. : одобрен Советом Федерации 5 декабря 2001 г. (ред. от 20.03.2025) // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 04.09.2025).

Стандарты

3. Национальный стандарт Российской Федерации. ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения: национальный стандарт Российской Федерации». – М. : Стандартинформ, 2021.

Книги, учебные пособия

4. Егоров, Н. Н. Криминалистика цифрового следа : учебное пособие / Н. Н. Егоров. – СПб. : Питер, 2022.

5. Шаньгин, В. С. Защита информации в компьютерных системах и сетях / В. С. Шаньгин. – М. : Инфра-М, 2021.

6. Жданов, Ю. Н. Киберполиция XXI века. Международный опыт / Ю. Н. Жданов, В. С. Овчинский. – М. : Международные отношения, 2020.

7. Ревенков, П. В. Основы документирования цифровых следов / П. В. Ревенков. – М. : Юрайт, 2023.

Статьи

8. Петров, П. П. Цифровые доказательства и их процессуальная значимость в уголовном судопроизводстве / П. П. Петров // Информационная безопасность. – 2023. – № 2.

ЗАКЛЮЧЕНИЕ

Подводя итог изучению данного учебного пособия, можно отметить, что оно позволило комплексно рассмотреть весь спектр вопросов, связанных с получением, анализом и оформлением оперативно значимой информации в информационно-телекоммуникационных системах. Логика изложения строилась от фундаментальных теоретико-правовых положений к конкретным прикладным аспектам, что обеспечило целостное понимание природы информации и ее значения в современном правоохранительном процессе.

В ходе изучения материала были раскрыты ключевые элементы правовой основы оперативно-разыскной деятельности, ее место и значение в системе защиты национальной и общественной безопасности. Особое внимание уделялось нормативными правовым актам, регламентирующим порядок проведения оперативно-разыскных мероприятий, что позволило понять строгую связь между практикой добывания информации и требованиями законодательства.

Существенную ценность представляет рассмотрение методов получения и обработки данных в условиях цифровой среды. Освоение тактик компьютерной разведки, мониторинга сетевого трафика, анализа конфигурации сетей и работы с социальными платформами формирует у обучающихся устойчивые профессиональные компетенции, необходимые для противодействия современным формам преступности. В равной степени значимым является изучение феномена социальной инженерии, который выступает одним из наиболее уязвимых направлений киберугроз. Знание ее методов и умение разрабатывать меры профилактики создают предпосылки для эффективного обеспечения информационной безопасности.

Особое место в пособии занимает раздел, посвященный оформлению результатов ОРД. Умение грамотно фиксировать сведения, добытые в ходе ОРМ, – необходимое условие их процессуальной легитимности и дальнейшего использования в доказывании. Таким образом, студенты получают представление не только о технической стороне работы, но и о ее юридическом закреплении, что формирует комплексный профессиональный подход.

Значение полученных знаний выходит далеко за рамки учебной аудитории. В условиях постоянного роста киберугроз и усложнения криминальных технологий специалисты, владеющие методами работы с оперативно значимой информацией, становятся ключевым звеном в системе обеспечения национальной безопасности. Их деятельность сочетает в себе техническую грамотность, аналитическое мышление и высокую степень ответственности за соблюдение прав и законных интересов граждан.

В заключение подчеркнем: данное учебное пособие призвано не только вооружить студентов необходимыми знаниями и навыками, но и сформировать у них осознанное понимание социальной значимости выбранной профессии. В условиях стремительного развития информационно-телекоммуникационных технологий специалисты правоохранительных органов должны быть готовы к постоянному совершенствованию, адаптации к новым вызовам и применению передовых методов работы.

Мы убеждены, что полученные знания и навыки станут прочной основой для профессиональной деятельности, помогут молодым специалистам успешно справляться с возложенными задачами и вносить достойный вклад в укрепление правопорядка и развитие системы информационной безопасности Российской Федерации.

Учебное издание

Новикова Онега Юрьевна,
кандидат технических наук

Технологии получения оперативно значимой информации в информационно-телекоммуникационных сетях

Редактор *Доставалов Ю. Н.*
Корректор *Васильевых Е. М.*
Компьютерная верстка *Гридчина Т. А.*

Формат 60×84 1/16. Усл. печ. л. 25,6.
Подписано в печать 16.12.2025. Заказ № 19.
Тираж 70 экз.

Отпечатано в Полиграфическом центре
Московского университета МВД России имени В.Я. Кикотя
https://мосу.мвд.рф, e-mail: support_mosu@mvd.ru