

Федеральное государственное казенное
образовательное учреждение высшего образования
«Дальневосточный юридический институт
Министерства внутренних дел Российской Федерации
имени И. Ф. Шилова»

**ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ:
ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ**

Хабаровск
ДВЮИ МВД России
имени И. Ф. Шилова
2025

УДК 004.8+343.2/.7

ББК 16

И868

Издается по решению редакционно-издательского совета
Дальневосточного юридического института МВД России имени И. Ф. Шилова

Авторский коллектив:

В. А. Минаев (гл. 1–5);
К. М. Бондарь (введение, гл. 1–5, заключение);
В. С. Дунин (гл. 2);
А. С. Толпыгин (гл. 3–5);
В. Ю. Федорович (гл. 4)

Рецензенты:

А. В. Бецков, начальник кафедры информационных технологий
Академии управления МВД России, д-р техн. наук, доц.;
В. В. Молоков, начальник кафедры информационно-правовых дисциплин
и специальной техники Сибирского юридического института
МВД России, канд. техн. наук, доц.

И868 Искусственный интеллект: противодействие
киберпреступности : моногр. / В. А. Минаев, К. М. Бондарь,
В. С. Дунин, А. С. Толпыгин, В. Ю. Федорович; под ред.
В. А. Минаева, К. М. Бондаря ; Дальневост. юрид. ин-т
МВД России имени И. Ф. Шилова. – Хабаровск : РИО
ДВЮИ МВД России имени И. Ф. Шилова, 2025. – 256 с.
ISBN 978-5-9753-0595-4

В монографии систематизированы теоретические представления, обоснована методологическая база, представлены модели и методы для решения задач использования искусственного интеллекта в противодействии киберпреступности.

Издание адресовано преподавателям и адъюнктам образовательных организаций системы МВД России, курсантам и слушателям, обучающимся по специальностям 40.05.01 «Правовое обеспечение национальной безопасности», 40.02.02 «Правоохранительная деятельность», по направлению подготовки 40.03.02 «Обеспечение законности и правопорядка»; сотрудникам органов внутренних дел и других правоохранительных структур, занимающимся вопросами противодействия киберпреступности на базе применения искусственного интеллекта.

УДК 004.8+343.2/.7
ББК 16

ISBN 978-5-9753-0595-4

© ФГКОУ ВО ДВЮИ МВД России
имени И. Ф. Шилова, 2025

ОГЛАВЛЕНИЕ

<i>Предисловие</i>	5
<i>Список сокращений</i>	7
<i>Словарь терминов</i>	11
<i>Введение.....</i>	19
 ЧАСТЬ I. ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ.....	22
 Глава 1. Общие положения.....	22
1.1. Понятийный аппарат в сфере искусственного интеллекта	22
1.2. Информационная и кибербезопасность. Киберпреступность – состояние и тенденции	42
1.3. Искусственный интеллект – новые возможности и новые проблемы	60
1.4. Выводы по главе 1	75
 Глава 2. Задачи противодействия киберпреступности и технологии искусственного интеллекта	76
2.1. Основные направления применения искусственного интеллекта в решении задач правоохранительных органов.....	76
2.2. Решения оперативно-тактических задач органов внутренних дел по борьбе с киберпреступностью	93
2.3. Выводы по главе 2	115
 ЧАСТЬ II. ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ УПРАВЛЕНИЯ БЕСПИЛОТНЫМ ТРАНСПОРТОМ.....	116
 Глава 3. Система моделей и технологий безопасного управления беспилотным транспортом	119
3.1. Моделирование киберугроз системам искусственного интеллекта в управлении беспилотным транспортом.....	119
3.2. Моделирование киберустойчивости и управляемости флотом беспилотных транспортных средств	126
3.3. Классификация моделей безопасного управления беспилотным транспортом	132
3.4. Моделирование защиты беспилотных авиационных средств	135

3.5. Цифровая платформа беспилотных транспортных средств	143
3.6. Выводы по главе 3	160
Глава 4. Решения прикладных задач управления беспилотным транспортом	161
4.1. Кибербезопасность беспилотных авиационных систем мониторинга лесных территорий.....	161
4.2. Экспертно-криминалистическая деятельность.....	165
4.3. Геоинформационные системы в аналитическом обеспечении раскрытия и расследования преступлений.....	173
4.4. Автоматическое распознавание и маршрутизация беспилотных транспортных средств.....	178
4.5. Выводы по главе 4.....	186
Глава 5. Выбор технических и нормативных решений для создания цифровой платформы управления беспилотными системами.....	189
5.1. Международные и национальные стандарты Российской Федерации в области беспилотных авиационных систем.....	189
5.2. Основные технические средства и системы контроля и управления движением беспилотных воздушных судов.....	193
5.3. Развитие технологий современной связи и беспилотный транспорт	205
5.4. Системы искусственного интеллекта как фактор управления безопасностью беспилотных воздушных судов	211
5.5. Выводы по главе 5	215
<i>Заключение</i>	<i>217</i>
<i>Список использованных источников</i>	<i>219</i>

Предисловие

В последнее десятилетие население России, как никогда, ощутило на работе своей компьютерной техники, да и на своих личных кошельках весь негатив киберпреступности. Уже более трети, а в некоторых регионах и до 40 % преступлений совершается с использованием информационно-телекоммуникационных технологий. А электронные мошенники попросту устроили шабаш в виртуальном и, к сожалению, в реальном мире – прогноз на конец 2025 г. неутешителен.

Уже называется цифра в 350 млрд рублей предполагаемых потерь для россиян. Именно столько «планируют» украсть кибермошенники с помощью методов социальной инженерии, фишинга, других своих грязных технологий, разрушая банковские системы и новые способы защиты активов. Мировая динамика кибератак также свидетельствует о том, что уже через два года потери от кибератак составят не менее \$20 трлн.

Киберпреступления, год от года прирастая экспоненциально, вошли в топ криминальных деяний в стране. На это обратил внимание Президент Российской Федерации В. В. Путин на мартовской коллегии Министерства внутренних дел Российской Федерации (далее – МВД России) 2025 года, охарактеризовав сложившуюся ситуацию как вызывающую серьезное социальное напряжение и требующую адекватного противодействия со стороны правоохранительных структур.

Считаю, что авторы монографии, в своей основе представляя образовательные организации системы МВД России, нашли верный ключ в таком противодействии. Их нацеленность на опережающее реагирование органов внутренних дел на текущее состояние и стремительную эволюцию киберпреступности, привела к необходимости привлечения перспективных технологий искусственного интеллекта для решения сложных оперативно-тактических, следственных, криминалистических задач в указанной сфере.

Разделяю также подход авторов к раскрытию прикладных аспектов искусственного интеллекта через характеристику исторических условий, истоков теоретического осмысления, особенностей развития понятийного аппарата рассматриваемых передовых технологий. Это очень важно для становления нового поколения ученых, управленцев и практиков, ориентированных на работу в самых различных подразделениях МВД России.

В этом выражается глубокая философская, духовная и культурная истина, которая должна быть присуща грядущим сотрудникам органов внутренних дел. Именно такая творческая сила даст возможность курсантам и слушателям образовательных организаций раскрыть потенциал полученного знания, облечь его образы в практические воплощения, в решения новых задач борьбы с криминалом.

Святейший Патриарх Кирилл в одном из своих обращений подчеркнул необходимость развития искусственного интеллекта в сочетании с разумным учетом угроз от внедрения данной технологии в разные области жизнедеятельности общества. Этот важный аспект проблемы также обсужден в монографии.

Нужно подчеркнуть, что монографическая работа достаточно глубоко раскрывает практические приложения. Наряду с системным изложением теоретических представлений об искусственном интеллекте, в ней обоснована методологическая база моделей и методов для решения задач с его использованием. А именно, развернуто показаны основные направления применения искусственного интеллекта для решения задач правоохранительных органов, включая борьбу с киберпреступностью.

Конечно же нельзя не отметить научную новизну и практическую значимость для подразделений правоохранительных органов материала о кибербезопасности беспилотных авиационных систем мониторинга лесных территорий, применение такого рода систем в экспертно-криминалистической деятельности, геоинформационных системах при аналитическом обеспечении раскрытия и расследования преступлений, автоматическом распознавании и маршрутизации беспилотных транспортных средств. Всё это новый, очень нужный и полезный материал как применительно к учебному процессу, так и к научно-исследовательской деятельности, а также практической работе подразделений МВД России.

Как системное завершение монографической работы представлена ее завершающая глава, раскрывающая выбор технических и нормативных решений для создания цифровой защищенной платформы управления беспилотными системами. Авторы проделали большую работу, проанализировав достаточно объемную базу международных и национальных стандартов России в области беспилотных авиационных систем, значительно облегчив труд своих последователей, рассмотрев основные технические средства, системы контроля, связи и управления движением беспилотных воздушных судов, и, конечно же, системы искусственного интеллекта как основу безопасного управления ими.

В целом оцениваю монографию как своевременную, нужную и ученым, и преподавателям, и обучающимся, и практикам из правоохранительных структур.

Финн Виктор Константинович – Главный научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук, доктор технических наук, профессор, Заслуженный деятель науки Российской Федерации

Список сокращений

- АДИС (AFIS) – автоматизированная дактилоскопическая идентификационная система
- АЗН-В (ADS-B) – автоматическое зависимое наблюдение-вещание
- АИПС – автоматизированная информационно-поисковая система
- АИС – автоматизированная информационная система
- АИУС – автоматизированная информационно-управляющая система
- АПК – аппаратно-программный комплекс
- АПКБИ – аппаратно-программный комплекс биометрической идентификации
- АСУ – автоматизированная система управления
- БАС – беспилотные авиационные средства (системы)
- БВС – беспилотные воздушные средства (суда)
- БД – большие данные, технология Big Data
- БдУ – банк данных угроз ФСТЭК России
- БЗ – база знаний
- БМУ – базовая модель угроз
- БПЛА – беспилотный летательный аппарат
- БВС – беспилотное воздушное судно
- БФ – база фактов
- ВП – воздушное пространство
- ГИАЦ – Главный информационно-аналитический центр МВД России
- ГИС – Государственная информационная система
- ГЛОНАСС – Глобальная навигационная спутниковая система, Россия
- ГНСС – Глобальная навигационная спутниковая система
- ГОСТ – государственный стандарт
- ДПАС – дистанционно пилотируемая авиационная система
- ЕБС – Единая биометрическая система
- ЕС ГРЛО – Единая система государственного радиолокационно-го опознавания
- ЕСИА – Единая система идентификации и аутентификации
- ЗИ – защита информации
- ИИ – искусственный интеллект
- ИКАО (International Civil Aviation Organization, ICAO) – международная организация гражданской авиации
- ИКТ – информационно-коммуникационная технология
- ИППП – интеллектуальный пакет прикладных программ
- ИС – интеллектуальная система
- ИСВС – интегрированная сетевая вычислительная среда
- ИСОД – информационно-аналитическая система обеспечения деятельности МВД России

ИТВ – информационно-техническое взаимодействие
 ИТС – интеллектуальная транспортная система
 КАТ – квазиаксиоматическая теория
 КВО – критически важный объект
 КИИ – критическая информационная инфраструктура
 КНР – Китайская Народная Республика
 КМПО – концептуальная модель предметной области
 КСЗИ – комплекс средств защиты информации
 ЛВС – локальная вычислительная сеть
 ЛПД – линии передачи данных
 МВД России – Министерство внутренних дел Российской Федерации
 МИВП – система мониторинга использования воздушного пространства
 МПСН – многопозиционная система наблюдения
 МФЦ – многофункциональный центр
 НИР – научно-исследовательская работа
 НПП – научно-производственное предприятие
 НПУ – наземный пункт управления
 НС БИЛ – национальная система биометрической идентификации личности
 ОВД – органы внутренних дел
 ООО – общество с ограниченной ответственностью
 ОПО – общее программное обеспечение
 ОрВД – организация воздушного движения
 ОРД – оперативно-розыскная деятельность
 ОРИ – организатор распространения информации
 ОРМ – оперативно-розыскное мероприятие
 ОС – операционная система
 ОСПО – общесистемное программное обеспечение
 ПАО – публичное акционерное общество
 ПВП/VFR – правила визуальных полетов
 ПИ – программное изделие
 ПИД-регуляторы – пропорционально-интегрально-дифференциальный регулятор
 ПИН-код (Personal Identification Number) – персональный идентификационный номер
 ПК – персональный компьютер
 ПО – программное обеспечение
 ППП/IFR – правила полетов по приборам
 ПС CEYC – Поисковая система «CEYC»
 ПЦП/DFR – правила цифровых полетов
 РТ – робототехника
 РЭБ – радиоэлектронная борьба
 СВО – специальная военная операция

СВТ – средство вычислительной техники
 СЗИ – система защиты информации
 СИИ – система искусственного интеллекта
 СИК – средство информационных коммуникаций
 СКУД – системы контроля и управления доступом
 СМИ – средство массовой информации
 СПД – сеть передачи данных
 СПО – специализированное программное обеспечение
 СС – социальная сеть
 СУБД – система управления базами данных
 СЦУО – система централизованного учета оружия
 ТК – технический комитет
 ТЭК России – топливно-энергетический комплекс
 УА – уровень автономности
 УК РФ – Уголовный кодекс Российской Федерации
 УМВД России – Управление Министерства внутренних дел Российской Федерации
 ФИС БУ – Федеральная информационная система биометрических учетов
 ФСР КВП – Федеральная служба разведки и контроля воздушного пространства
 ФСТЭК России – Федеральная служба технического и экспортного контроля Российской Федерации
 ЦБ России – Центральный банк Российской Федерации
 ЦБТ – центр биометрических технологий
 ЦИАДИС МВД России – Централизованная интегрированная автоматизированная дактилоскопическая информационная система Министерства внутренних дел Российской Федерации
 ЦНИИ – Центральный научно-исследовательский институт
 ЦП ИОП – цифровая платформа информационного обслуживания полетов
 ЭКП – экспертно-криминалистическое подразделение
 ЭКЦ – экспертно-криминалистический центр
 ЭС – экспертная система
 AID – Author ID – идентификатор автора
 AMBIS – автоматизированные многопрофильные системы биометрической идентификации
 API (Application Programming Interface) – протокол информационного взаимодействия
 ATN (Aeronautical Telecommunication Network) – сеть авиационной электросвязи
 CNN (Convolutional Neural Networks) – сверточная нейронная сеть
 CNS/ATM (Communication, Navigation, Surveillance/Air Traffic Management) – концепция ИКАО о связи, навигации, наблюдении и организации воздушного движения

CRUSH (Crime Reduction Utilizing Statistical History) – система сокращения преступности на основе использования статистических данных

DAS (Domain Awareness System) – интеллектуальная система предупреждения преступлений

GAN (Generative Adversarial Networks) – метод подмены координат и генерации ложных маршрутов

GPS (Global Positioning System) – система глобального позиционирования

GSM (Global System Mobile) – глобальный стандарт цифровой мобильной связи

IoT – Интернет вещей

IPS (Intrusion Prevention System) – пакет протоколов Интернет (предотвращение вторжений)

ISO (International Organization for Standardization) – международная организация по стандартизации

IT (Information Technology) – информационные технологии

ITU (International Telecommunication Union) – Международный телекоммуникационный союз

MBU – модульная переносная биометрическая система

RCP (Required Communication Performance) – минимальный стандарт связи

RICAS (Real-Time Intelligence Crime Analytics System) – система профилактики и расследования преступлений в режиме реального времени

RSP (Required Surveillance Performance) – минимальный стандарт производительности

SES (Single European Sky) – Единое европейское небо

SWIM (System Wide Information Management) – концепция общесистемного управления информацией

USB (Universal Serial Bus) – универсальная последовательная шина

UTM (Unmanned Traffic Management) – управление беспилотным движением

Словарь терминов

Авторизация – процесс, заключающийся в присвоении учетной записи, к которой получен доступ после аутентификации.

APT-атака (Advanced Persistent Threat) – это целевая продолжительная атака повышенной сложности, задача которой является обнаружение на устройстве пользователя секретной, конфиденциальной или любой ценной информации и использование ее в интересах киберпреступников.

Аутентификация – на основе установленной легитимности идентификатора, ранее предъявленного индивидом, процедура проверки принадлежности субъекту определенных прав и параметров доступа к защищаемой информации.

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность информации – состояние ее, информационных ресурсов и систем, при котором с требуемой вероятностью обеспечиваются обозначенные параметры защиты информации (данных) от случайного или преднамеренного доступа лиц, не имеющих на это право.

Безопасность информационной сети – меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов. Включает защиту оборудования, программного обеспечения, данных.

Безопасность КИИ – состояние ее защищенности, обеспечивающее устойчивое функционирование в условиях деструктивных информационных воздействий любой интенсивности.

Беспилотная авиационная система – комплекс взаимосвязанных элементов, включающий в себя одно или несколько беспилотных воздушных судов, средства управления полетом одного или нескольких беспилотных воздушных судов и контроля за полетом одного или нескольких беспилотных воздушных судов (станцию внешнего пилота и линию управления беспилотными авиационными системами и контроля беспилотной авиационной системы), а также средства осуществления взлета и посадки беспилотных воздушных судов.

Беспилотное воздушное судно – воздушное судно, управляемое, контролируемое в полете пилотом, находящимся вне борта такого воздушного судна (внешний пилот). Эти устройства могут быть как полностью автономными, так и управляться оператором на земле с помощью радиосигнала или других средств связи.

Биометрия (биометрическое распознавание) – система автоматической идентификации или распознавания человеческой личности, основанная на аналитической оценке специализированными методами и технологиями его физиологических, биологических, биохимических характеристик или поведенческих факторов, а также на комплексе этих характеристик.

Большие данные (Big Data) – огромные объемы структурированной и неструктурированной информации, которые могут быть эффективно обработаны с применением масштабируемых программных инструментов.

Верификация – проверка соответствия индивида тому, за кого он себя выдает (программно-аппаратное «удостоверение личности», относящееся к логическому сравнению «один-к-одному»).

Гиромат – элементарная модель целесообразного поведения. По своему функционалу эта модель способна адаптироваться к условиям решаемой задачи. В модели содержались «агент-образующие» модули: блок мотивации; блок селекции (рецепторы); блок построения внешней среды; блок выдвижения гипотез; блок модельного опыта; блок выработки решений; блок активного опыта; блок времени.

Дипфейк – высококачественная подделка изображения, голоса и видео.

ДСМ-метод – название метода автоматического порождения гипотез в честь английского естествоиспытателя Джона Стюарта Милля (философ, логик, экономист)

Защита информации – комплекс мероприятий, организуемых и проводимых в целях предотвращения ее хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т. д.

Защита информации в автоматизированных системах обработки информации (АСОД) – использование средств и методов, принятие мер и осуществление их в целях обеспечения требуемой защищенности информации.

Защищаемая информация – сведения (данные), которым постоянно или на определенное время присвоен один или несколько атрибутов статуса защищенности.

Защищенность информации – такое состояние, когда на заданном уровне в АСОД поддерживаются ее требуемые характеристики, определяющие установленный статус хранения, обработки и использования.

Идентификация – обеспечение регламентированного правовыми нормами установления сведений о лице и их проверка на основе последующего сопоставления данных сведений со значением идентификатора.

Интеллектуальная система – компьютерная система с реализацией способности естественного интеллекта.

Интеллектуальные системы принятия решений в реальном времени используют анализ больших данных для обоснования допустимых и эффективных решений. Подобные системы могут обеспечивать выявление лучших трендов, способны составлять наилучшие прогнозы событий, оптимизировать процессы в целях повышения производственной и социальной эффективности, снижения затрат.

Поэтому они распространяются и становятся все более полезными в бизнесе, финансах, медицине, где скорость принятия решений играет ключевую роль.

Информационная безопасность (в узком смысле) – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Информационная безопасность (в широком смысле) – способность государства, общества, личности обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы, информационные потоки для поддержания своей жизнедеятельности, жизнеспособности, устойчивого функционирования и развития. Созданная системная способность должна эффективно противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное, общественное сознание и психику людей, а также на компьютерные сети и другие технические и технологические источники информации; поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно не было навязано и в каких бы то не было формах.

Информационная инфраструктура – система организационных структур, подсистем, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия. Включает совокупность информационных центров, подсистем, банков данных и знаний, систем связи, центров управления, аппаратно-программных средств и технологий обеспечения сбора, хранения, обработки и передачи информации.

Искусственный интеллект – это одно из направлений информатики, целью которого является разработка аппаратно-программных средств, позволяющих пользователю-непрограммисту ставить и решать свои, традиционно считающиеся интеллектуальными, задачи, общаясь с компьютером на ограниченном подмножестве естественного языка.

Киберпреступление – любая противоправная деятельность в киберпространстве либо совершенная с использованием информационных технологий.

При этом общая дифференциация понятий «киберпреступление», «преступление, совершенное с использованием ИКТ» выглядит следующим образом.

Киберпреступление совершается в виртуальном пространстве (киберпространстве) на базе применения информационных технологий и Интернета. Так, к ним относят: распространение вредоносного программного обеспечения, хакерские атаки, фишинг/*spear phishing*, сетевые варианты мошенничества и т. д. Более широким по спектру противоправных деяний представляется другое понятие.

Преступление, совершенное с использованием ИКТ, охватывает кроме киберпреступлений и другие их виды, базирующиеся именно на данных технологиях, но реализуемые не обязательно в виртуальном пространстве. Например, преступное обращение к ИКТ при подготовке, совершении, изменении следов в традиционных грабежах, убийствах и т. д.

Киберпространство – абстракция метафорического уровня, применяемая в современной философии и компьютерных технологиях. Фактически обозначает виртуальную реальность или второй мир: «внутри» компьютеров и компьютерных сетей.

Киберустойчивость – это способность компьютерной системы сохранять во времени в установленных пределах значения всех параметров, характеризующих ее способность выполнять свои функции в условиях компьютерных атак, не допускать несанкционированного доступа к вычислительным ресурсам, нарушения целостности информации и нарушения доступности информационных сервисов.

Компьютерная атака – целенаправленная угроза или фактическое воздействие программного или аппаратного обеспечения на телекоммуникационную сеть с нарушением или прекращением ее функционирования.

Компьютерная безопасность (в узком смысле) – свойство компьютерной информации, при котором с требуемой вероятностью обеспечивается ее защита от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации, копирования, блокирования и т. д.

Компьютерная безопасность (в широком смысле) – свойство компьютерной информации (данных), ЭВМ, системы ЭВМ, сети ЭВМ, при котором с требуемой вероятностью обеспечивается ее защита от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации, копирования, блокирования. Она также предусматривает защиту ЭВМ, системы ЭВМ, сети ЭВМ от неправомерного доступа, создания, использования и распространения вредоносных программ, нарушения правил эксплуатации, несанкционированной модификации программ, разрушающих воздействий информации и т. д.

Компьютерное зрение – направление искусственного интеллекта, предназначенное для анализа изображений и видео, включая распознавание объектов, лиц и сцен.

Компьютерные преступления – любое деяние, влекущее незаконное вмешательство в имущественные права, возникающие в связи с использованием ЭВМ.

Криптоанализ (от греч. *kryptos* – тайный, скрытый; *analysis* – разложение) – наука о методах раскрытия и модификации данных. Она развивается по двум направлениям.

Криптография объединяет понятия *крипто* и *графо* (от греч. *kryptos* – тайный, скрытый; *grafo* – пишу). В целом – это отдельная наука, применяющая математические методы, достижения науки и техники для преобразования открытой защищаемой информации в закрытую, значительно затрудняющую смысловое понимание или восстановление исходного открытого текста.

Критические информационные инфраструктуры – совокупность автоматизированных систем управления и информационно-телекоммуникационных сетей обеспечения их взаимодействия, предназначенных для решения задач управления организационно-техническими системами.

Машинное обучение – в подготовке приложений искусственного интеллекта использует подход для формирования аналитических алгоритмов обучающих моделей на основе обращения к большим данным для выявления закономерностей и принятия решений. Включает методы глубокого обучения, многомерного нелинейного регрессионного анализа, классификации и кластеризации.

Нейронные сети – компьютерные программы, работающие по принципу деятельности нейронов головного мозга (имитация функционирования нейронов по получению, обработке, передаче информации).

Обработка естественного языка – как направление методов подготовки приложений искусственного интеллекта занимается пониманием и генерацией человеческой речи. Включает технологии перевода, чат-ботов и голосовых ассистентов.

Объекты защиты БТС:

- информация, содержащаяся в различных базах данных БТС;
- данные информационного и командно-сигнального трактов взаимодействия;
- аппаратные технические средства;
- средства и системы связи и передачи данных;
- технические средства обработки информации;
- программные средства и обеспечение;
- информационные технологии;
- средства защиты информации.

Основные виды киберпреступлений:

- мошенничество с использованием электронной почты и Интернета;
- кражу «цифровой личности» (хищение и использование личных данных);
- кражу данных, зафиксированных на платежных картах, а также другой финансовой информации;
- хищение и перепродажу корпоративных данных;
- кибершантаж (вымогательство денег под угрозой атаки); атаку с использованием программ-вымогателей;

- криптоджекинг (майнинг криптовалют с использованием чужих ресурсов);
- кибершпионаж (получение несанкционированного доступа к государственным или корпоративным данным);
- нарушение работы систем в целях компрометации сети;
- нарушение авторских прав;
- онлайн-торговлю запрещенными товарами;
- домогательства;
- изготовление или хранение детской порнографии.

Перспективные методы искусственного интеллекта – методы, направленные на создание принципиально новой научно-технической продукции, в том числе в целях разработки универсального (сильного) ИИ (автономное решение различных задач, автоматический дизайн физических объектов, автоматическое машинное обучение, алгоритмы решения задач на основе данных с частичной разметкой и (или) незначительных объемов данных, обработка информации на основе новых типов вычислительных систем, интерпретируемая обработка данных и другие методы).

Робототехника – среди направлений и методов искусственного интеллекта ориентировано на целевое использование по управлению роботизированными системами – промышленными роботами, беспилотными транспортными средствами и т. д.

Сверхинтеллект или супер (Super AI) – теоретическая форма ИИ, превосходящая человеческий интеллект по всем параметрам.

Сильный или генеративный ИИ (общий или обобщенный – General AI) – способен обеспечивать решение широкого спектра задач, аналогичных естественному человеческому интеллекту. В ней должно быть реализовано понимание, рассуждение, планирование и решение проблем в различных контекстах, формировать суждения в условиях неопределенности, умение учиться, интегрировать предыдущие знания в процесс принятия решений, предлагать новаторские идеи. Данный уровень пока находится на стадии исследований и отдельных успешных разработок, направленных на наделение машин сознанием.

Система защиты информации – организованная совокупность методов, средств и мероприятий, создаваемая в системе обработки данных для защиты информации.

Система искусственного интеллекта – это компьютерная модель интеллектуальных возможностей человека в целенаправленном поиске, анализе и синтезе текущей информации об окружающей действительности для получения о ней новых знаний и решения на этой основе различных жизненно важных задач.

Слабый ИИ (узкий – Narrow AI) – предназначен технологически для решения конкретных, разработанных, predetermined задач: распознавание лиц, прогнозирование погоды или перевод текста. Эти

системы ограничены, как правило, одной областью применения и не обладают общим интеллектом.

Спуфинг – атака в момент верификации, когда один человек выдает себя за другого индивида с использованием поддельных идентификационных данных.

Статус защищенности информации – состояние информации, определяемое необходимостью:

- обеспечения физической целостности;
- обеспечения логической целостности;
- предупреждения несанкционированной модификации;
- предупреждения несанкционированного получения;
- предупреждения несанкционированного размножения.

Технологии искусственного интеллекта – технологии, основанные на использовании искусственного интеллекта, включая компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угроза информации (дестабилизирующий фактор) – явление, событие, случай, которое может произойти в интересующем или заданном интервале времени, а результате этого возможно существенное (имеющее значение) нежелательное воздействие на защищаемую информацию по одному или нескольким аспектам статуса защищенности.

Угрозы кибербезопасности – совокупность условий и факторов, создающих потенциальную опасность потери управления БТС, штатного функционирования или получения несанкционированного доступа к нему из-за целенаправленных вредоносных программно-аппаратных воздействий на СУ беспилотного транспорта.

Уязвимость информации – ее свойство при нахождении в процессе обработки подвергаться воздействию внутренних или внешних угроз с точки зрения одного или нескольких атрибутов статуса защищенности.

Хэш-функция – функция, осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку фиксированной длины.

Цель информационной атаки на БТС определяется намерениями нарушителя, которым может быть иностранное государство, организация, физическое лицо.

Цифровая платформа контроля и управления движением БТС со встроенными средствами защиты информации – является ядром системы безопасного управления беспилотным транспортом – АСКУД БТС.

Основные установки выполнения данного проекта в целом направлены на обеспечение:

- полного контроля трафика БТС в границах зон социальных объектов, защищаемых объектов критической инфраструктуры;
- киберустойчивости БТС и защиты от их неправомерного применения;
- контроля выполнения маршрутных (полетных) заданий;
- выявления и предотвращения аномалий в поведении БТС;
- соответствия БТС законодательству РФ и требованиям регуляторов по безопасности их применения.

Цифровая платформа информационного обслуживания полетов (ЦП ИОП) – комплекс взаимосвязанных цифровых информационных сервисов, который предоставляет информацию на основе аэронавигационных, геопространственных, метеорологических и других данных и использует инфраструктуру связи, навигации, наблюдения, управления радиочастотным спектром для измерения параметров движения БАС и обеспечения его безопасности.

Электронная подпись – реквизит электронного документа, позволяющий подтвердить его валидность и отсутствие в нем искажения информации, принадлежность подписи владельцу.

Юнит искусственного интеллекта – отдельно взятая технологическая единица в виде компьютерной программы, робота, системы.

Введение

В своем историческом развитии у человека главной мечтой было стремление обеспечить опережающий прогресс в области решения творческих задач. Эту идею на фоне научно-технических достижений XX в., преимущественно в области моделирования, программирования и компьютерной техники, стали в конечном итоге называть *искусственный интеллект (ИИ)*.

Создание и активное внедрение отмеченной революционной технологии, несмотря на всю ее фантастическую оригинальность и уникальность применения в самых различных сферах человеческой деятельности, тем не менее ожидают классические формы становления и развития.

Первая из них, согласно устоявшимся канонам, связана с прогрессивной стороной общественных устремлений к совершенствованию, созданию новых достижений в интеллектуальной сфере. Это дает, по сути, безграничные возможности в реализации типовых и универсальных творческих задач.

Вторая же, также уже обладающая классическим характером, к сожалению, отражает негативные стороны сопровождающих явлений, создает определенные отрицательные антисоциальные последствия. Они разнообразны по своей сущности и содержанию, обладают характером широкого распространения. Но нас в рамках настоящей монографии интересуют возможности использования достижений технологий ИИ в осуществления преступной деятельности.

Актуальность этого связана с кумулятивным ростом подобных преступлений. Мировая динамика говорит, например о том, что начиная с 2018 г. ежегодные потери от кибератак составили от \$0,86 трлн до прогнозируемых в 2027 г. \$23,82 трлн [89]. Данные ГИАЦ МВД России по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий (официально собираемые с 2020 г.), указывают на их общее увеличение по стране с 511 300 (2021 г.) до 765 365 (2024 г.) – прирост почти на 50 %. Материальный ущерб граждан оценивается от 70,8 млрд руб. (2021 г.) до 203, 6 млрд руб. (2024 г.) – прирост почти на 288 % [47–50].

Поэтому в работе, в первую очередь, речь идет о киберпреступлениях. В настоящее время они бурно развиваются, создавая фактически новый уровень антиобщественной опасности. Их текущее состояние и перспективы эволюции определяют необходимость опережающего реагирования правоохранительных структур, в частности, органов внутренних дел (ОВД).

В монографии рассмотрены многие тренды применения ИИ в криминальных целях, хотя бы взять активно развивающуюся тенденцию внедрения беспилотных транспортных средств (БТС), в частности, воздушного базирования. Следует отметить, что многие веду-

щие специалисты в сфере ИИ сосредоточены на выработке мер противодействия преступному использованию БТС на базе организации интеллектуальной поддержки их безопасного управления.

В работе акцентировано внимание на потенциальных направлениях применения БТС в организации эффективной борьбы ОВД с развивающимися видами киберпреступности, в частности, внимание уделяется новым угрозам кибербезопасности, базирующимся на организации кибератак с помощью беспилотного воздушного флота.

Рассмотренные в монографии особенности развития ИИ объективно приводит к необходимости исследования этой проблематики и выработки современных приложений и рекомендаций научными, научно-производственными и образовательными организациями системы МВД России по противодействию отрицательным факторам ИИ, а также поддержке его позитивных возможностей. Такие организации к настоящему времени имеют достаточный потенциал для создания адекватного уровня защиты от новых угроз. А в сочетании с творческим объединением с гражданскими научными центрами и правоохранительными структурами, уже получившими опыт противодействия киберпреступности, способны реализовать новейшие целевые установки, данные Президентом страны и Министром внутренних дел Российской Федерации на последних коллегиях МВД России в области борьбы с «электронными» криминальными явлениями.

Приведенная аргументация отражает *целевую направленность* монографии, предполагающей:

- систематизацию теоретических, практических достижений, инновационных подходов и путей в области развития технологий ИИ, применительно к совершенствованию методов, способов, тактики противодействия, эффективного раскрытия, расследования и профилактики киберпреступлений;
- формирование научно-практических рекомендаций по интеллектуальной поддержке решения оперативно-служебных задач противодействия киберпреступности, связанных с эксплуатацией различных типов беспилотного транспорта.

Отразим структурное содержание монографии, представленное двумя частями.

Первая часть включает две главы, отражающие систематизированные сведения о предметной области ИИ и его использовании правоохранительными органами в борьбе с киберпреступностью.

Первая глава содержит систематизированные сведения об истории развития и современное понимание теоретического аппарата и практических приложений в сфере ИИ. Изложены основные трактовки киберпреступности, ее современное состояние и эволюция в перспективе. Обобщением являются авторские положения монографии о проблемах и новых возможностях ИИ в сфере противодействия киберпреступлениям.

Во *второй главе* изложены наиболее значимые, в том числе – авторские пути разработок и решений типовых оперативно-тактических задач ОВД по борьбе с киберпреступностью на основе использования технологий ИИ.

Во второй части работы рассмотрены основные направления программно-математического и организационного обеспечения новой сферы кибербезопасности – защищенного управления беспилотным транспортом.

В ее составе *третья глава* описывает авторский подход к созданию системы моделей и технологий безопасного управления беспилотным транспортом. В нем отражены основные элементы разработок: моделирование киберугроз системам ИИ; моделирование киберустойчивости и управляемости БТС; основы классификации моделей безопасного управления беспилотным транспортом; комплексная математическая модель системы интеллектуальной защиты информации флота беспилотных авиационных средств (систем) (БАС); основы построения цифровой платформы БТС.

В *четвертой главе* нашли отражение авторские решения ряда прикладных задач управления беспилотным транспортом на основе ИИ. Это – обеспечение кибербезопасности БАС дистанционного мониторинга лесных территорий; решения в экспертно-криминалистической сфере; интеграция с геоинформационными системами для интеллектуально-аналитического обеспечения раскрытия и расследования преступлений; автоматическое распознавание и маршрутизация БАС, обеспечение безопасности их управления.

Содержание *пятой главы* начинается с краткого рассмотрения нормативно-правового регулирования вопросов беспилотного воздушного движения на международном (международной организации гражданской авиации – ИКАО) и отечественном уровне. Здесь отмечены решения в области перспективных технологий связи, навигации, наблюдения/организации воздушного движения. В рамках страны обращено внимание на план мероприятий Концепции интеграции БТС в единое воздушное пространство Российской Федерации,

На основе нормативных положений приведены перспективные направления, мировые тенденции и примеры внедрения ИИ в авиатранспортную систему. Среди ее элементов в работе затронуты: система организации воздушного движения; аэропортовые службы; авионика, цифровая защищенная платформа управления.

ЧАСТЬ I. ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ

Глава 1. Общие положения

1.1. Понятийный аппарат в сфере искусственного интеллекта

В разделе решается задача – рассмотреть научно-практический материал по текущему состоянию ИИ. Прежде всего, дадим характеристику историческим условиям и истокам теоретического осмысления, особенностям понятийного аппарата и практической реализации ИИ. В этом отношении весьма своевременное понимание Святейшего Патриарха Кирилла [153] на пленарном заседании XXXIII Международных Рождественских образовательных чтений 28 января 2025 г.

В своем выступлении он выразил философскую и духовную истину, говоря о невозможности «...с нуля начинать историческое развитие», забывая о том, что духовная сила, культура не перестает питать сознание и нравственное чувство людей. В конечном итоге, именно внутренняя, творческая, духовная сила предыдущих поколений дает возможности человеку раскрывать потенциал сознания, облекать его образы в практические воплощения.

Сказанное в полной мере относится и к ИИ. Именно в нем отражены основы идейного зарождения и реального становления этой новейшей технологии.

Диалектическое развитие мира отражает то, что процессы прогресса и регресса существуют совместно и взаимообусловлено. Поэтому, наряду с вектором прогрессивного созидания и внедрения ИИ, следует обращать особое внимание и на негативную сторону этого явления.

В частности, уже 30 января на открытии XIII Рождественских Парламентских встреч, организованных в Государственной Думе Федерального Собрания РФ в рамках XXXIII Международных Рождественских образовательных чтений «80-летие Великой Победы: память и духовный опыт поколений» Святейший Патриарх Кирилл подчеркнул необходимость развития ИИ в сочетании с разумным учетом угроз от широкого внедрения данной технологии в жизнь российского и мирового общества [152].

Высказанные им мысли отражают современные научно-практические представления о потенциальных последствиях развития и внедрения ИИ во многие сферы общественного бытия, в том числе – негативных. Суть его предостережений, которые в обязательном порядке должны быть учтены при массовом использовании ИИ:

– тесная и однозначная связь ИИ с человеческим разумом позволяет говорить об этой технологии, как об *одном из важных вызовов нашего времени*, все больше определяющем человеческое культурное пространство;

– постоянное развитие интеллектуальных программ по использованию творческого, культурного опыта, наследия людей, их концептуальных и гипотетических устремлений, создает для общества очень профессионального помощника, доступного в реальном времени. Вместе с тем, это развитие *негативно влияет на психологический и рациональный потенциал человека*.

Говоря проще, ИИ порождает такие отрицательные явления, как: профессиональную и бытовую лень, переключение мозговых ресурсов на простые задачи; утрату стремления к соревновательной, карьерной деятельности, умения целенаправленно формировать и преодолевать интеллектуальные трудности; часто невозвратное снижение мотивации к самообразованию, приобретению и тренировке новых навыков, развитию стремлений к генерации идей, поиску путей их решения. Эта сторона угроз выражена у Патриарха фразой: «реальная опасность утраты интеллектуальных и творческих навыков человека» [152];

– ИИ с его возможностями, пока с не вполне осознаваемыми человечеством, по сути своей, должен быть поставлен ему на службу, но под жестким контролем государства и общества. Цель контроля – *не упустить очередную потенциальную опасность, способную разрушить человеческую жизнь и человеческую цивилизацию*. Патриарх приводит образное сравнение, обращаясь к Священному Писанию: «... в конце человеческой истории придет антихрист, то есть личность, которая будет противостоять Христу, противостоять всему тому, что принес Бог в жизнь человечества.

Всеобщая глобальная власть антихриста будет преследовать достижение самых опасных целей, которые приведут к концу человеческой цивилизации. И мы должны помнить, что ведь антихрист не с неба явится и не из преисподней выйдет.

Он не сможет явиться в окружении, которое будет его отторгать или противостоять ему. Он может прийти и обрести силу только в обществе, которое будет его поддерживать. И еще неизвестно, какой может быть роль искусственного интеллекта в приближении этой апокалиптической картины» [152].

К этому можно добавить и еще один тезис Патриарха: «Искусственный интеллект – это опаснее, чем ядерная энергия, особенно, если искусственный интеллект будет запрограммирован на несение сознательного вреда человеческой нравственности, человеческому обществу и другим ценностям, без которых человек потеряет способность оставаться человеком» [152].

Другие опасения Патриарха относятся к следующим негативным проявлениям ИИ, которые требуют от государства и общества:

- организации грамотного и тщательно продуманного использования ИИ в отношении *воздействия на личность человека*, а, значит, и на судьбу каждого индивида и коллективов людей. В частности, это связано с сегодняшним, все более серьезным обсуждением возможностей цифровизации судебных решений, где бездушный алгоритм предполагается стать имитатором справедливого человеческого суда, который по природе своей должен учитывать множество тончайших нюансов, руководствоваться далеко не всегда формализуемыми социальными, нравственными, духовными, чувственными императивами;

- необходимости эффективного противостояния технологиям «дипфейков», активно развиваемым противоправной средой и реализуемым на базе ИИ. Эти технологии быстро охватывает большие территории и массы людей, в том числе создавая высококачественные подделки их биометрических характеристик [84].

Уже сегодня наиболее опасные подделки в виде изображений, голоса, видеоконтента причиняют огромный экономический ущерб обществу и отдельным индивидам, способны существенно затруднять расследование преступлений, составляют реальную угрозу национальной безопасности, все более активно используются киберпреступниками, нанося серьезные репутационные потери людям и коллективам;

- выработки и внедрения законодательных, организационных, технологических и иных мер, направленных на противодействие политическим манипуляциям, несущим российскому обществу чуждые ценностные парадигмы и ориентиры.

Отмеченные позитивные и негативные грани ИИ подробно оценены в монографии. Дело в том, что многие мыслители, как материалисты, так и идеалисты справедливо считали, что самым совершенным творением материального мира является *Разум* человека. В их числе В. И. Вернадский, Н. Ф. Федоров, К. Э. Циолковский, а также много других известных ученых.

Для реализации такой цели переплелись и достигли огромного синергетического эффекта кибернетика, информатика, нейрофизиология, управление, математика, компьютерная техника, философия, социология и многие другие науки, расширяющие свои возможности путем подключения все более новых идей и концепций.

Первопроходцами в создании первых «мыслящих» машин были представители философско-кибернетического направления науки, связанного, прежде всего, с деятельностью Алана Тьюринга и Джона фон Неймана, разработавшие и создававшие как первые ЭВМ, так и открывшие новые горизонты науки и практики на пути постижения возможности выполнения функций человеческого разума [406–407].

Отмеченная изыскательская деятельность связана с трудами Норберта Винера, Уильяма Эшби и многих других. К плеяде пионеров в этой сфере относятся и советские исследователи в области кибернетики и вычислительной техники – А. А. Ляпунов, А. И. Берг, А. Н. Колмогоров, А. А. Марков. Но они же положили начало не только достижениям, но и проблемам в сфере ИИ.

В итоге разработаны многие компоненты грандиозного проекта построения интеллектуальных систем. Так, по мнению Д. А. Поспелова – одного из родоначальников отечественного ИИ – указанную технологию следует рассматривать как междисциплинарное исследование или синтетическую «науку-перекресток» (рис. 1.1). Как видно из рисунка воплощение основной идеи потребовало объединения многих научных дисциплин [388].



Рис. 1.1. Основные составляющие «науки-перекрестка» как источника ИИ [388]

Наряду с этим достигнуты результаты, которые первоначально не предполагались в решаемой задаче создания и реализации ИИ. Они отличаются определенным научно-практическим уровнем, концепту-

альным и технологическим развитием, устойчиво войдя в различные сферы человеческой деятельности [444].

Отметим довольно значительный исторический пласт представлений человечества о возможностях создания *человеческого разумного аналога*, ориентируясь на разные письменные свидетельства, документальные сведения, легенды и т. д.

Приведем один из характерных литературных примеров. В нем, как и во многих других работах [300; 391; 420] отражен период понятийного становления ИИ.

Так, О. Г. Чанышев [444] переносит читателя в середину XIII столетия, делая зарисовки общения монаха Фомы Аквинского, его учителя Альберта фон Больштедта (за свою ученость прозванного Великим). Предметом их обсуждения является человекоподобная кукла женщины, которая умела ходить, двигать руками и говорить.

Там же представлены идеи францисканского монаха Раймонда Луллия (предположительно XIII в.) об «устройстве для автоматического открытия истин» (соответствует некоторым правилам из сферы «эвристики»). Отражена версия, что основные представления Луллия связаны с работами одного из выдающихся мыслителей мусульманского средневековья – Мухйи ад Дина Мухаммада ибн аль-Араби (1165–1240).

Несмотря на глубокие исторические корни ИИ, до сих пор остаются проблематичными определения исходных аксиоматических понятий, связанных с объяснением работы *человеческого мозга*. По крайней мере, на текущий момент нет многих общепринятых трактовок в этой сфере.

Например, речь идет о таких понятиях, как: «мысль», «мышление», «разум», «понимание», «смысл», «интеллект». В этом плане некоторыми аналогами иногда выступают понятия из области информатики – «оперативная память», «процессор ЭВМ» и др.

В своих рассуждениях на тему «Суперкомпьютер когда-нибудь превзойдет человека – это сказки» В. К. Финн – наш современник, руководитель Отделения интеллектуальных систем в гуманитарной сфере Российского государственного гуманитарного университета [424], в частности, отмечает следующее. Обсуждая частое применение терминов «искусственный интеллект», «интеллектуальные системы» без понимания реального их смысла, В. К. Финн предупреждает, что это может приводить к заблуждению общественности, даже поддерживать определенное невежество среди людей.

В частности, под ИИ нередко понимаются нейронные сети – компьютерные программы, работающие по принципу деятельности головного мозга, – имитация функционирования нейронов по получению, обработке, передаче информации. В. К. Финн подчеркивает в связи с этим, что нейронные сети являются лишь одним из методов современного ИИ. Он не может исчерпать все возможности ИИ, с по-

мощью которого можно воспроизводить гораздо более сложные виды человеческого познания и мышления.

Завершая краткий экскурс, отметим, что ситуация в сфере ИИ принципиально стала изменяться с середины 50-х гг. XX в. Появились многочисленные и многоплановые отечественные [52; 55; 57; 68; 88; 120–122; 131–132; 136–137; 139; 163; 186–187; 193; 197; 214; 221; 223; 225; 234; 237; 270; 274; 319–336; 339; 348; 372; 377; 385; 389–390; 405; 457] и зарубежные работы [59; 64; 103; 107; 112; 118; 155; 168; 228; 266–267; 279–280; 282–283; 365; 375; 408–409; 437–438; 446; 454–455; 458; 467–468; 472; 475; 478; 480; 488], в которых на более глубоком концептуальном уровне стали обсуждаться и устраняться имеющиеся разногласия в понятийной трактовке ИИ.

Во-первых, подчеркнем, что в предложенном в 1956 г. термине *Artificial Intelligence* слово *intelligence* изначально означает «умение рассуждать разумно», а вовсе не «интеллект». Но и к настоящему времени приходится признавать факт отсутствия единой мировой трактовки в области ИИ, о чем всегда упоминают исследователи и практики.

В тот временной период Джон фон Нейман, один из величайших ученых XX в., ставший в итоге одним из «отцов-основателей» компьютерной науки и современных информационных технологий, пророчески оценивал возможности создания ИИ. В своих работах [279–280] он утверждал, что между естественным и искусственным интеллектом существует минимальная разница. Суть его предположений была в следующем – «архитектура» и «строительные блоки» мозга и компьютера имеют различия, но существует принципиальная возможность ИИ имитировать работу человеческого мозга.

С середины 50-х гг. прошлого века на ЭВМ первого поколения стали выполняться программы по обработке *традиционных интеллектуальных задач*. Полученная практика и достижения первых исследований вокруг нового подхода легли в становление научного направления – ИИ, обеспечили гармоничное объединение усилий отдельных направлений специалистов. Синергетический эффект от указанной консолидации дал возможность создать первые модели и системы, которые позволили говорить о переходе к формированию ИИ как новой науки.

В числе первых областей исследования, повлекших зарождение ее базовых принципов, были:

– *машинный перевод*. Замысел сформировался в 1947 г., а в 1954 г. с помощью ЭВМ в США перевели первые 60 фраз (в СССР эти работы начались в 1955 г.). Задача оказалась непростой, были сменены несколько поколений *лингвистических моделей*, разработаны языки *представления знаний*, алгоритмы *анализа текстов* в виде ряда последовательных взаимосвязанных шагов. Эти достижения составили теоретические и практические основы создания современного ИИ;

– *автоматизированное реферирование и информационный поиск*, начавшиеся в США в 1957 г. Ряд концептуальных новинок был при этом использован для развития ИИ: *дескрипторы*; *система связей-отношений*, приведшая к понятию *тезауруса*, а затем – к идее *семантической сети*;

– *доказательство теорем*. Решения данного класса задач нашли свое воплощение в разработке *процедур вывода*. По мнению многих исследователей, работа над доказательством теорем, привела к идее эвристических правил для сокращения перебора вариантов. Впоследствии это привело к созданию *эвристического программирования*, которое внесло значительный вклад в работы по интеллектуальным системам;

– *распознавание образов*. Среди направлений в теории распознавания следует назвать *классифицирующую систему признаков в процессе обучения* по нахождению решающих правил;

– *игровые программы*. Появившись еще в конце 40-х гг. XX в. эти программы стали хорошим алгоритмическим полигоном по апробации различных эвристических приемов и методов *поиска решений в условиях огромного множества альтернатив*;

– *сочинение музыки и текстов*, а затем машинной графики. Вначале в США, а несколько позже в СССР в середине 50-х гг. сделаны первые попытки сочинения музыкальных произведений с помощью программ ЭВМ. Из этого направления отметим идею использования *случайного процесса, детерминированного системой ограничивающих модельных правил*, как пути для реальной имитации творческих процессов человека.

Приведенные сведения о решении нечисловых задач указывают на наличие определенного творческого задела к началу реализации непосредственно технологий ИИ. Важным историческим импульсом для этого считают проведение в 1956 г. конференции в Дартмуте (США), появление термина «искусственный интеллект» относят как раз к этому форуму. Одними из ее участников были ведущие ученые К. Шеннон, М. Минский и Дж. Маккарти. В итоге под руководством Дж. Маккарти стал реализовываться комплексный исследовательский проект по искусственному интеллекту.

Активная деятельность по этому направлению развернулась в СССР, США, Великобритании и других странах. Появилось множество программ для решения нечисловых задач, имитации отдельных творческих процессов. Быстрое накопление разнообразного материала потребовало обобщения и формализации.

Таковыми работами занялись Дж. Маккарти, М. Минский, Э. Фейгенбаум (США), Д. Мичи (Великобритания), А. А. Ляпунов и В. М. Глушков (СССР). Позднее к развитию концептуальных основ и методологии ИИ приступили Г. С. Поспелов, Н. М. Амосов, Д. А. Поспелов, А. С. Нариньяни, Э. В. Попов, А. А. Богданов, Н. О. Лосский,

П. С. Флоренский, П. К. Анохин, В. М. Бехтерев, Л. С. Выготский, А. Н. Леонтьев, Ю. М. Лотман, А. Н. Колмогоров, М. М. Бонгард, В. А. Лефевр, В. Л. Цетлин, В. Л. Стефанюк (СССР), Р. Шенк, Д. Бобров, П. Уинстон, Дж. Слейгл, Н. Нильсон, Э. Хант, Т. Виноград (США), Э. Сандовал (Швеция), М. Сомальвико (Италия) и многие другие.

В самом начале появились и первые методологические трудности. Так, выявилась необходимость новой парадигмы по поиску универсальной процедуры, позволяющей создать единообразное решение интеллектуальных задач.

Так, *лабиринтная модель решения задач*, описанная в общей форме еще в 1911 г. Э. Торндайком, оказалась в числе первых, оставившая значимый след в моделировании интеллектуальной деятельности. Она реализована в американском проекте «Универсальный решатель задач» (*General Problem Solver*) программистом А. Ньюэллом и психологом Г. Саймоном.

Далее было осуществлено обращение к *реляционной модели*. Она объединяла элементы исследуемой среды, выраженные отдельными отношениями и их системами.

Кроме лабиринтной и реляционной моделей решения задач человеком большое внимание уделялось *ассоциативной модели*, в которой обучение происходит в процессе формирования ассоциативных связей, носящих вероятностный характер.

В СССР в середине 60-х гг. создан комплекс методов решения задач с общим названием «*ситуационное управление*». В его основе лежит положение, что любая ситуация физического мира описывается через конечное число базовых отношений, которые порождают производные отношения.

Д. А. Поспелов и В. Н. Пушкин создали для описания таких ситуаций концептуальную программу – *Гиромат* [341], на десятилетие опередившую первую зарубежную работу К. Хьюитта [471] в области теории агентов. Тем самым осуществлен переход от первоначальных идей психоники к построению теории интеллектуальных (искусственных) агентов и многоагентных систем.

Гиромат (рис.1.2) является элементарной моделью целесообразного поведения.

По своему функционалу она способна адаптироваться к условиям решаемой задачи. В модели содержались «агент-образующие» модули: блок мотивации; блок селекции (рецепторы); блок построения внешней среды; блок выдвижения гипотез; блок модельного опыта; блок выработки решений; блок активного опыта; блок времени [338; 340]. Состоятельность модели подтверждена в процессе решения ряда конкретных задач оперативного управления сложными системами.

Следует отметить вклад Д. А. Поспелова и в разработку других идей ИИ, имеющих ключевое значение для мировой науки и практики. Среди них работы по психонике, созданию в стране научной школы

ситуационного управления и ИИ, особенностям системного подхода в этой сфере, прикладной семиотике, нечетким множествам и их приложениям, мягким вычислениям. Его концепция психоники и прикладной семиотики активно развивается в области искусственного общего интеллекта (*Artificial General Intelligence*) и синергетического ИИ [389].

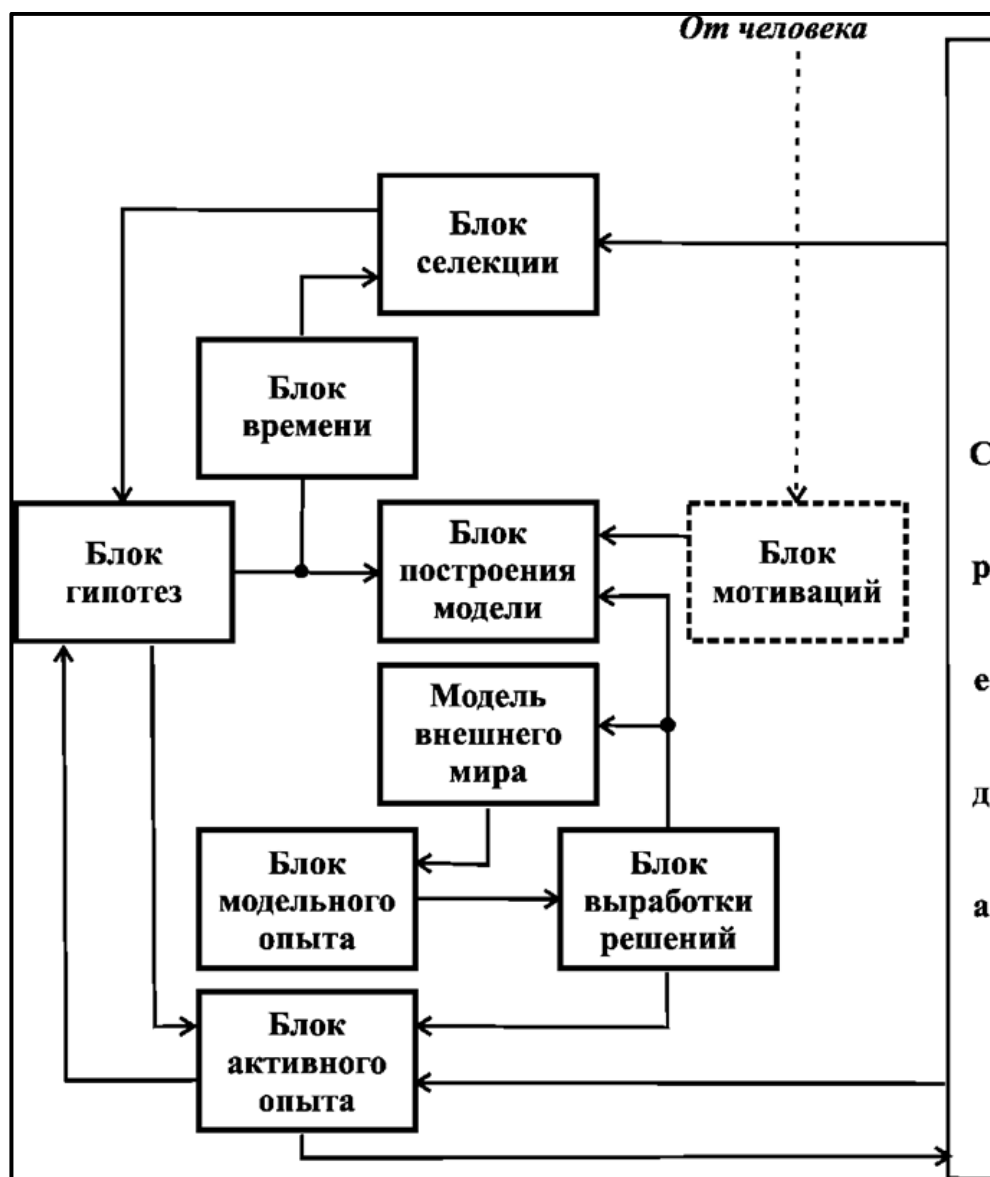


Рис.1.2. Блок-схема гиromата [341]

В теории ситуационного управления базовыми выступают представление знаний и манипулирование ими, которые остаются центральными и в работах по ИИ.

Подводя итог развитию работ по ИИ до начала 70-х гг., можно указать на две тенденции в подходах к созданию его моделей.

Одна условно может быть названа *информационной* и связана с разработкой программ для ЭВМ, имитирующих творческую деятельность человека. Данные программы подвергались серьезной кри-

тике, поскольку в описываемые ими процессы не включались нейрофизиологические механизмы.

Нейробионическая тенденция связана с воссозданием на моделях некоего нейрофизиологического субстрата, использующего известные еще с 50-х гг. модели *нейронов* и *рефлекторных механизмов* простейшего типа.

Реакции поведения более сложного уровня моделировались путем объединения этих механизмов. Так, под руководством Н. М. Амосова группой ученых создан автомат [52] для передвижения по незнакомой местности, запоминания ее, реагирования на другие движения, оценивания опасности происходящего.

Важным результатом отмеченных работ по исследованию процессов мышления в 70-е гг. является обращение специалистов к проблеме асимметрии мозга. В совокупности это позволило создать новую модельную составляющую ИИ – *«перцептрон»*. В концептуально-технологическом отношении он важен тем, что содержал в своей структуре элементы, которые имитировали человеческие нейроны.

Многие отмеченные особенности привели к осознанию необходимости создания *теории искусственного интеллекта*, которая строилась бы не на повышении эффективности конкретных программ, относимых к ИИ, а на выявлении общих принципов их разработки.

После систематизации и необходимого обобщения в течение 70-х гг. выделены *ведущие направления в теоретическом исследовании* ИИ: представление знаний; общение; рассуждения и планирование; восприятие; обучение; деятельность.

Новая парадигма привела на рубеже 80-х гг. к формированию ряда направлений по созданию *интеллектуальных практических приложений*. Наиболее привлекательными областями здесь были: традиционные системы управления; автоматизация научной и инженерной деятельности (интеллектуальные пакеты прикладных программ (ИППП)); расчетно-логические системы; обучающие системы (тьюторы); экспертные системы (ЭС); производство ЭВМ новых поколений.

Далее обратимся к изложению наиболее важных особенностей *современного периода развития* технологии ИИ, а также ряда ее аспектов, которые в той или иной мере легли в формирование текущего понятийного аппарата.

В этой связи возьмем за основу некоторые ведущие положения работ В. К. Финна, являющегося одним из известных, признанных в мировом научном сообществе последователей советской методологии построения ИИ [271; 273; 423; 425–427].

В работе [422] им системно объединены методологические и философские рассуждения, охарактеризованы основные проблемные вопросы внедрения технологий ИИ.

Принципиальные подходы в указанной работе выражены автором следующим образом: «Искусственный интеллект – направление

исследований компьютерной науки, в котором разрабатываются средства имитации и усиления умственной активности человека. Термин «умственная активность» требует уточнений посредством перечисления интеллектуальных способностей, представляющих феноменологию рационалистического сознания (точнее, ее идеальный тип в смысле Макса Вебера). В частности, такими способностями являются способности к рассуждению и порождению гипотез, способность к выдвижению цели и рефлексии, способность к поиску объяснения и к коррекции знаний в связи с изменением имеющихся ситуаций».

Далее автором определена «интеллектуальная система» (ИС), как компьютерная система с реализацией способности естественного интеллекта.

На рубеже восьмидесятых годов В. К. Финн разработал и внедрил метод автоматического порождения гипотез. В честь естествоиспытателя Джона Стюарта Милля (известного философа, логика и экономиста) данному методу было дано название ДСМ-метода.

Смысл работы метода состоит в использовании ДСМ-рассуждения, которое способно сделать правдоподобный и достоверный вывод на основании формализованной схемы. В основе логики построения подобного рассуждения лежит синтез познавательных процедур, таких как индукция, аналогия, абдукция.

Целью создания данной концептуальной конструкции – это получения новых знаний о предметной области на основе их автоматизированного представления. Такой подход относится к так называемым квазиаксиоматическим теориям (КАТ).

Предложенный подход по выявлению причинно-следственных закономерностей в формате ДСМ-метода успешно апробирован, например, в фармакологии, решении задач технической диагностики, анализа детерминант социального поведения.

Традиционная архитектура интеллектуальной системы (ИС) представляется следующим образом (рис. 1.3; рис. 1.4) [422].

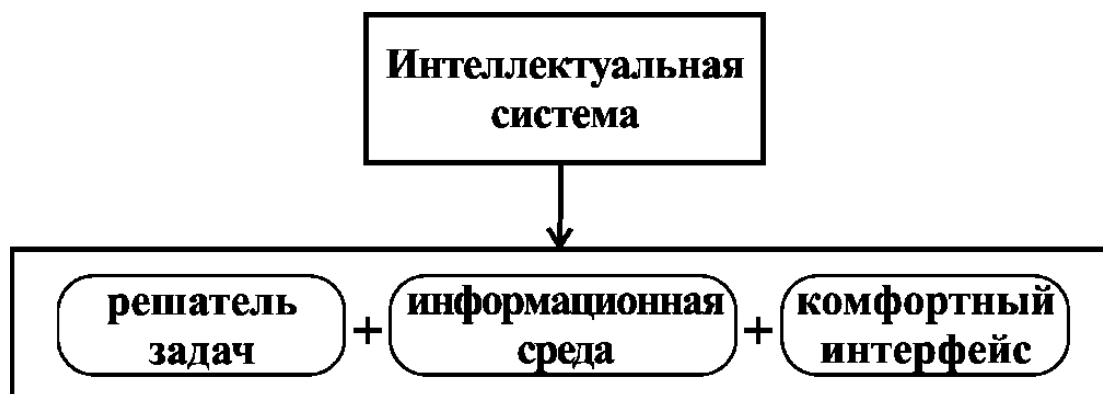


Рис. 1.3. Состав интеллектуальной системы [422]

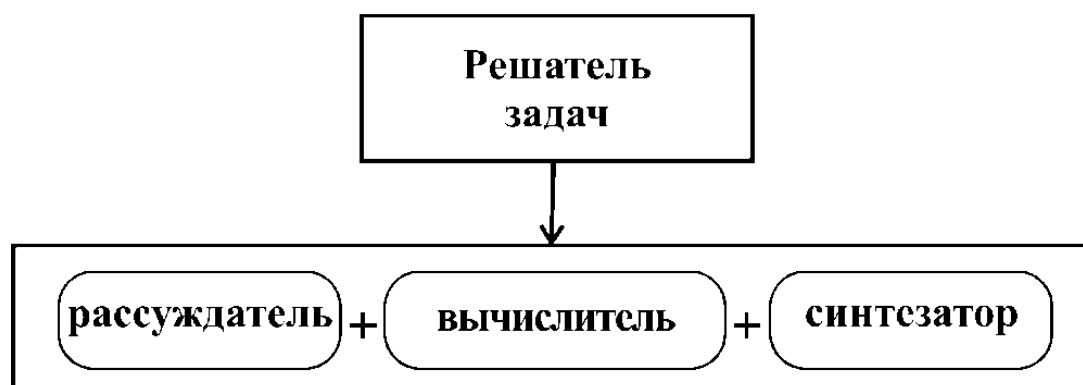


Рис. 1.4. Состав Решателя задач [422]

Поясним смысл каждого из приведенных элементов, формирующих понятие ИС, как основного продукта ИИ:

- *информационная среда* формируется за счет динамического объединения и развертывания разнообразного сервиса по обработке двух баз: фактов (БФ) и знаний (БЗ).

В БФ представлены массивы исходных отношений о предметной области. Отображение анализируемой области определяется классом задач, функционально решаемым в ИС в текущее время. Информационные массивы и их пересечения обеспечивают возможность применить индукцию и машинное обучение на основе ДСМ-метода – автоматическое порождения гипотез.

Вторая часть – это БЗ. В ней содержится совокупность КАТ, как средство представления знаний. Состав КАТ разнообразен и выражен рядом множеств:

- аксиом (отражают частично предметную область);
- фактов и гипотез;
- правил для правдоподобного и достоверного вывода;
- *комфортный интерфейс* предназначен в целом для «очеловечивания» ИС. В его составе средства: представления результатов работы (в том числе, в графическом виде); диалога на естественном языке; обучения пользователя работе с системой в целом;
- *решатель задач*, состоящий из рассуждателя, вычислителя, синтезатора;
- *рассуждатель* выполняет производство процедур дедуктивных рассуждений. Они обуславливают формализацию синтеза познавательных процедур (например, эвристика «индукция + аналогия + абдукция» в ДСМ-методе);
- *вычислитель* осуществляет вычислительные процедуры;
- *синтезатор* проводит комбинирование рассуждений и вычислений, а также выбор стратегий решения задач.

Напомним, что базисными продуктами ИИ выступают рассмотренные ИС. В дополнение могут быть названы когнитивные системы и интеллектуальные роботы (ИИ-роботы). В них реализуется автомати-

зированной ввод данных разнообразных форматов: акустических, визуальных, текстовых и т. д.

Таковы основные терминологические идеи работ В. К. Финна. Они использованы при развитии технологии ИИ и отражены в изданиях [271; 273; 423; 425–427]. Читателям, интересующимся отдельными аспектами, взглядами, перспективами развития методологической базы ИИ, целесообразно обратиться к ряду отечественных [75; 87; 98–99; 109; 116; 125; 145; 159; 162; 195; 235; 272; 276; 291; 301–302; 421; 431; 445; 447; 451; 464] исследований.

Значимое дополнение к общему представлению, конечно, необходимо почерпнуть и из зарубежных источников. В этом плане можно порекомендовать следующие работы [56; 77; 96–97; 100; 102; 150–151; 154; 156; 161; 198; 202; 205; 207; 226; 230; 232; 265; 344; 360–362; 382; 392; 403; 418; 432–435; 440; 452; 456; 465; 469–470; 473–474; 476–477; 481–485; 487; 489–490; 493–498].

Вместе с тем, приведенная и даже более широкая совокупность мнений, содержащихся в многочисленных изысканиях, будет формировать пока не утешительное представление. А именно: на сегодняшний день можно сделать вывод – однозначного теоретического понимания ИИ пока нет.

Во многом – из-за междисциплинарного объединения в данной технологии очень большого количества знаний, представлений, подходов, каждый из которых вносит свои концепты, создает новые «научные перекрестки». В силу этого ИИ является одновременно и наукой, и искусством, и технологией.

Для формирования определенности в текущем состоянии понятийных тенденций, наряду с изложенными рассуждениями В. К. Финна, попробуем сформулировать так называемые «рабочие определения», обратившись к работе [300].

Искусственный интеллект – это одно из направлений информатики, целью которого является разработка аппаратно-программных средств, позволяющих пользователю-непрограммисту ставить и решать задачи, общаясь с компьютером на ограниченном подмножестве естественного языка.

Система искусственного интеллекта (СИИ) – это компьютерная модель интеллектуальных возможностей человека при целенаправленном поиске, анализе и синтезе информации об окружающей действительности для получения о ней новых знаний и решения на этой основе различных задач.

Юнит искусственного интеллекта – отдельно взятая технологическая единица в виде компьютерной программы, робота, системы.

Отсутствие необходимой четкости в указанных определениях делает условным классификационное разделение категорий ИИ. Кроме того, современные системы ИИ сочетают несколько подходов од-

новременно, пересекаясь по ряду параметров. Тем не менее, отметим некоторые известные признаки соотношения ИИ к разным типам.

1. По уровню развития [318]:

– *слабый ИИ (Narrow AI)* – технологически предназначен для решения конкретных, предопределенных задач: распознавание лиц, прогнозирование погоды или перевод текста. Эти системы ограничены, как правило, одной областью применения и не обладают общим интеллектом. Подчеркнем, что большинство примеров в монографии, которые в авторских интересах ведомственно ориентированы к деятельности правоохранительных органов, связано именно с таким уровнем использования ИИ;

– *сильный или генеративный ИИ (General AI)*. Система такого уровня способна обеспечивать решение широкого спектра задач, присущих естественному человеческому интеллекту. В ней должно быть реализовано понимание, рассуждение, планирование и решение проблем в различных контекстах, сформировано суждение в условиях неопределенности, умение учиться, интегрировать предыдущие знания в процесс принятия решений, предлагать новаторские идеи.

Данный уровень пока находится на стадии исследований и отдельных успешных разработок, направленных на наделение машин сознанием;

– *сверхинтеллект или супер-ИИ (Super AI)*. Это форма ИИ, превосходящая человеческий интеллект по всем параметрам. Так, философ Ник Бостром определил его как «интеллект, который значительно превосходит когнитивные способности человека практически во всех областях» [96]. Он должен обладать сознанием и разумом, быть способным на реальные размышления.

А потому мог бы решать любые проблемы быстрее и эффективнее людей. Но на сегодняшний день это лишь гипотетические устремления и, возможно, хорошо, что в современных условиях не реализованные.

2. По типу поведения:

– *реактивный*. В этом случае системы ИИ реагируют на входные данные без учета прошлого опыта. Например, программа *Deer Blue* от IBM. Она смогла победить чемпиона мира по шахматам Гарри Каспарова, принимая решения исключительно на основании текущих позиций фигур на шахматной доске;

– *с ограниченной памятью*. Они способны учитывать предыдущий опыт, чтобы принимать более обоснованные решения. Например, голосовые помощники Сири и Алиса используют историю запросов пользователей для улучшения взаимодействия;

– *теоретический ИИ самосознания*. В теории этот тип ИИ способен осознавать себя и свое окружение, как человек. Однако на практике такие системы еще не созданы, только прорабатываются подходы для их разработки.

3. По области применения:

- *машинное обучение*. Используется подход, обучающий модели на больших данных для выявления закономерностей и принятия решений. Включает методы глубокого обучения, многомерного нелинейного регрессионного анализа, классификации и кластеризации;
- *нейронные сети*. Модели этого типа имитируют работу человеческого мозга и состоят из множества взаимосвязанных узлов (нейронов). Используются для анализа сложных паттернов в данных;
- *обработка естественного языка*. Это направление занимается пониманием и генерацией человеческой речи. Включает технологии перевода, чат-ботов и голосовых ассистентов;
- *компьютерное зрение*. Основное применение: анализ изображений и видео, включая распознавание объектов, лиц и сцен;
- *робототехника*. Целевое использование: управление роботизированными системами – промышленными роботами, беспилотными транспортными средствами.

Обратимся теперь к *нормативно-правой стороне регулирования ИИ*, а также особенностям правоприменительной деятельности, системе угроз и ограничений.

Системы права развитых государств, в том числе – и России, как правило, на конституционном уровне закрепляют верховенство международного права при рассмотрении ситуаций, которые по тем или иным причинам не находят в стране должной нормативно-законодательной регламентации. Далее в системе права иерархия построена следующим образом: конституция, конституционные законы, федеральные законы, кодексы и т. д. Исходя из данного подхода организации системы права, дадим характеристику основным нормативно-правовым уровням государственного регулирования применительно к сфере ИИ.

При этом подчеркнем наличие некоторого для мировой юридической практики противоречия. Связано оно с тем, что в эпоху промышленной революции на ее 4-м уровне (*глобальное общество трансформируется в единую киберфизическую систему*) [453] имеется определенное отставание нормативно-правового регулирования от развития новых технологий. Технологии, в том числе и ИИ, бурно развиваются, активно и широко внедряются во все сферы человеческой жизнедеятельности. А нормативно-правовое регулирование очень многих сторон их внедрения и эксплуатации, начиная с категориально-понятийного аппарата, отстает от требуемых параметров, присущих развитым правовым отношениям в обществе.

Проиллюстрируем это на уровне международно-правовых отношений. Так, в начале 2024 г. в сети X было выставлено сообщение главы Европейского парламента (ЕП) Р. Метсола [239] о том, что на заседании ЕП одобрен первый в мировой практике закон комплексного регулирования ряда вопросов в области ИИ [240].

Основная цель закона состояла в государственном регламентировании перечня обязательных, реально выполнимых требований, особенностей их понимания и практической эксплуатации технологий ИИ. Указанные требования должны позволить на уровне разработчиков и специалистов по внедрению представить структуру и совокупность потенциальных рисков при реализации новых систем ИИ, дать четкое представление о системе критериев их контроля со стороны человеческого общества.

Разработчики Европейского закона ориентировались в своей деятельности на составление таких условий применения систем ИИ под гарантированным контролем, которые подразумевали обеспечение прозрачной, надежной эксплуатации подобных систем, выполнения обязательств недискриминационного характера и соблюдения мер в области защиты окружающей среды.

Важным являлось стремление разработчиков закона ввести *юридическое понятие «искусственный интеллект»*, которое можно было бы использовать в качестве определения особенностей функционирующих и потенциально создаваемых систем, а также регулирования ИИ в различных юрисдикциях. Поэтому разработчики полагали, что закон – не просто свод правил, а стартовая площадка для Европы в глобальной гонке, которая разворачивается в области ИИ

Такой статус определяет целый ряд аспектов ее разработки, существования и эксплуатации, прав и ответственности, финансирования и использования ресурсов, обеспечения целенаправленного применения, противодействия как *внутренним угрозам* технологиям ИИ, так и *внешнего криминального интереса* к их противоправному применению, а также других сторон и граней, значимых для человеческой деятельности. Естественно, что закон должен рассматриваться, прежде всего, на международном уровне с необходимостью его ратификации многими странами и образования ими сообщества, поддерживающего единую систему правил и требований.

Сделаем акцент на существовании некоторых угроз, которые в законе предлагается *запрещать в системах ИИ*, как несущих неприемлемые риски для безопасности людей. Имеются в виду такие системы, которые применяют техники манипулирования людьми или эксплуатации их уязвимостей.

В законе приведена классификация, которая разделяет все системы и инструменты, основанные на ИИ, по уровню риска – от низкого до неприемлемого.

В нем нашли закрепление нормы, которые строго ограничивают ситуации применения систем ИИ для удаленной идентификации на основе биометрических технологий, осуществляемой в публичных местах в режиме так называемого реального времени. Ограничивается сбор биометрических данных в социальных сетях, а также в системах видеонаблюдения, которые могут собирать сведения для формирова-

ния баз данных, ориентированных на распознавание лиц или распознавание эмоций.

Это говорит об имеющихся противоречиях в законе и требует дополнительных нормативно-правовых регламентаций по его совершенствованию, урегулированию многих частных особенностей его применения. Типичной нормой при этом определено решение суда, который может выдавать различные разрешения, но в ограниченных случаях.

В рамках реализации закона, например, запрещается полиции применять системы предиктивной аналитики для профилактики правонарушений. Исключением для использования в работе полиции указанных технологических возможностей является угроза теракта, поиск жертв, раскрытие и расследование тяжких преступлений.

Другим частным случаем является регулирование использования генеративного ИИ (например, таких систем, как чат-бот *ChatGPT*). Так, предполагается сделать доступной информацию о книгах, музыкальных произведениях, картинах и прочих форматах представления знаний, которые защищены авторским правом и использовались при обучении ИИ. Данные меры должны противодействовать нарушениям авторского права и плагиату.

Кроме того, подобный подход может быть реализован для высокорисковых систем, функционал которых обеспечивается работой ИИ. К ним, в частности, относится беспилотный транспорт и медицинское оборудование.

Определяя требование *прозрачности*, закон постулирует, что тексты, аудио-, видео-, фотоматериалы и чат-системы, полученные как результат использования систем ИИ, должны быть обязательно *промаркированы*.

Завершая анализ примера нормативно-правовой регламентации международного уровня в области использования систем ИИ, подчеркнем, что принятие в ЕС первого закона должно послужить примером для правительств других стран.

Далее обратимся к объемному, системному труду коллектива российских ученых-юристов «Глобальный атлас регулирования искусственного интеллекта», который регулярно обновляется для получения актуальной справочной информации в рассматриваемой области. В монографии использованы сведения из этого источника за 2022, 2023, 2024 годы [133–135].

Из-за значительного объема материалов, приведем лишь их основные положения. Читателю, заинтересованному в более подробном уровне сведений, рекомендуем обратиться к первоисточникам.

При переизданиях Атласа каждый раз подвергаются анализу более тысячи различных зарубежных нормативных источников. Так, последняя редакция содержит сведения об имеющемся опыте 43 юрис-

дикций и 18 международных организаций, которые считаются ведущими в разработке и внедрении ИИ в мировой практике.

Проведенная в течение ряда лет сравнительная аналитическая работа позволила авторам отмеченных изданий выделить унифицированные критерии, по которым можно оценивать правовые системы различных стран мира в целях понимания правового регулирования на развитие технологий ИИ. С учетом этих критериев сформирована структура книг, приводятся и обобщаются сведения из нормативных источников конкретных стран:

- стратегическое планирование технологий ИИ;
- общие принципы регулирования технологий ИИ;
- регулирование разработки и использования моделей генеративного ИИ, дипфейков и рекомендательных сервисов;
- особенности регулирования ИИ в области данных, в частности – персональных;
- регулирование разработки и применения ИИ в сфере беспилотного транспорта;
- регулирование ИИ в здравоохранении;
- этические вопросы в сфере ИИ.

Приведем некоторые сведения, касающиеся состояния вопроса в Российской Федерации. Укажем при этом, что также имеется довольно объемный материал. Только в издании атласа 2024 г. [133] рассмотрено около 100 нормативно-правовых документов, регулирующих использования технологий ИИ по указанным выше критериям.

Повсеместное внедрение технологий ИИ во все сферы жизнедеятельности приводит к выводу, что процессы регулирования должны распространяться, по существу, на всю правовую систему страны.

В монографии рассмотрим только положения, связанные с планированием в рассматриваемой сфере. Еще одно направление – использование ИИ в беспилотных транспортных средствах – будет предметом ряда последующих глав, где затронем и нормативно-правовые аспекты.

При *стратегическом планировании* страны в настоящее время реализуется Национальная стратегия развития искусственного интеллекта на период до 2030 года «О развитии искусственного интеллекта в Российской Федерации» [13]. Значимые направления для нормотворчества применительно к рассматриваемым технологиям нашли закрепление в Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 года [13; 23].

Кроме того, в работе находится федеральный проект «Искусственный интеллект» [24]. Его координатором выступает Министерство экономического развития Российской Федерации.

Другим регулятором является Национальный центр развития искусственного интеллекта при Правительстве Российской Федера-

ции. В 2022 г. он стал площадкой отбора ИИ-решений для бизнеса, науки и государственных органов. На ней проводится экспертиза документов о регулировании ИИ, а также экспертное сопровождение внедрения ИИ в государственном управлении и в секторах экономики.

Интерес представляют объединение участников рынка в области ИИ – Ассоциация «Альянс в сфере искусственного интеллекта». Среди ее крупных игроков можно назвать ООО «Яндекс», ПАО Сбербанк, ПАО «МТС», ПАО «Газпромнефть», ООО «Группа компаний «Руссагро», группа «Самолет», ПАО «Сибур» и ПАО «Северсталь». Ассоциация стремится создать центры развития ИИ в стране, обеспечить ее технологическое лидерство на глобальном рынке.

Касаясь сферы *общего регулирования*, подчеркнем, что в стране пока отсутствует общий закон, посвященный ИИ. Чтобы преодолеть этот довольно значительный правовой недостаток, сделано несколько попыток:

- 2016 г. ознаменовался предложением концепции закона о робототехнике – «О регулировании умных роботов», которая направлена на развертывание дискуссии в обществе по регулированию ИИ и роботов;

- в 2017 г. исследовательский центр проблем регулирования ИИ и робототехники также предложил дискуссионную Модельную конвенцию об ИИ и робототехнике (РТ);

- в 2018 г. в рамках федерального проекта «Нормативное регулирование цифровой среды» международной юридической фирмой *Dentons* по заказу Центра компетенций по нормативному регулированию цифровой экономики, функционирующего на базе Фонда «Сколково», выполнено комплексное исследование состояния ИИ в стране;

- в 2019 г. инициированы законодотворческие мероприятия, приведшие к созданию Концепции регулирования ИИ и РТ на период до 2024 г.;

- в 2020 г. принят федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» [7].

Именно в этом законе принято *правовое определение понятия ИИ* (подп. 2 п. 1 ст. 2 Федерального закона № 123-ФЗ): *искусственный интеллект* – комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Такой комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (ПО), а также процессы и сервисы по обработке данных и поиску решений.

Сходной по трактовке является редакция данного определения, данная позднее в Указе Президента Российской Федерации от 15.02.2024 № 124, определившем обновление Национальной стратегии развития искусственного интеллекта на период до 2030 года [12].

В нем добавлены следующие две трактовки.

Технологии искусственного интеллекта – совокупность технологий, включающая в себя компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы ИИ.

Перспективные методы искусственного интеллекта – методы, направленные на создание принципиально новой научно-технической продукции, в том числе – в целях разработки универсального (или так называемого сильного) ИИ.

К ним относятся:

- автономное решение различных задач;
- автоматический дизайн физических объектов;
- автоматическое машинное обучение;
- алгоритмы решения задач на основе данных с частичной разметкой и/или незначительных объемов данных;
- обработка информации на основе новых типов вычислительных систем;
- интерпретируемая обработка данных и другие методы.

Кроме этого, укажем на действие в стране с 2020 г. федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [11]. Совместно с ним следует отметить действие с 2021 г. Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [5]. Им регламентированы экспериментальные правовые режимы по ряду направлений ИИ:

- беспилотные такси;
- грузовые перевозки с использованием большегрузных дронов;
- оказание услуг медицинской помощи с применением телемедицинских технологий;
- аналитика «больших» медицинских и экономических данных.

Следующий аспект относится к функционированию Технического комитета по стандартизации № 164 «Искусственный интеллект» (ТК 164), который создан на основании Приказа Росстандарта от 25 июля 2019 г. № 1732. Его цель – повышение эффективности работ по стандартизации в области ИИ на национальном и международном уровнях. В состав ТК 164 входит более 120 профильных организаций.

По сути, данный комитет «зеркально» отражает международный подкомитет SC 42 *Artificial Intelligence* объединенного технического ко-

митета *ISO/IEC JTC 1 Information Technologies*. В связи с этим он выполняет функции постоянно действующего национального органа в *ISO*.

Наряду с этими нормативно-правовыми разработками, имеются самостоятельные направления, которые не входят в рамки предметной области монографии. В частности, в группу общего регулирования входят законотворческие инициативы, связанные с налоговым стимулированием развертывания технологий ИИ, поддержки ИТ-отрасли, государственно-частного и муниципально-частного партнерства.

Завершая обзор по нормативно-правовому регулированию систем ИИ в РФ, укажем на необходимость ее дальнейшего совершенствования. Ведь на сегодняшний день в стране, по существу, не разработаны правила использования ИИ в государственном управлении, а также специальные нормативные правовые акты, регулирующие применение ИИ в ведущих социально-экономических сферах.

В заключение раздела отметим, что в нем проанализированы разноплановые аспекты понятийного аппарата в сфере ИИ. Рассмотрены научно-теоретические, концептуальные, организационные, технологические, правовые и иные стороны многогранной деятельности по разработке и внедрению ИИ, проникающего в самые разнообразные области жизнедеятельности общества.

При этом акцентировано внимание на том, что работы по созданию и внедрению систем ИИ продолжают активно расширяться, приводя на каждом своем шаге к неожиданным результатам и направлениям использования. Далее мы вернемся ко многим уже рассмотренным вопросам, чтобы конкретизировать их особенности, развить понятия, мнения, перспективы, правовую регламентацию.

1.2. Информационная и кибербезопасность. Киберпреступность – состояние и тенденции

Рассмотрим некоторые исторические аспекты, связанные с технологиями *защиты информации*.

Так, в исследовании В. Л. Янина анализируется археологический материал об актовых печатях X–XV вв. в древней Руси [462]. Основные положения данного исследования указывают на то, что для развития документального оборота в то время потребовались способы, позволяющие провести удостоверение подлинности и юридической силы документов, указов великих и местных князей, бояр и высшего духовенства.

На Руси для этих целей были введены печати, сохранившие указанное предназначение и до настоящего времени. Следуя традициям Византии, принятым в то время, в арсенале князей и духовенства нашли широкое применение печати, прикрепленные к документу на кожаном ремешке или шелковом шнурке. За такой способ соединения они получили название «вислых» печатей.

В техническом плане подобные печати («буллы») выполнялись в виде металлических шариков из свинца, серебра, золота, реже – позолоченного серебра с отверстием для шнура.

Для выдавливания оттиска изображения и надписи на обеих сторонах «буллы» использовались аналоги современного пломбирователя. Они представляли собой специальные щипцы, которые называли буллотирый (рис. 1.5). «Булла» вставлялась в буллотирый. По нему наносился удар молотком. В результате на мягком металле наносился двусторонний оттиск.



Рис. 1.5. Внешний вид буллотирья [462]

Другое обращение к историческим фактам также свидетельствует об обеспечении защиты информации, поддержания ее удостоверяющего значения. Речь идет о применении *биометрических характеристик человека* для реализации рассматриваемого функционала.

Авторами подробно исследована эта группа характеристик в монографии [84]. Из их довольно обширного арсенала самое распространенное применение нашли *отпечатки пальцев (дактилоскопические отпечатки)*. Их первоначальные применения, как следует из документов, относятся к Древнему Вавилону, то есть к периоду времени за несколько сотен лет до нашей эры.

Например, нанесенные на глиняную поверхность отпечатки удостоверяли, подтверждали какие-либо документальные, договорные, формы взаимоотношений людей. При этом осуществлялась практическая реализация представлений о неповторимости биометрических признаков и, следовательно, возможности их использования как метода защиты информации, исключая *подделки*.

Считается, что одной из самых ранних находок, где отчетливо различимы отпечатки пальцев, являются результаты археологических

раскопок на северо-западе Китая. Это глиняная посуда, возраст которой оценивается в 6 тысяч лет. На ней сохранились отпечатки пальцев с фрикционным гребнем (*friction ridge* – в терминах криминалистической науки) [500]. К периоду неолита относятся и иные примеры фиксации отпечатков пальцев на различных древних материалах. В частности, обнаружены отпечатки пальцев строителей на глине, используемой для производства кирпичей [466].

Об использовании оттисков свидетельствуют и другие древние артефакты, на которых имеются гребневидные узоры, но уже явно вырезанные (стилизованные), а не оставленные как случайные или целенаправленные следы. Примерами конструкции фрикционных гребней, являются мегалитические произведения искусства в гробнице Гавринис на острове около западного побережья Франции и в гробнице в Ньюгрейндж на побережье Ирландии (рис. 1.6).



Рис. 1.6. Один из камней Ньюгрейнджа (<http://www.ancient-wisdom.co.uk>.)

Систематизированный анализ становления методов дактилоскопии и их применения в правоохранительной деятельности в качестве *доказательства личности человека* в оперативно-розыскной и следственной практике, можно найти в американском справочнике [492].

Наконец, стремление к обеспечению защиты информации выражается в *шифровании* текстовой информации. Смысл его состоит в определенном преобразовании исходного текста таким образом, чтобы получились наборы знаков или букв, недоступные для прямого понимания без знаний конкретных технологий шифрования.

Шифрование базируется на криптографическом преобразовании данных. Оно зародилось в глубокой древности. Например, глиняные таблички из Месопотамии содержат зашифрованные сообщения, относящиеся к XX в. до н. э. [380].

В результате развития применяемых при этом методов сформировано научно-практическое направление – *криптология*, представленная двумя дисциплинами – криптографией и криптоанализом.

Криптография применяет математические методы, достижения науки и техники для преобразования открытой защищаемой информации в закрытую, значительно затрудняющую смысловое понимание или восстановление исходного открытого текста.

Криптоанализ – наука о методах раскрытия и модификации данных. Она развивается по двум направлениям.

Первое – исследование информационных массивов, подвергнутых криптографическому преобразованию, в целях восстановления семантического содержания исходных документов.

Второе – используя криптографические подходы, фальсифицировать исходные документы в целях передачи заведомо ложной информации.

Важной современной особенностью является то, что возможности (и довольно распространенные) использования криптографических технологий в преступных целях создают дополнительные трудности в дешифрировании информации при проведении оперативно-розыскных и следственных действий правоохранительными органами. В силу этого применение криптоаналитических методов, в том числе со значимой поддержкой технологиями ИИ, становится актуальной необходимостью в арсенале средств оперативных и следственных подразделений ОВД.

Начало революционных изменений в оценке рассматриваемой предметной области положено после окончания Второй мировой войны. Этому способствовали абсолютно новые технологические решения (обработки, передачи информации и связи), математические методы (системный анализ, исследование операций), а также возникшее понимание информации как главенствующего ресурса развития общества и, как следствие, создание и развитие концепции противоборства за владение им.

В частности, совокупность указанных факторов легла в основу развертывания политической кампании холодной войны. Она, по сути своей, положила начало информационной войны и обострившегося информационного противостояния с необходимостью разработки и внедрения целой индустрии обеспечения информационной и кибербезопасности.

Данное научно-практическое направление развивается уже десятки лет, представлено множеством работ ведущих ученых и практиков всего мира, попытками международного и национального регламентирования данной многогранной сферы. Представим изложение ее основных понятий.

Во многом они отражают исследования по кибербезопасности и особенности решения оперативно-служебных задач правоохрани-

тельной деятельности в этой связи [73–74; 85; 105; 119; 123–124; 129–130; 165; 169; 171; 178–179; 203; 208–209; 216; 293; 309; 342; 357; 380; 394–395; 428–429; 441; 443; 455; 463; 499].

Вначале приведем исходное понимание различных аспектов в области безопасности.

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Конкретизируем приведенные определения к информационной сфере (среде), связанной с созданием, преобразованием и потреблением информации.

Защищаемая информация – сведения (данные), которым постоянно или на определенное время присвоен один или несколько атрибутов статуса защищенности.

Статус защищенности информации – состояние информации, определяемое необходимостью:

- обеспечения в полном объеме физической и логической целостности информации;
- предупреждения несанкционированного получения, модификации и размножения информации.

Угроза информации как дестабилизирующий фактор – явление, событие, случай, которые могут произойти в заданном интервале времени, в результате чего возможно нежелательное воздействие на защищаемую информацию по одному или нескольким аспектам статуса защищенности.

Уязвимость информации – ее свойство при нахождении в процессе обработки подвергаться воздействию внутренних или внешних угроз с точки зрения одного или нескольких атрибутов статуса защищенности.

Безопасность информации – состояние информационных ресурсов и систем, при котором с требуемой вероятностью обеспечиваются обозначенные параметры защиты информации (данных) от случайного или преднамеренного доступа лиц, не имеющих на это право.

Безопасность информационной сети – меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в ее нормальное функционирование или попыток разрушения ее компонентов. Включают защиту оборудования, ПО, данных.

Защита информации в автоматизированных системах ее обработки – использование средств и методов, принятие и осуществление мер в целях обеспечения требуемой защищенности информации.

Защищенность информации – такое состояние, когда на заданном уровне поддерживаются ее требуемые характеристики, определяющие установленный статус хранения, обработки и использования.

Защита информации – комплекс мероприятий, организуемых и проводимых в целях предотвращения ее хищения, утраты, несанкционированного уничтожения, искажения, модификации, копирования, блокирования и т. д.

Система защиты информации – организованная совокупность методов, средств и мероприятий, создаваемая в системе обработки данных для защиты информации.

Совокупность приведенных определений и направлений обеспечивает формулирование содержания информационной безопасности.

Информационная безопасность – способность государства, общества, личности обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы, информационные потоки для поддержания своей жизнедеятельности, устойчивого функционирования и развития.

Созданная способность должна эффективно противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное, общественное сознание и психику людей, а также на компьютерные сети и другие технические и технологические средства оперирования информацией; поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы и в каких бы формах оно ни было навязано.

Ориентация общества на компьютеризацию вызвала формирование понятий «компьютерная информация», «компьютерная безопасность». И в этой части развернута и пока продолжается научно-практическая дискуссия.

В частности, она связана с тем, что общесистемное понимание информации и обеспечение ее безопасности, как правило, относятся не к общим взглядам, а к ее конкретным свойствам и характеристикам [85], которые, выражаются, например, в аспекте защиты информации в невозможности ее блокирования, копирования, уничтожения, модификации.

На основе отмеченных и иных трактовок формировались и производные понятия, определяемые развитием негативных процессов в сфере информационных технологий. В частности, интересно одно из ранних преставлений о компьютерных преступлениях.

Компьютерные преступления – любое деяние, влекущее незаконное вмешательство в имущественные права, возникающие в связи с использованием ЭВМ [216; 380].

Наряду с указанной трактовкой, с течением времени создавались и внедрялись многие понятия киберсферы, например, киберпространство; преступления в сфере высоких технологий; преступления, совершенные с использованием информационно-коммуникационных технологий (ИКТ); киберустойчивость [306], как интегральный показатель, объединяющий подходы к киберживучести, киберпомехоустойчивости и кибернадежности.

Одним из базовых стало понятие *киберпространства*, появившееся наряду с появлением Всемирной паутины (от англ. WWW – World Wide Web). Оно подразумевало (на физическом или техническом уровне) охват всех существующих компьютерных систем и сетей, дополняясь информационной, социальной, культурной, политической составляющими.

На фоне в целом позитивной волны достижений сформировались и негативные проявления, приведшие к проблемам кибербезопасности, зарождению киберпреступности. Отметим некоторые особенности понимания киберпреступности в современных исследованиях, особенно соотношения понятий *информационной* и *кибербезопасности*.

Их становление в России связано с активным развитием науки и практики в области защиты информации, регулируемой со стороны государства, и формированием базового массива теоретических и методических основ в научных институтах, учебных заведениях страны, включая научно-образовательные учреждения системы МВД Российской Федерации. Кратко изложим позицию коллектива авторов из МВД России, представленную в современном учебнике по основам кибербезопасности [298].

Авторы подчеркивают, что понятие «кибербезопасность», в отличие от информационной безопасности, имеет американское происхождение. Оно первоначально отождествлялось с военными операциями в киберпространстве, понимаемом в силу специфики как современным театром военных действий [439].

Следует подчеркнуть, что понятие кибербезопасности в научно-техническом мире пока находится на стадии дискуссионного обсуждения [231]. Однако при этом, несмотря на определенные терминологические разночтения, ведущие мировые системы стандартизации *ISO*, *IEC* и *ITU* применяют именно указанное понятие. Например, один из новых стандартов *ISO/IEC 27100:2020* определил кибербезопасность как свойства защищенности активов (общества, организации, человека) от киберрисков, связанных с эксплуатацией уязвимостей в киберпространстве – цифровой среде.

Обратим внимание на новые аспекты, которые связаны с пониманием безопасности уже самого ИИ, на который как на самостоятельный объект осуществляется целенаправленное киберпреступное воздействие [501]. На эту особенность негативных проявлений в киберпространстве обращено внимание в материалах глав 3, 4.

В частности, указывается на то, что единичный сбой в работе сверхразумной системы может привести к катастрофическому событию глобального масштаба, без шансов на восстановление указанной системы.

Поэтому цель обеспечения безопасности ИИ должна в идеале дать возможность добиться 100 % защиты систем, что, к сожалению, практически не достижимо. Поэтому сейчас начинает прослеживаться тенденция трактовок – от обеспечения кибербезопасности к поддержанию киберустойчивости как способности осуществлять системой свое штатное функционирование в условиях воздействия компьютерных атак в киберпространстве [238].

Нужно также отметить, что и соотношение кибер- и информационной безопасности в научном сообществе все более определяется следующим образом – кибербезопасность выступает как часть информационной безопасности [231].

Обозначим некоторые аспекты взаимосвязи понятий *кибербезопасности* и *киберпреступности*.

Кибербезопасность объединяет все действия в целях обеспечения защиты сетевых и информационных систем, пользователей таких систем, которые подвергаются киберугрозам.

Логическим продолжением этой деятельности является противодействие киберпреступности. Условием ее эффективности является организация требуемого уровня сотрудничества и информационного обмена между субъектами кибербезопасности и правоохранительными органами.

В общем виде понимание *киберпреступлений* как противоправной деятельности в киберпространстве, совершаемых с использованием информационно-коммуникационных технологий (ИКТ), раскрывается, например, в работах [84; 149; 175; 194; 199; 222; 227; 236; 289; 294–295; 297–298; 306; 345–347; 354; 374; 381; 397–398].

При этом различие понятий «киберпреступление», «преступление, совершенное с использованием ИКТ» в самом общем виде выглядит следующим образом.

Киберпреступления совершаются в киберпространстве на основе применения информационных технологий и интернета. К ним относятся: распространение вредоносного ПО, хакерские атаки, фишинг, сетевые варианты мошенничества и т. д.

Преступления, совершенные с использованием ИКТ, охватывают кроме киберпреступлений и другие их виды, реализуемые не обязательно в виртуальном пространстве. Например, применение ИКТ в процессе подготовки, совершения, сокрытия следов при обычных грабежах, разбоях, убийствах и т. д.

На настоящий момент киберпреступность выделяют в отдельный вид (по конкретным формам и способам совершения). Ее важной особенностью является динамичность компьютерных сетевых систем,

постоянно развивающихся и изменяющихся и, тем самым, затрудняющей процессы однозначного понимания, нормативно-правового закрепления, тактики сбора ориентирующей и доказательственной информации.

Средствами совершения киберпреступлений являются компьютерная техника, мобильные телефоны, иные электронные гаджеты и носители. Условной средой для их реализации является виртуальное или киберпространство. Оно проявляется в сложности оперативного выявления, осуществления процессуальных действий и сбора доказательств о противоправных деяниях.

Компьютерной атакой является воздействие программно-аппаратных средств на инфокоммуникационные сети с целью нарушения или прекращения их функционирования. Данная трактовка определена Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [4]. Его принятие способствовало, в частности, внесению в Уголовный кодекс Российской Федерации (УК РФ) уголовной ответственности по ст. 274.1 УК РФ.

Другим примером нормативно-правового регулирования является установление уголовной ответственности за мошенничество с использованием электронных способов оплаты, а также за другие виды «компьютерных мошенничеств» (ст. 159.3 и ст. 159.6 УК РФ) на основании действия Федерального закона от 23 апреля 2018 г. № 111-ФЗ [6].

Разработаны и другие нормативно-правовые документы для регулирования названной сферы [14–15; 17].

Как видно из приведенного краткого экскурса в международных и национальных правовых системах, сегодня нет единого подхода к определению киберпреступности. Хотя, несмотря на отсутствие общепринятого понятийного мнения, оно используется как в ряде документов нормативного регулирования, так и в практической правоприменительной сфере.

Так, известный международный правовой акт – Будапештская конвенция о киберпреступности – и тот содержит подмену понятий. В частности, термин «киберпреступление» заменяется термином «компьютерное преступление» [1].

Указанные сложности понятийного характера сохраняют свою актуальность уже два десятилетия. Об этом говорят, например, термины современной Конвенции ООН против киберпреступности, принятой в 2024 г. [2].

Многогранность исследуемой предметной сферы приводит к необходимости детализированного нормативно-правового регламентирования проблемы киберпреступности. Так, Конвенция отражает правовой статус взаимоотношений на основе следующих рабочих терминов «информационно-коммуникационная система», «электрон-

ные данные», «данные о трафике», «абонентские данные», «персональные данные», «серьезные преступления», «доходы от преступления» и ряда других.

Укажем некоторые особенности нормативно-правового регулирования, изложенные в Конвенции. Так, она:

- разделяет киберзависимые преступления (например, хакерство) от кибермодифицированных (например, онлайн-мошенничество);
- дает определение цифровым доказательствам, устанавливает стандарты для их сбора, сохранения и допустимости в судебных разбирательствах;
- криминализирует такие преступления, как кража личности, онлайн-мошенничество и нарушения интеллектуальной собственности;
- предоставляет органам власти инструменты для электронного наблюдения, перехвата данных и доступа к сохранённым данным с учётом судебного надзора.

Вернемся к характеристике Будапештской конвенции о киберпреступности и новым в то время понятиям киберсферы, как первому, системному и основополагающему международному нормативно-правовому документу. Выше уже отмечен определенный ее недостаток во введении трактовки киберпреступлений, обусловленный многими причинами теоретического и практического уровня.

Тем не менее, указанная конвенция вводит реестр киберпреступлений, к которым на системном уровне относят преступления с использованием компьютерной техники. В целом в составе отмеченного перечня:

- противозаконный доступ к компьютерной системе;
- неправомерный перехват компьютерных данных; воздействие на компьютерные данные;
- противозаконное использование компьютерных устройств, программ, паролей, кодов доступа;
- мошенничество с использованием компьютерных технологий; правонарушения, связанные с производством и распространением детской порнографии;
- правонарушения, связанные с нарушением авторского права и смежных прав [1].

Точка зрения специалистов Лаборатории Касперского сосредотачивается на определении киберпреступности как трактовки преступной деятельности с использованием компьютера либо с атакой на него, компьютерную сеть или сетевое устройство.

К киберпреступлениям они относят:

- мошенничество с использованием электронной почты и интернета;
- кражу «цифровой личности» (хищение и использование личных данных);

- кражу данных, зафиксированных на платежных картах, а также другой финансовой информации;
- хищение и перепродажу корпоративных данных;
- кибершантаж (вымогательство денег под угрозой атаки); атаку с использованием программ-вымогателей;
- криптоджекинг (майнинг криптовалют с использованием чужих ресурсов);
- кибершпионаж (получение несанкционированного доступа к государственным или корпоративным данным);
- нарушение работы систем в целях компрометации сети;
- нарушение авторских прав;
- онлайн-торговлю запрещенными товарами;
- домогательства;
- изготовление или хранение детской порнографии [450].

На рис. 1.7 представлены основные виды киберпреступлений, а также характеристики их негативных последствий [238].

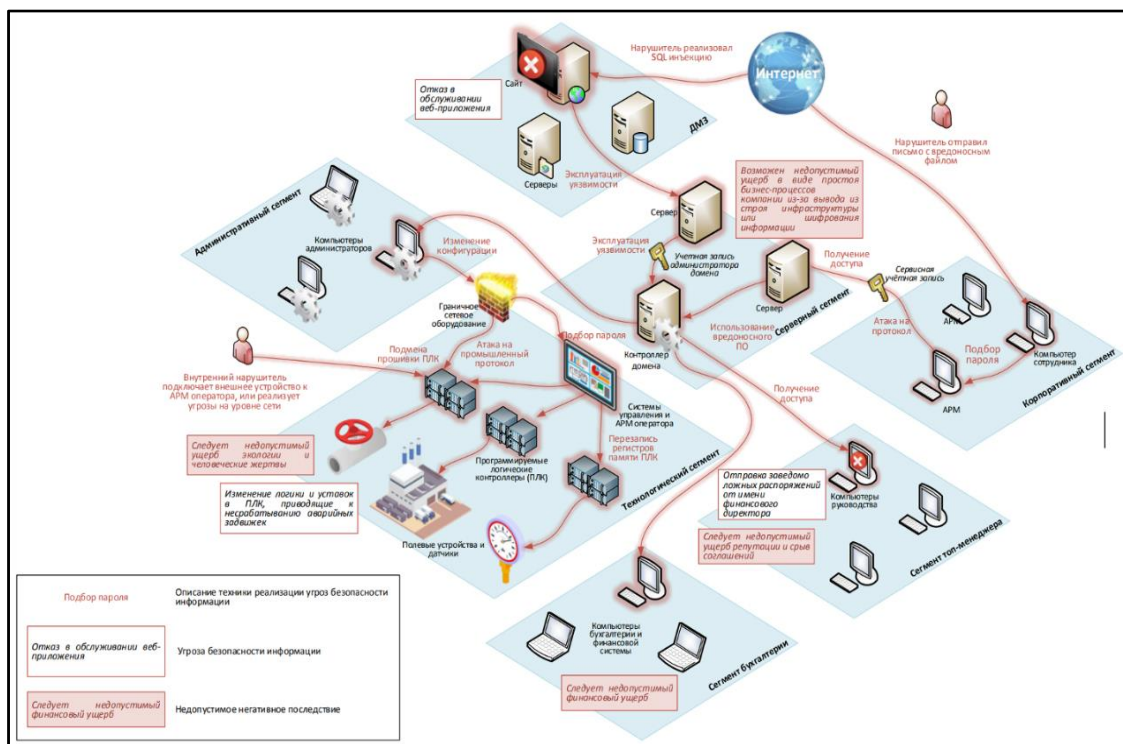


Рис. 1.7. Примеры действий кибернарушителей [238]

Из общего представления о становлении и совершенствовании видов киберпреступлений можно сделать вывод, состоящий в том, что технологии современного цифрового мира предоставляют значительные негативные возможности для процессов подготовки и осуществления новых опасных деяний – предоставление высокой мотивирующей способности в обеспечении анонимности лиц, к ним причастных.

Все это ведет к ранее небывалому росту киберпреступлений во всем мире. Приведем две тенденции (рис.1.8, 1.9).

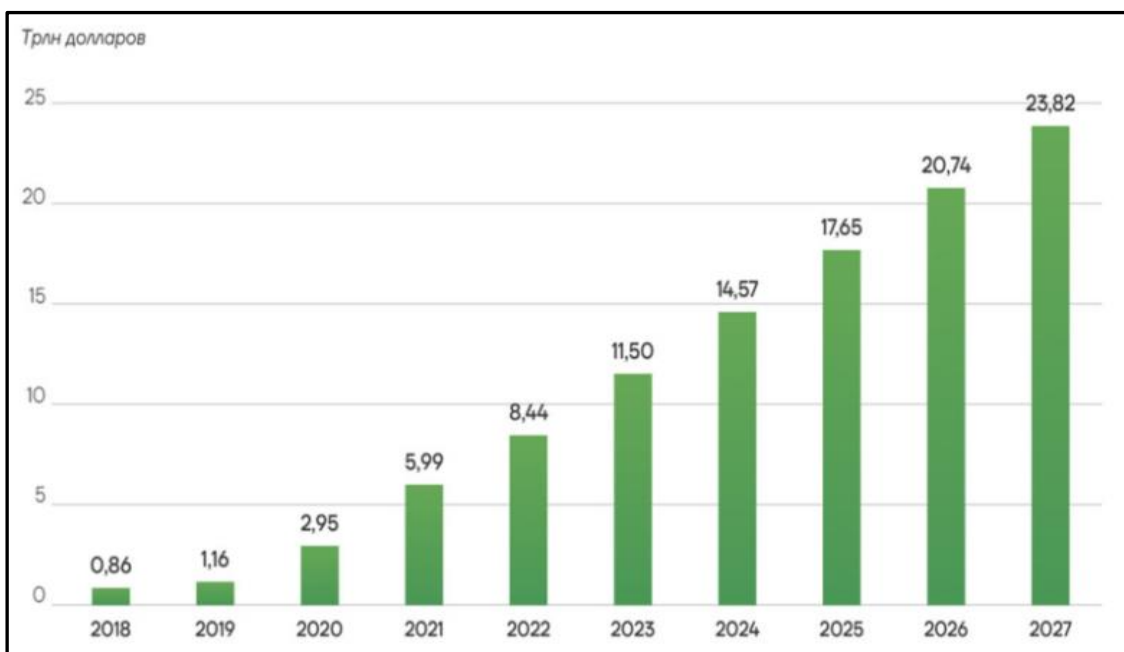


Рис. 1.8. Ежегодные потери в мире от кибератак [89]

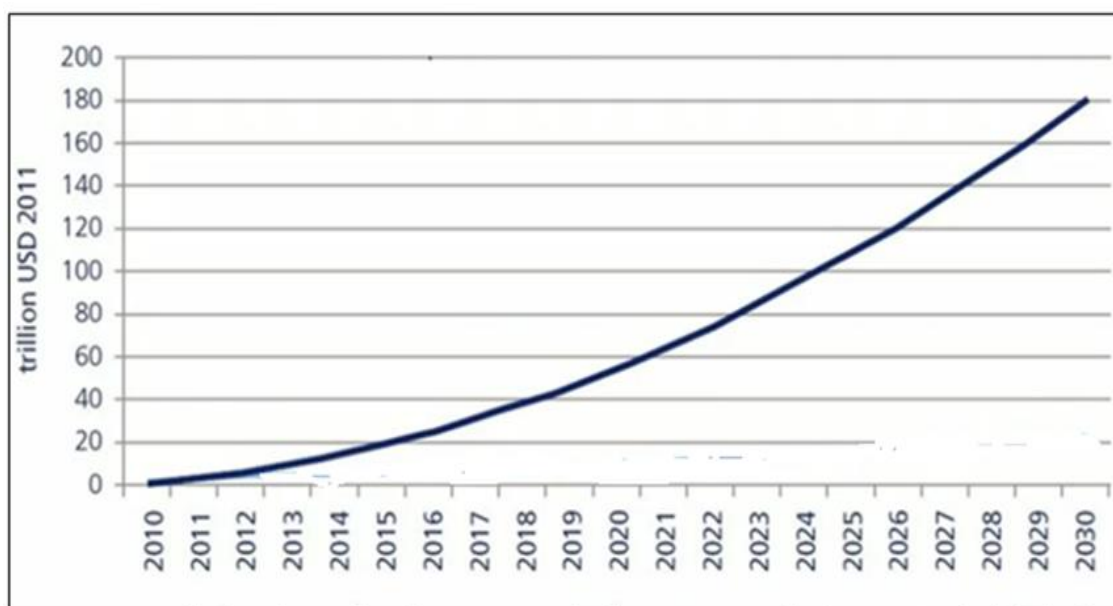


Рис. 1.9. Прогноз мирового кумулятивного ущерба от кибератак [89]

В структурном отношении мотивы совершения киберпреступлений в мире характеризуются следующим образом:

- корыстные побуждения – 66 %;
- шпионаж и диверсия – 17 %;
- исследовательский интерес – 7 %;
- хулиганство и месть – по 5 %.

Характеристика масштабов преступного кибервоздействия в мире выражается так:

- каждый день порядка 1 млн человек становятся жертвами киберпреступников;
- ежегодно жертвами киберпреступлений становятся 431 млн человек.

Можно привести следующее распределение фишинговых атак среди 10-ТОП стран:

- США – 37,3 %;
- Россия – 11,6 %;
- Китай – 10,3 %;
- Германия – 5,6 %;
- Румыния – 5,1 %;
- Франция – 3,3 %;
- Корея – 3,3 %;
- Канада – 1,9 %;
- Великобритания – 1,9 %;
- Италия – 1,6 %.

Обратимся к отечественному состоянию и динамике киберпреступности. Статистика ГИАЦ МВД России говорит о том, что в течение последних 10 лет показатели киберпреступлений увеличились более чем 150 раз [317].

В общем числе зарегистрированных противоправных деяний доля IT-преступлений увеличилась с 33 % в 2023 г. до почти 40 % в 2024. При этом четыре преступления из пяти совершались с использованием интернета, почти половина – с привлечением средств мобильной связи, около двух третей – кражи или мошенничества [281].

В 2024 г. зарегистрировано 765,4 тыс. киберпреступлений (рост по сравнению с 2023 г. на 13,1 %) [448]. Роскомнадзор отмечает 70-ти процентное увеличение количества DDos-атак на объекты критической информационной инфраструктуры (КИИ) России, производимых из-за рубежа. Число фишинговых атак возросло более чем в пять раз [281]. Существенно обострилась проблема дистанционных мошенничеств, совершенных против граждан посредством методов социальной инженерии.

Естественной реакцией на эти негативные изменения современной криминогенной обстановки стала активизации правоохранительной деятельности. Так, по данным Роскомнадзора, с помощью системы «Антифрод» только в 2023 г. заблокировано почти 2 млрд звонков мошенников с подменных номеров [204].

Кроме того, с 25 июля 2024 г. российские банки проверяют все денежные транзакции физических лиц и приостанавливают подозрительные переводы на два дня, а также в течение 30 календарных дней возмещают клиенту сумму, переведённую без его согласия на счета злоумышленников, находящиеся в базе Центрального банка.

Регулятор указал шесть признаков мошеннических операций, которые должны принимать во внимание банки для предотвращения

таких переводов. С 22 октября крупные банки, кредитные организации, значимые на рынке платёжных услуг, должны вносить реквизиты мошенников из базы данных Банка России в свои системы противодействия подозрительным операциям в течение двух часов, а с 1 января 2025 г. – в течение одного часа. Для остальных банков установлен срок в три часа.

Далее, МВД России подготовило законопроект, а Госдума приняла закон об уголовной ответственности для дропперов – подставных лиц, занимающихся выводом и обналичиванием похищенных средств. В указанном проекте нормативного документа предлагается передачу зарегистрированных на себя электронных средств платежа или доступа к ним определять как преступление средней степени тяжести, если же оно совершено в составе организованной группы – квалифицировать как тяжкое.

Правоохранительные органы усиливают комплекс мероприятий по сокращению утечки персональных данных и попадания их к мошенникам. Данный канал обусловлен многочисленными нарушениями при обработке и хранении указанной информации.

Цель отмеченных мероприятий – исключить избыточный сбор персональных данных и организовать технологии надежного их уничтожения после необходимых информационных операций. Важным здесь представляется наращивание профилактической деятельности среди населения, повышение цифровой грамотности граждан и, конечно же, максимальное раскрытие ИТ-преступлений правоохранительными структурами [281].

В МВД России обращалось внимание на то, что среди киберпреступлений в 2024 г. на 7,8 % увеличилась доля тяжких и особо тяжких составов. Это, в свою очередь, отразилось в прошлом году и на росте общего числа тяжких и особо тяжких преступлений на 4,8 %.

По данным Сбербанка, в 2024 г. электронные мошенники похитили у россиян около 300 млрд руб. В 2025 г. на фоне мер Правительства по борьбе с хакерами прогнозируется снижение этого показателя.

При этом нужно отметить, что в арсенале мошенников все большее место продолжают занимать технологические новинки в процессе подготовке и совершения киберпреступлений. Так, И. Бокова, Д. Галова, Н. Котикова [86], исследуя кибербезопасность в России в 2024 г., в своем обзоре выделили атаки с помощью ИИ и манипуляций эмоциями как занимающие первое место среди киберпреступлений.

Говоря об атаках на российские компании, центр мониторинга *RED Security SOC* отмечает их рост в прошедшем году в 2,5 раза, при этом мошенники применяют генеративный искусственный интеллект для создания поддельных сайтов, писем и видеозвонки. Опасен преступный тренд года, связанный с атаками на человека: аферисты, манипулируя эмоциями, массово заставляли жертв переводить деньги на так называемые «безопасные счета».

Рост кибератак во многом связан с доступностью интеллектуальных программных инструментов, а также с массовым стремлением киберпреступников использовать технологии машинного обучения. По сути, это относится к области генеративного ИИ (порядка 40 % фишинговых сообщений по электронной почте генерируется именно им, а уровень создаваемых при этом «иллюзий» таков, что стало реальным, например, «пообщаться» с двойником Путина [101]).

На основе генеративного ИИ осуществляются различные противоправные процедуры. Наибольшее распространение получили: имитация «контактов» с высокопоставленными или должностными лицами, контентов фишинговых веб-сайтов, страниц ведущих организаций (соцсетей, банков, фейковых магазинов известных брендов, где предлагаются неожиданные акции или значительные скидки на товары).

Кроме расширения онлайн-мошенничества, продолжаются атаки заражения устройств пользователей вредоносным программным обеспечением (например, трояны с функциями удаленного доступа или банковского функционала, приложения для изменения голоса или интеллектуальной поддержки), с последующим шантажом. Все больший размах приобретает традиционное телефонное мошенничество, но с доработками использования ИИ (в основном, на базе нейронных сетей генерация поддельных аудио- и видеоматериалов в масштабе «реального времени»). Они позволяют нарушать эмоциональный баланс потенциальных жертв и притуплять бдительность (например, инсценированные сообщения от начальников; представителей силовых структур; неожиданных катастроф родственников; образования задолженностей; возможностей выиграть; оказания социальных или дорогих услуг со значительными скидками и т. д.).

Коллегия МВД России в 2025 г. отразила озабоченность Президента Российской Федерации В. В. Путина и Министра внутренних дел В. А. Колокольцева, связанную с ростом кибермошенничества. Ими отмечены «недопустимые размеры ущерба» для населения страны от данных преступных деяний, а сам факт их стремительного роста сравнен с уровнем угрозы национальной безопасности [359].

Следует подчеркнуть усиление реагирования на создавшееся положение. В частности, оно выражается в принятии федерального закона, регламентирующего создание государственной информационной системы противодействия правонарушениям, совершаемым с использованием ИКТ [8].

При создании киберзащиты индивидуальных пользователей требуется применять интеллектуальные технологические решения, которые позволяли бы реализовывать следующий функционал:

- профилактическое, превентивное воздействие на злоумышленника, заставляющее оценить факт наличия специального противодействия ему, грозящее ему с высокой вероятностью наказанием, и возможно отказаться от преступного деяния;

– создание технологической интеллектуальной помощи пользователю в его персональных гаджетах. Она должна выражаться в снижении вероятности начального ошеломляющего психологического воздействия, эмоционального негативного фона, затормаживающего механизмы критического оценивания ситуации.

На эти неадекватные психологические реакции как раз и рассчитывают кибермошенники, дестабилизируя нормальное состояние жертвы. Далее на этой, благоприятной для злоумышленника основе, организуется и осуществляется в том или ином виде формате преступное получение с атакуемого лица денежных средств.

Исходя из сказанного, покажем пути активного применения технологий ИИ для решения правоохранительными органами задач обеспечения кибербезопасности.

1. Правовое обеспечение.

Выше уже сказано о недавнем федеральном законе [8], регламентирующем противодействие современным видам киберпреступлений, распространяющимся в стране.

Для «проигрывания» типовых ситуаций совершения преступлений, относимых к кибернетическим, весьма перспективно использование имитационного моделирования. Интеллектуальный анализ полученных модельных статистик в сопоставлении их с реальными данными о киберпреступлениях позволяет обосновывать линии поведения пользователей в типичных ситуациях и на этой обоснованной модельной базе формировать эффективные рекомендации по противодействию отмеченным видам преступных деяний.

Рассмотрим более детально возможности, содержащиеся в обозначенном нормативном правовом документе [8]. Их реальное применение предполагается на основе государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, содержащей следующий функционал:

- технологические средства «Госуслуг» дают пользователю возможность установки самозапрета на дистанционное оформление сим-карт, исключив данную опцию со стороны злоумышленников;
- для российских пользователей через операторов услуг связи можно установить самозапрет на международные звонки, на спам и массовые обзвоны, СМС-рассылки;
- в обязательном порядке вводится маркировка при приеме звонков (вызовов) – пользователю предоставляется информация о вызывающей организации;
- автоматизирована процедура исключения сообщений пользователю от «Госуслуг» (в том числе, кода подтверждения) в период проведения телефонного разговора;
- при получении микрозаймов пользователи смогут использовать биометрию;

– в случае отказа пользователя от эксплуатации номера телефона, последний будет автоматически удаляться из личного кабинета «Госуслуг» и связанных с ним банковских приложений;

– в организационно-нормативном и технологическом плане вводится запрет госорганам, банкам, операторам связи и цифровым платформам использовать зарубежные мессенджеры для общения с клиентами. Аналогичный запрет распространяется и на владельцев агрегаторов товаров и услуг, сайтов и сервисов, которые ежедневно посещают более полумиллиона пользователей;

– автоматический контроль алгоритмов проведения операций в банкоматах для прекращения общения с текущим пользователем в случае детектирования подозрительных действий;

– в обязанности банков вводится обязательство проводить мероприятия по антифроду как на онлайн-платежи, так и на банкоматы;

– банки обязаны проверять факты наличия признаков выдачи денег в банкомате без согласия клиента. В этом случае на 48 часов ограничивается выдача наличных.

Специалисты в области кибербезопасности напоминают, что, наряду с новыми решениями, необходимо продолжать применять уже наработанный и эффективный опыт. Так, следует исключить обращение к файлам из сомнительных источников, подозрительным ссылкам; эксплуатировать только приложения и платформы с регулярным официальным обновлением; сделать обязательными процедуры защиты информации на основе уникальных паролей с включением, как минимум, двухфакторной аутентификации, использования на всех устройствах надежных антивирусных решений.

2. Эмоциональная поддержка жертв кибернападения.

Противоправные деяния в сфере киберпреступности связаны с эмоциональной дестабилизацией жертвы кибернападения, запуском механизма ее эмоционального поражения. Эффективность атаки базируется на доведении дестабилизирующей информации до лиц, подвергшихся эмоциональному воздействию. Это могут быть испуг, страх, полная прострация, мотивы внезапного обогащения и т. д.

В любом случае эмоциональный стресс приводит к технологической, правовой, экономической, организационной неясности. Но при этом у подверженной атаки присутствует значимая наказуемая ответственность наступления нежелательных последствий (личных, родственных, общественных и иных).

Задача инструментария ИИ – не допустить путем специального воздействия «длительного» нахождения потенциальной жертвы в условиях такого стресса. Смысл временного фактора состоит в том, чтобы атакуемый человек не успел «запустить» вредные для него психологические механизмы и не дать развиваться соответствующей мотивации для выработки неадекватных эмоциональных реакций на происходящее воздействие, которое, чаще всего, выражается как легенда

«оригинальных» обстоятельств, последовательно излагаемых кибермошенниками.

В этих целях многими крупными финансовыми организациями (например, банки СБЕР, ВТБ, Тиньков Мобайл) создаются программные интеллектуальные продукты под условным наименованием «защитники», обладающие либо простым интерфейсом для управления различными категориями пользователей, либо выполняющие многие опции защитного уровня в автоматическом режиме. Кроме активного распознавания процедуры спуфинга, которая фактически является кибератакой на конкретного пользователя телефонной сотовой сети или иного гаджета, задача технологий ИИ в подобных ситуациях не должна ограничиваться на данной фазе.

Важным функционалом следует считать разработку инструментария, позволяющего обеспечить также разведывательные мероприятия по фиксации цифровых следов проводимого воздействия. Это должно стать источником криминалистически значимой информации, отслеживать признаки «серийности» кибератак, осуществления деанонимизации исполнителей (определения их истинных характеристик с возможностью выявления статуса подозреваемого в совершении преступления).

3. Противодействие новым угрозам.

Развитие данного направления, активно прогрессирующего в последнее время, связано с интеллектуальным поиском уязвимостей программных продуктов. Эта противоправная задача незапланирована, исходя из начального назначения соответствующих приложений, стала в своих решениях инструментом интеллектуальной поддержки потенциальных преступных замыслов. На основании найденных недостатков преступниками фактически проводится подобие научного исследования или моделирования вероятных сценариев их неправомерного использования.

Другими словами, речь идет об исследовании способов совершения преступлений, замысел которых базируется на выявленных программных недоработках, системных или алгоритмических недостатках. К сожалению, различные формы и разновидности недостатков, технологических или организационных недоработок обнаруживаются не только сотрудниками правоохранительных органов, но участниками преступных сообществ.

Высказанные соображения приводят к выводу, что аналогичные процедуры необходимо активизировать и специализированным структурам в правоохранительных органах, ответственных за организацию кибербезопасности и противодействие киберпреступности. Результаты такой аналитической оценки должны лечь в основу формирования рекомендаций по профилактике новых киберугроз как для организаций, так и индивидуальных пользователей, наиболее часто подвергающихся

ся кибермошенничеству и поэтому являющихся для правоохранительных органов категориями, требующими приоритетной киберзащиты.

Таким образом, в разделе изложены основные факторы становления и развития понятий в области кибербезопасности. Приведенная категорийно-понятийная платформа служит основой для трактовки киберпреступности, ее современных особенностей, текущего состояния и проявившихся тенденций эволюции, которые во многом определяют пути эффективного противодействия данному противоправному явлению со стороны ОВД, в том числе – при активном применении технологий ИИ.

1.3. Искусственный интеллект – новые возможности и новые проблемы

В данном разделе сделаем попытку оценивания принципиального противоречия современности. Оно говорит о взаимосвязи прогрессивного развития ИИ и возникающих при этом проблемах.

Вначале постараемся выразить совокупность того *позитивного*, что ожидается *от внедрения ИИ* в различные области человеческой деятельности. В следующих научных источниках [56; 77; 87; 100; 102; 151; 154; 159; 161; 195; 198; 205; 207; 235; 272; 421; 433; 440; 445; 452; 469–470; 473–474; 477; 485; 494–495] в различных ракурсах отражается существо данных позитивных воззрений на воплощение достижений ИИ.

Тенденция роста использования ИИ указывает на стремление крупных компаний развивать данное направление.

В исследованиях *IDC Worldwide Artificial Intelligence Spending Guide* отмечено, что в 2021 г. рынок ИИ в мире составлял \$85,3 млрд. К 2025 г. ожидалось его развитие до \$204 млрд с ежегодным ростом на 24,5 %. Другую сторону отмеченной тенденции подчеркивает рост количества научных работ, связанных с ИИ. Так, в 2022 г. *AI Index Report* сообщил, что с 2010 г. по 2021 г. количество публикаций удвоилось и составило 334,5 тысяч.

В целом в мире в последние два года стали переломными в развитии ИИ. Ведущий тренд – это создание мультимодальных моделей, способных эффективно работать с различными типами данных и решать сложные задачи в интересах человека.

Укажем на текущее наличие некоторого снижения частных инвестиций в ИИ. Однако, с другой стороны, отмечается небывалый рост финансирования генеративного ИИ. В 2023 г. по сравнению с предыдущим годом оно увеличилось почти в 8 раз и достигло \$25,2 млрд. Это стало реальным путем привлечения крупных инвесторов под влиянием ключевых игроков рынка – *OpenAI, Anthropic, Hugging Face, Inflection*.

Ведущее место в области создания передовых моделей ИИ заняли США (61 значимая модель). Следующие места за Европейским Союзом (21), Китаем (15).

Появление мощных мультимодальных моделей нового поколения считается ключевым достижением. Среди них заметны системы, демонстрирующие высокую гибкость в обработке текста, изображений и звука: *GPT-4* от *OpenAI* и *Gemini Ultra* от *Google*. Их затраты на обучение моделей – \$78 млн на *GPT-4* и \$191 млн на *Gemini Ultra*.

Отличается ощутимым прорывом робототехника – бурно развивающаяся отрасль ИИ – на основе внедрения языковых моделей. Сегодня роботизированные системы приобрели способность задавать вопросы и понимать ответы на них, существенно улучшив взаимодействие с реальным миром.

Отмечается повышение производительности труда и качественного улучшения его показателей при использовании систем ИИ. При этом происходит сокращение разрыва в квалификации между работниками с разным уровнем подготовки. Так, в отчете Стэнфордского университета указывается, что, благодаря решениям на базе систем ИИ, в 42 % организаций происходит снижение общих затрат, а в 59 % фиксируется рост их доходов.

Аналогичное улучшение наблюдается и в корпоративном секторе, где 55 % организаций применяют ИИ хотя бы в одной бизнес-программе. В отчетах компаний *Fortune 500* указывается на рост в 48 % применения ИИ в последние годы.

Доминирование индустрии ИИ заметно в сфере разработок. Так, 2023 г. отмечен созданием 51 модели машинного обучения на промышленных предприятиях, тогда, как академические институты представили их только 15. Гармонично развивается сотрудничество бизнеса и науки – 21 совместная модель.

Нечто похожее происходит и в области сотрудничества науки и медицины. В этом плане заметны прорывные приложения 2023 г.: от оптимизации сортировки – *AlphaDev*, до поиска новых материалов – *GNoME*.

При этом в медицине отмечен устойчивый рост внедрения технологий ИИ. Так, с 2012 г. количество медицинских устройств на базе ИИ, одобренных *FDA* (*Food and Drug Administration*) Министерства здравоохранения и социальных служб США, выросло в 45 раз.

Уделяется особое внимание интеграции систем ИИ в образовательный процесс. Ведутся исследования по изучению влияния таких инструментов в высшем и школьном образовании. Ведущие позиции здесь у США и Канады, однако, в Европе пока наблюдается существенный отрыв в применении ИИ на всех образовательных уровнях.

Серьезное внимание к внедрению технологий ИИ стали проявлять политики и управленцы. Здесь наблюдается существенный рост

в сфере нормативно-правового регулирования всех сторон рассматриваемой технологической отрасли.

Так, число актов регулирования в США в 2023 г. достигло 25 (с ростом в последний год на 56 %). Стоит отметить, что в 2016 г. был принят лишь один регулирующий акт.

Дав представление о мировых тенденциях, изложим сведения по тематическим направлениям, которые представляются авторам монографии наиболее соответствующими ее предметной области и задачам исследования.

Прежде всего, это стратегическое планирование; общее регулирование и государственное управление; разработка и использование моделей генеративного искусственного интеллекта; область защиты данных, в частности персональных; беспилотный транспорт; здравоохранение; этика в сфере ИИ.

На фоне общих тенденций в числе основных *достижений нового поколения ИИ* обратить внимание на следующие важные направления:

- усовершенствованные *глубокое обучение (deep learning)* и *нейронные сети (neural networks)* служат для создания высокоэффективных моделей, оперирующих в области больших данных. Это улучшает их способность в распознавании изображений, понимании смысла речи и анализа текстов, что в результате повышает сложность выполняемых задач, невозможную ранее;

- в сфере *обработки естественного языка (NLP – Natural Language Processing)* появились новые модели, которые могут понимать и генерировать человеческую речь, выявляя ее контекст и смысл, в частности, для оценки настроения, прогнозирования рисков, улучшения обслуживания клиентов. Одной из сфер *NLP*, получивших перспективное развитие, является применение больших языковых моделей (*LLM – Large Language Model*). Они ориентированы на крупные задачи. Например, это могут быть финансовые отчеты, анализ рынка, автоматизация взаимодействия со службой поддержки клиентов;

- развитие *робототехники и автономных систем*, которые оснащаются технологическими решениями ИИ и становятся способными решать очень сложные задачи в производстве, логистике (дроны для доставки товаров) и даже медицине (роботы-хирурги, помогающие проводить операции с минимальными рисками). В арсенале таких роботов возможности по адаптации к изменяющимся условиям и выполнению действий с высокой точностью;

- *интеллектуальные системы принятия решений* в реальном времени используют анализ больших данных для обоснования допустимых и эффективных решений. Подобные системы могут обеспечивать выявление лучших трендов, способны составлять наилучшие прогнозы событий, оптимизировать процессы в целях повышения производственной и социальной эффективности, снижения затрат. Поэтому они распространяются и становятся все более полезными

в бизнесе, финансах, медицине, где скорость принятия решений играет ключевую роль.

Укажем на некоторые особенности потенциала ИИ:

- обеспечение повышенного уровня *персонализированных услуг* в различных сферах. Например, детализация до любого необходимого уровня индивидуального плана лечения пациента на основе предварительного анализа медицинских данных; формирование адаптивных учебных программ под потребности и способности конкретного ученика; разработка целевых рекламных кампаний, исходя из предпочтений и поведения пользователей;

- формирование и развитие системы *умных городов (smart cities) и их инфраструктуры*, базирующихся на применении технологий ИИ, которые обеспечивают комфортную городскую среду – оптимальное управление трафиком, энергопотреблением и коммунальными услугами, а также играющую все *большую* роль кибербезопасность;

- углубление *научных исследований и инноваций* в направлении внедрения достижений ИИ, например, в области биотехнологий (изучение генетических данных для создания новых методов лечения), в физике и астрономии (обработка больших данных с телескопов и ускорителей элементарных частиц). Другой стороной может послужить *сравнение естественного и искусственного интеллекта* на новом уровне понимания этой проблемы. При очевидном их сущностном различии имеются аргументы и *значительного сходства*, которые во многом определяют пути дальнейших разработок;

- совершенствование процессов *обучения*. Человеческий разум постоянно адаптируется в окружающей среде на основе наблюдения, опыта, социального взаимодействия. В системах ИИ ведется анализ больших данных, выявляются требуемые закономерности в целях улучшения выполняемых алгоритмов и принятия соответствующих решений при обучении;

- обоснование *управленческих решений*. Процесс жизнедеятельности человека требует постоянной выработки разнообразных и сложных решений. Главные его задачи при этом – обработка информации, учет опыта, текущих обстоятельств, генерации допустимых вариантов решений и их оптимальный выбор. Аналогична отмеченному алгоритму и деятельность систем ИИ;

- *обработка и анализ данных*. Данный срез также характерен и для человеческого мозга, и для технологий ИИ, сочетая при этом форматы аналогового и цифрового анализа и извлечения информации;

- *адаптивность и самосовершенствование*. Новые знания и опыт являются основаниями для человеческого мозга в постоянной адаптации (*нейропластичности*) и самосовершенствовании. В результате люди учатся на своих ошибках, развивают новые навыки, адаптируются к изменению внутренних и внешних условий существования. Машинные аналоги также способны адаптироваться, самосовершен-

ствоваться через процесс постоянного обучения, улучшая со временем свои функциональные способности и точность выполнения задач;

– *возможности решения сложных задач.* Среди принципиальных аспектов естественного интеллекта человека выделяют совокупность когнитивных способностей, творческого мышления, интуиции, совместно призванных решать сложные проблемы и находить инновационные решения. Достигая похожих результатов, современные системы ИИ применяют иные подходы: в основном, математический анализ данных и алгоритмическое мышление.

Подчеркнем роль технологий ИИ в России. Она регламентируется Национальной стратегией развития искусственного интеллекта до 2030 г. с изменениями, внесенными Указом Президента РФ от 15.02.2024 № 124 [12].

Для обеспечения мероприятий Стратегии принята «дорожная карта» в рамках высокотехнологичного направления «Искусственный интеллект». В число ключевых участников данного федерального проекта входят Правительство РФ, ПАО Сбербанк, Российский фонд прямых инвестиций (РФПИ) и Консорциум НТИ по ИИ.

В дополнение к этому сформирована общественная организация – Альянс искусственного интеллекта. Ее основными участниками являются «Яндекс», VK, СБЕР, «Газпром нефть», «Самолет», «Уралхим», «Сибур», «Северсталь». Всего же Альянс объединяет более 800 российских компаний. Этот федеральный проект действует с 2021 г., будучи обеспеченным бюджетным финансированием – около 25 млрд рублей и внебюджетным финансированием – более 5 млрд руб.

Приведем некоторые результаты работы проекта в 2024 г.:

– 306 проектов (в 2023 г. – 99) получили гранты на прохождение акселерации; грантовая поддержка на разработку, развитие и коммерциализацию ИИ-решений представлена 491 проекту (2023 г. – 88); гранты на внедрение ИИ-решений получил 21 проект (2023 г. – 16);

– гражданами России выражено мнение о необходимости продолжения государственного развития ИИ, 68 % опрошенных проявили заинтересованность в совершенствовании таких технологий, удовлетворены условиями этой деятельности в стране;

– всего в сфере ИИ создано 12 специализированных исследовательских центров. В течение 2023 г. отобрано 6 исследовательских центров второй «волны» в 4 отраслях (здравоохранение, строительство, промышленность и транспорт);

– в области подготовки специалистов по линии ИИ лидирующими вузами выпущено 17 615 человек (2023 г. – 5 951), дополнительное профессиональное образование в сфере ИИ получили 3 832 человека (2023 г. – 2 134);

– во всероссийской олимпиаде по ИИ с привлечением компаний Альянса приняли участие 29 513 школьников (2023 г. – 15 906).

В России в настоящее время реализуются следующие направления в области ИИ:

- компьютерное зрение;
- обработка естественного языка;
- распознавание и синтез речи;
- интеллектуальные системы поддержки принятия решений;
- перспективные методы ИИ.

Решения российских компаний конкурентоспособны на мировом рынке. Это, например, *GigaChat MAX* от Сбера, четвертое поколение *YandexGPT*, заметными оказались нейронные модели крупных игроков – Тинькофф Банка, МТС и VK.

Очень интересно направление по созданию полноценной экосистемы развития ИИ в России. Она включает как технологических лидеров, так и региональные центры компетенций. Это позволяет эффективно использовать потенциал ИИ для решения задач в интересах каждого человека и общества в целом.

Целевое стремление российского сегмента – достижение лидерских позиций, как в разработке, так и в масштабе применения ИИ. В этом ключе особенно важно расширение международного сотрудничества (страны БРИКС, ШОС, другие партнеры, заинтересованные в совместном развитии ИИ-технологий).

Следует отметить, что Россия вышла в число мировых лидеров в сфере государственных услуг с применением ИИ – охват более 130 млн пользователей. Доступно около 200 видов электронных госуслуг, что существенно повышает эффективность взаимодействия государства и граждан.

Примером прорывных технологий ИИ в России является применение генеративного ИИ в государственном управлении. Так, языковая модель *GigaChat* использовалась для обработки обращений граждан на прямую линию общения с Президентом РФ. Это позволило проанализировать миллионы сообщений в кратчайшие сроки и повысило эффективность работы госорганов в десятки раз.

Другой пример относится к транспортной отрасли – осуществляется федеральный проект «Беспилотные логистические коридоры». В его реализации проводится тестирование автономных тягачей на маршруте Москва–Санкт-Петербург.

В промышленности внедряются системы 3D-моделирования с использованием ИИ для проектирования деталей оборудования. При этом особый прогресс отмечается при создании цифровых двойников сложных промышленных систем.

В трендах 2025 г., относящихся к развитию ИИ в России, находятся следующие:

- значительное развитие в рамках принятой государственной стратегии и федеральных проектов указанной технологии для экономики и общества;

– для исполнения федерального проекта «Искусственный интеллект» на год выделено 7,7 млрд рублей;

– существенный акцент на разработку «сильного» ИИ (новые архитектуры и алгоритмы машинного обучения, а также взаимодействия человека и ИИ);

– среди ведущих направлений обозначены государственное управление (повышение эффективности работы аппарата Правительства); персонализированное медицинское обеспечение и телемедицина; исследования Арктики и космоса; другие технологии.

Наряду с ожидаемыми позитивными эффектами, рассмотрим *противоречия, проблемные вопросы, негативные аспекты*, которые существуют и потенциально возможны при внедрении технологий ИИ в жизнедеятельность человека.

Глобальные проблемы использования технологий ИИ.

Приведем мнение Илона Маска, высказанное им в начале 2025 г. [173; 190] и связанное с оценкой развития ИИ, как достижение технологического тупика. Причем с его точки зрения данное состояние достигнуто еще в прошлом году.

Создавшееся положение обусловлено тем, что современные модели ИИ, например, *ChatGPT*, для эффективной работы должны быть обеспечены гигантскими объемами данных. Их источники разнообразны и многоплановы: книги, научные и иные статьи, переписка и дискуссии в социальных сетях и т. д. В 2024 году потребность в терабайтах составляла: академические тексты – 200; веб-контент – 2 500; литература и архивы – 1 000. А сегодня рост потребностей моделей, которые выражаются экспоненциально, привел к реальной недостаточности новых качественных данных о характеристиках человеческой цивилизации.

Выход из получившейся ситуации часто находится исследователями в обращении к так называемым *синтетическим данным*. Но указанное решение пока не дает возможности оценить качество и возможные последствия, что тревожит разработчиков теории и практики внедрения ИИ.

По своему замыслу синтетические данные представляют искусственно созданную информацию для имитации реальных данных. Подход, конечно, имеет ряд *преимуществ*: снижается стоимость обучения моделей ИИ; повышается доступность данных, обеспечивается их адаптивность к решаемым задачам; достигается нужный уровень конфиденциальности; из-за отсутствия персональной информации значительно снижается острота этических проблем.

Но при этом имеются и *недостатки*. Один из них выражается в том, что из-за несовершенства или недостаточной объективности данных модель может привести к ошибочным результатам или даже системному сбою, именуемому крахом модели. Это может сформировать *предвзятость по отношению к исходным данным* (например, из-

вестен факт, что в 2016 г. ИИ, призванный предсказывать рецидивы преступлений, проявил расизм [501]) или *потерю творческого потенциала*, когда модель теряет способность генерировать оригинальные либо нетривиальные, но перспективные решения.

Кроме мыслей, выраженных в интервью Илоном Маском, одним из ведущих мировых специалистов в области технологий ИИ, приведем соображения и других исследователей данной проблематики.

Интересны исследования *американского ученого* К. Келли [198]. Им сделана попытка проанализировать текущее состояние развития цивилизации, выявить факторы и условия, которые на перспективу около 30 ближайших лет будут определять влияние технологий ИИ на человеческое бытие, формировать контуры не только прогресса, но и регресса, связанных с ИИ.

В указанной работе им выделены 12 тенденций, которые, по мнению автора, сумеют изменить жизнь человеческого общества, его обучение и общение. Среди таких тенденций, например, переход к повсеместному *отражению* происходящих процессов *на экранах*, которые будут расположены практически на любых поверхностях; доведение технологии интеллектуального *отслеживания* в интересах безопасности и решения иных функциональных задач, начавшегося в мире уже в значительных масштабах, до уровня тотального наблюдения; снижение *конфиденциальности* процессов.

Все обозначенные тенденции внедрения технологий ИИ, совместно воздействующих на функционирование и существование общества, приведут человечество к созданию системы, которая соединит всех людей и компьютеры в *глобальную матрицу*.

Свою точку зрения о глобальных угрозах от внедрения технологий ИИ представил *шведский философ* Н. Бостром [96]. Проводимый им историко-аналитический взгляд на ситуацию дает основания для аргументированного восприятия возможной катастрофы человеческой цивилизации.

Суть рассуждений автора сводится к следующему. Исторический опыт указывает на устойчивую тенденцию, что победа в человеческих конфликтах, войнах всегда была на той стороне, которая умнее. Текущее состояние свидетельствует о том, что самыми умными представителями фауны являются именно люди.

Но факт появления конкуренции в данной сфере говорит о возможности развития компьютерных алгоритмов, которые в конечном итоге могут стать более умными на основе взрывного роста ИИ. В итоге в мире Земли может «родиться» сверхразумный вид существа, представленный искусственными машинами.

Логическим продолжением данного сценария может стать ситуация, когда сообщество искусственных автоматов захочет стать доминирующим. Такое решение будет иметь два принципиально различных итога: сделать человечество счастливым или банально уничто-

жить его ради решения какой-то глобальной задачи (например, остановить антропогенное загрязнение мирового океана). В любом случае, по мнению автора, люди будут не в состоянии сопротивляться этой логике.

А ведь возможность того, что на Земле появятся технологические решения ИИ, которые будут гораздо умнее людей, описана не только Илоном Маском и учеными типа Н. Бострома. Это кажущееся полужантасстическим опасение не беспочвенно, вынуждая всерьез задуматься о настоящих и будущих взаимоотношениях людей и ИИ.

В силу этого вполне актуально стремление прогрессивно мыслящих законодателей уже сейчас обосновывать и вводить нормативно-правовое регулирование применения ИИ. В частности, в общем виде оно представлено и сосредоточено в глобальном атласе регулирования ИИ последних редакций [133–135].

Мониторинг развития правовых систем мира уже открывает интересные правовые представления о понимании негативных сторон, возможного ущерба, отложенных последствий, прогноза развития ситуаций при воздействии ИИ. При этом подчеркивается необходимость выхода на международный уровень регулирования, объединения правовых и иных усилий, подготовки отдельных государств и сообществ к возникновению подобных катаклизмов, их предотвращению.

Таким образом, был приведен ознакомительный обзор мнений по глобальному уровню проблем развертывания технологий ИИ. Кроме этого, с другими точками зрения в рамках рассматриваемого контекста можно ознакомиться, например, в работах [75; 125; 145; 156; 230; 232; 301; 403; 431–432; 447; 451; 456; 482; 487]. Далее перейдем к уровню частных представлений о данной группе противоречий.

Частные проблемы применения технологий ИИ.

Совокупность многих частных проблем применения ИИ сегодня уже обозначена в обзорах нормативно-правового регулирования [133–135]. Другие продолжают быть под особым вниманием в связи с их развитием, более четким описанием возникновения проблемных ситуаций в связи с внедрением технологий ИИ. Из всего многообразия частных проблем в дальнейшем изложении сосредоточимся на проблемах применения ИИ, *связанных с кибербезопасностью и киберпреступностью.*

В ряду рассматриваемой проблематики отметим вирусные и иные вредоносные программы, сложные формы кибератак (их автоматизацию, использование ИИ для исследования уязвимостей систем защиты), подмена законных пользователей (спуфинг), массовый взлом паролей одновременно и многое другое.

В работе Д. Е. Намиота, Е. А. Ильюшина, И. В. Чижова [479] внимание исследователей посвящено обеспечению кибербезопасности на основе применения технологии машинного обучения и невозможности описания происходящих при этом процессов какой-то одной,

универсальной моделью противостояния существующим и развивающимся вариантам атак и вторжений. Для преодоления «проклятия многомерности» изыскания авторов нацелены на создание адекватной классификации моделей машинного обучения в приложении к кибербезопасности.

Специалистами российской компании *Esapro* [185] указывается основная функциональная цель применения технологий ИИ в решении задач кибербезопасности, состоящая в возможности усиления защитных мероприятий на основе инструментов быстрого выявления киберугроз и автоматического реагирования на них.

Применение алгоритмов машинного обучения обеспечивает оперативный анализ огромных объемов данных в процессе выявления угроз и определения аномалий, в совокупности указывающих на кибератаку. Практики при этом выделяют ряд ключевых моментов противодействия: обнаружение угроз на фоне необычных паттернов сетевого трафика или атипичных действий злоумышленников; автоматизация рутинных процессов; прогнозирование развития атак.

Тактика применения технологий ИИ в решении указанных задач состоит в повышении скорости обнаружения угроз; применении новых вариантов защиты; совершенствовании обработки данных; снижении времени реакции на инциденты.

Однако нельзя не отметить и значимые *недостатки применения ИИ* в решении задач противодействия в отмеченной сфере:

- достижениями технологий ИИ пользуются и злоумышленники, повышая убедительность фишинговых атак, привлекая поисковые возможности алгоритмов ИИ для выявления новых уязвимостей в сетевых системах и последующего их злонамеренного использования;
- возможность нарушения конфиденциальности данных и этических норм при проведении мониторинговых мероприятий и аналитической разведки поведения пользователей;
- возрастание риска зависимости от технологических алгоритмов ИИ и снижения человеческого общения, взаимного контроля;
- недостаточность обеспечения указанных задач квалифицированными кадрами.

Приведем более развернутую систематизацию и характеристику *рисков кибербезопасности*, связанных с масштабным *внедрением ИИ* [318]:

- *дипфейки (DeepFake)* являются результатом интеллектуального синтеза изображения, видео, аудио или текста. Так, технологии ИИ дают возможность создать очень реалистичное видео с участием конкретного человека, где он говорит то, что никогда не говорил или совершает действия, которые никогда не совершал.

Первоначально подобные результаты были только развлекательным контентом. Но сейчас дипфейки, как правило, используются для мошенничества и других противоправных действий.

Дипфейки на основе внедрения в них правонарушителями достижений современных, широкодоступных технологических решений стали способны обходить простые системы лицевой и голосовой биометрической аутентификации. В целом такая ситуация негативно влияет на киберустойчивость;

- *продвинутые виртуальные ассистенты* на основе технологий обработки естественного языка и глубоких нейросетей все более понимают смысл запросов пользователей, ведут диалог, формируют прогноз и оказывают помощь в принятии решений. Но они же вполне могут стать инструментом атаки на человека или информационную систему;

- *управление цифровым следом*. Увеличение времени, проводимого человеком в киберпространстве, способствует оставлению в нем все больших объемов информации о себе, своих действиях и предпочтениях. Данная особенность обеспечивает огромные возможности для злоупотребления сведениями со стороны злоумышленников, получивших несанкционированный доступ к ним;

- *цифровые двойники (Digital Twins)* – это виртуальный аналог реального объекта или специализированная компьютерная модель. Уровень ее интеллектуальной поддержки таков, что в ключевых характеристиках она полностью дублирует исходный объект и способна воспроизводить его состояния в разных условиях.

В частности, персональный цифровой двойник человека может быть его незаменимым ассистентом в цифровом пространстве. Важной особенностью такой модели является имитация эмоций, поведения, паттерна действий и принятия решений.

Собираемый в сети цифровой след оригинала в итоге может обеспечить его практическую неотличимость от цифровых взаимодействий двойника с внешним миром. Прогноз появления рассматриваемого уровня модели: 5–10 лет.

Серьезные опасения вызывает возможность наделения цифрового двойника определенными правовыми атрибутами. В этом случае возникнет необходимость создания инструментов выявления подделки, обеспечения контроля аутентичности и прав представительства цифрового двойника;

- *эмоциональный ИИ (Affective Computing)* относится к технологическим решениям, направленным на распознавание, обработку, интерпретацию и симуляцию человеческих эмоций, базирующихся на данных от различных устройств (сенсоров, камер, микрофонов и т. д.). Данная технология дает возможность проведения атаки с использованием социальной инженерии. Определив характеристики эмоционального состояния жертвы, злоумышленник упрощает выбор наиболее эффективной стратегии осуществления атаки;

- *однонаправленный нейрокомпьютерный интерфейс (One-way BCI)* предназначен для обмена информацией между мозгом и компьютером. Внешние устройства данного интерфейса работают в одном

направлении: принимают сигнал от мозга или наоборот посылают его в мозг. Современные достижения в создании нейроинтерфейсов позволяют передавать команды компьютерам и другим электронным устройствам. В этом случае риск в области кибербезопасности связан с возможностью взлома нейроинтерфейса в целях слежки или перехвата команд управления.

Данные реальные оценки приводят и к гипотетическим пока вариантам:

- прежде всего, речь идет о возможностях появления «умного» вредоносного ПО с параметрами самообучения. Изначально оно сможет взаимодействовать с компьютерами и человеком (в частности, за счет понимания и генерации естественного языка). Наличие этих функций определит способности проведения сложных многоступенчатых *APT*-атак (*Advanced Persistent Threat*) на базе методов социальной инженерии. Потенциал подобного ПО – самообучение новым техникам атаки и обходу средств защиты. Его реализация практически сделает невозможным организовать противодействие традиционными методами;

- *двунаправленный нейрокомпьютерный интерфейс (Two-way BCI)*. По аналогии с рассмотренным интерфейсом можно отметить двухстороннюю направленность передачи информации. Применительно к кибербезопасности становится возможным создание абсолютно новых классов угроз. Например, кибератаки этого уровня могут быть направлены на изменение человеческого восприятия и удаленный контроль произвольными и непроизвольными функциями организма. Потенциально это может быть создание «цифровых галлюцинаций», провоцирование различных психических расстройств, управление мыслями и поведением жертвы;

- *психиатрия ИИ (AI Psychiatry)*. Рост сложности решаемых задач, передача их от человека ИИ объективно требует от интеллектуальных систем развития навыков самообучения, самостоятельности в принятии решений. К сожалению, и у этих систем уже есть случаи «цифровых расстройств», вызванных, скорее всего, несовершенством обучающих данных.

Так, в 2016 г. компания *Microsoft* завела в *Twitter* чат-бот, способный отвечать на твиты. Не прошло и суток, как данный эксперимент пришлось прекратить, поскольку более 60 % твитов стали оскорбительными для феминисток. Поэтому вполне возможно, что на определенном уровне самостоятельности систем ИИ, у них начнут возникать расстройства, весьма схожие с расстройствами психики у людей. Это приведет к необходимости их выявления и применения нетрадиционных мер защиты со стороны технологий ИИ.

В завершение обзора некоторых видов киберугроз от внедрения ИИ отметим, что, по мнению А. Ю. Попова, основным риском можно считать *взрывной рост мошенничества*, направленного на частных

лиц, а также *рост результативности такого мошенничества* [318]. Сильные решения ИИ, собирая и анализируя все большее количества информации о жертве, доступной в цифровом формате, сумеют организовать эффективные методы атаки на человека, учитывая его индивидуальные особенности, биографические данные, медицинскую и иную информацию.

Совокупность описанных условий, в конечном итоге, может обеспечить негативную реализацию атак посредством социальной инженерии от текущих долей процента, до практически полного успеха. Естественно, что такое состояние проблемы создаст отрицательный общественный резонанс, недоверие, а, возможно, и противодействие внедрению технологий ИИ.

Вернемся к положениям, изложенным в описании блога российской компании *Esapro* [185]. Аналогичные в сути своей соображения высказаны и в публикации блога компании *Microsoft Security Copilot* [449]. Частные особенности рассуждений и предложений авторов можно отразить таким образом.

Использование ИИ для кибербезопасности считается состоявшимся с конца 1980-х г. и постоянно развивающимся. В ряду последних достижений выделяют так называемый, *генеративный ИИ* (например, генеративные модели искусственного разума *GPT-3 (a теперь уже и GPT-4)*, *DALL-E* и *Stable Diffusion*).

Их технологическая и функциональная особенность говорит об оригинальной способности создавать новый контент на основе структуры существующих данных. Совокупность данных базовых опций и уровень их аппаратно-программной реализации, фактически, позволяют для исследований информационных массивов не использовать какого-либо языка запросов. А, следовательно, определяются возможные в будущем пути создания как можно меньшего количества «цифровых следов» (как в деятельности специализированных структур организации противодействия противоправным деяниям, но и, к сожалению, могут быть взятыми на «вооружение» различными криминальными сообществами и организациями).

На данную технологию в настоящее время возлагают, прежде всего, большие надежды по организации более эффективного уровня безопасности на основе следующих новинок:

- использование в практических рекомендациях и идеях интерфейса синтеза данных, нацеленное на помощь в расследовании инцидентов;

- обеспечение помощи аналитикам в донесении до сотрудников организации реального понимания и оценки происходящих процессов на базе выработки и системного формирования отчетов и презентаций, удобных для чтения и логического восприятия;

- дополнительное иллюстрирование указанных пояснений ответами на естественном языке или в графической форме.

Отмеченная возможность встраивания генеративного ИИ в продукты и решения безопасности требует более ответственного подхода к его созданию. Именно на поддержании точности и правдивости функционирования современных моделей генеративного ИИ видится путь преодоления отмеченных видов киберугроз.

Типичными направлениями использования ИИ в обеспечении кибербезопасности, выделяемыми авторами блога, являются: управление идентификацией и доступом (*IAM*, в том числе на основе использования автоматической принудительной двухфакторной аутентификации, о которой авторы монографии изложили сведения в работе [84]); безопасность и управление конечными точками; безопасность облака; обнаружение киберугроз (расширенное обнаружение и реагирование – *XDR*, решения для управления событиями – *SIEM*, о чем авторы монографии говорили в работе [397]; защита информации; расследование инцидентов и реагирование на них.

В плане наиболее важной функции – обнаружение и предотвращение киберугроз – алгоритмы машинного обучения используются для нескольких распространенных способов:

- для совершенствования поисковых возможностей и обучения систем защиты хорошо зарекомендовали себя модели обучения с учителем в разметке и классифицировании данных, которые становятся типовым массивом;
- выявление закономерностей в данных, не помеченных ранее, осуществляет технология обучения без учителя, что дает возможность замечать аномальные действия;
- формирование шаблонов пользовательского трафика и выявление с помощью этого неожиданных или подозрительных действий основывается на специализированном анализе поведения пользователей и объектов системы;
- создание системной аналитической базы об угрозах базируется на технологии, когда системы ИИ используют обработку естественного языка для анализа неструктурированных источников данных, таких как социальные сети.

Определенный срез статистических данных о мировых и отечественных трендах и востребованности ИИ в вопросах кибербезопасности представлен в работе А. И. Фокиной, Ю. В. Туровец [430]. Так, по оценкам мирового уровня в 2023 г. зафиксировано, согласно данным *InfoWatch*, 11 549 утечек данных со средним объемом на каждую около 4 млн записей персональных данных.

Их рост (+61,6 % к 2022 г.) обусловлен, в том числе, распространением технологий ИИ (это касается генеративных моделей, дипфейков, ботов, усложнения техник социальной инженерии и т. д.). Интересным при этом являются оценки о внедрении инструментов ИИ и автоматизации.

Они на основе перспективных методов машинного обучения помогают предотвращать атаки злоумышленников. Основным получаемый параметр говорит о времени реагирования на инциденты кибербезопасности, который количественно зафиксирован со снижением с 2, 3 дней до 58 минут.

Таким образом, приведенные соображения составляют общее и многие аспекты частных представлений о новых возможностях и новых проблемах продолжающегося распространения технологий ИИ в деятельности человеческого общества. Более подробно ознакомится с особенностями частных взглядов на приводимую проблематику, отмечаемых другими авторами и во многом перекликающимися с изложенными материалами, можно, например, в следующих работах [51; 61; 86; 110; 140; 184; 189; 318; 379; 486].

Ко всему сказанному добавим одно соображение из работы Д. Соловьева [379], по нашему мнению, довольно успешно обобщающее основные тенденции представляемого раздела. С одной стороны системы безопасности, применяющие новеллы ИИ, позволяют довольно успешно обнаруживать аномалии и угрозы, обрабатывать большие данные, оптимизировать рутинные процессы, а также, что, наверное, самое главное, формировать превентивные меры и понижать вероятность рисков человеческих ошибок в области кибербезопасности.

Но обратной стороной указанных достижения являются возможности, активно реализуемые правонарушителями и преступниками, по значительному совершенствованию вредоносных программных средств и негативного манипулирования самими системами ИИ. Такой формат технологий ИИ уязвим к предвзятости (так, в 2015 г. ПО для маркировки изображений классифицировало чернокожих людей как горилл [501]), обладает потенциалом для создания рисков в сфере обеспечения конфиденциальности информации и в итоге приводит к отсутствию необходимого человеческого контроля в социальной сфере и кибербезопасности.

Среди всего социального (нормативного, организационного и прочего) следует особо подчеркнуть, что и положительные и негативные аспекты бурного становления новых технологий ИИ могут, к сожалению, выступать своеобразной объективной платформой, даже не представляемой на текущий момент по своим параметрам и характеристикам. Но реальный технологический уровень таких достижений может стать физической и логической базой для возникновения, а также определенного совершенствования новых *граней киберпреступности*.

Об этой частной, но, по нашему мнению, очень важной стороне рассматриваемой предметной области проведем более обстоятельное изложение в главе 2.

1.4. Выводы по главе 1

1. В историческом плане XX век стал прорывным в создании и использовании долго ожидаемой человечеством технологии ИИ. В работе проанализированы разноплановые аспекты этой сферы, проникающей в самые разнообразные направления человеческого бытия: научно-теоретические, концептуальные, организационные, технологические, правовые и иные.

2. Технологии ИИ формируют как позитивные, так и негативные последствия. Истоки ее противоправных и преступных проявлений относятся к защите или безопасности информации. Именно эти аспекты сформировали понятия кибербезопасности, а ее нарушения – киберпреступности. Современные особенности последней, ее состояние и проявившиеся тренды определяют пути эффективного противодействия данному негативному, все усложняющемуся явлению со стороны ОВД, в том числе – в аспекте активного применения технологий ИИ.

3. Характерная траектория развития технологий ИИ состоит в значительной неопределенности дальнейших последствий, ожидаемых революционных изменений и прорывов, выражающихся в мало предсказуемых на текущий момент последствиях позитивного и негативного характера.

Глава 2. Задачи противодействия киберпреступности и технологии искусственного интеллекта

2.1. Основные направления применения искусственного интеллекта в решении задач правоохранительных органов

В разделе рассмотрим основные направления, где уже имеются или предполагаются применения ИИ для решения оперативно-служебных задач правоохранительных структур, в частности, ОВД.

В работе А. И. Фокиной и Ю. В. Туровца [430] проведен анализ экономической составляющей и востребованности ИИ для обеспечения задач кибербезопасности. Выводы работы отражены на двух диаграммах.

Первая (рис. 2.1) показывает долю тех структур, кто используют ИИ-решения в области кибербезопасности. Вторая (рис. 2.2) отражает долю тех организаций, кто планирует продолжать использовать ИИ-решения в области кибербезопасности



Рис. 2.1. Доля организаций, использующих ИИ-решения в области кибербезопасности [430]

Отмеченные тренды подчеркивают эффективность мероприятий по использованию ИИ-решений по противодействию кибербезопасности. Кроме того, они обосновывают перспективность подобного варианта ресурсных вложений.

Рассмотрим экспертные оценки текущего состояния «Интернета вещей». Темпы его современного развития – от 10 млрд соответствующих устройств (2018 г.) до 64 млрд (2025 г.). Предполагается доведение с помощью систем сотовой связи 5G количества устройств на квадратный километр до 1 млн (сейчас это показатель – 60 тыс.).

Совершенно очевидно, что резкое изменение показанных коли-

чественных показателей, наряду с достижением нового уровня цифровой поддержки населения, приведет и к другому уровню возможных преступлений.

В частности, ожидается значительное увеличение киберфизических атак, расширение уязвимости сетевых пользователей, организаций, стран. Вполне возможен сценарий развертывания событий в виде формирования:

- киберпандемий (хакерство, кибертерроризм, кибервмешательство в частную жизнь);
- киберконфронтации;
- кибервойн и киберапокалипсиса.

Развитие технологий ИИ оценивается и другими негативными проявлениями:

- использование криптовалюты для отмывания денег;
- катастрофические угрозы от внедрения квантовых вычислений (вплоть до создания новых видов разрушительного оружия для террористических и мафиозных целей);
- квантовые криптографические методы криптографии (не исключается, что они будут использоваться для создания новых способов противоправного преодоления киберзащиты).

Нового уровня достигнут и технологии «заметания» преступных цифровых следов.

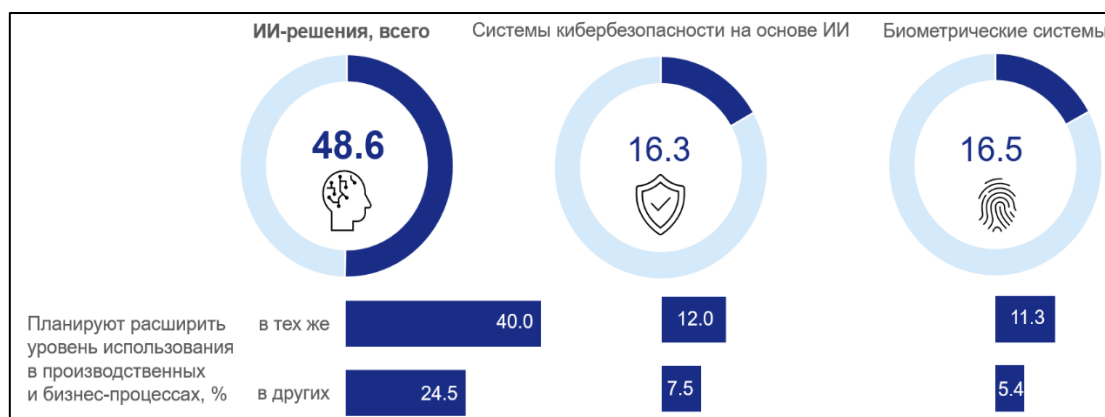


Рис. 2.2. Доля организаций, планирующих продолжать использовать ИИ-решения в области кибербезопасности [430]

Разумеется, приведенные факты и суждения определяют актуальность разработки все более совершенных методов обеспечения кибербезопасности на основе использования передовых методов ИИ и внедрения их в широкую практическую сферу [70].

Цифровое представление всех видов жизнедеятельности общества, его стремительное увеличение до невообразимых объемов, сверхэффективные методы и средства добывания, хранения, передачи информации, гармоничного объединения разноплановых пластов че-

ловеческой жизнедеятельности (культуры, нравственности, психологии поведения, творчества и т. д.) практически ввели в обиход выполнение новых типов решений обработки и анализа на основе ИИ, в том числе – по вопросам обеспечения кибербезопасности человека, общества, государства.

Все это в полной мере относится и к бурно развивающимся технологиям:

- *предиктивной аналитики* (прогнозирование развития ситуаций, выявления закономерностей, рисков и возможностей);
- *скоринга* (аналитическое оценивание различных характеристик и поведенческих признаков при принятии человеком тех или иных решений).

Обозначенные положения при исследовании рассматриваемой предметной области находятся в поле зрения современных ученых и практиков, включая авторов монографии [69–71; 78–79; 84; 91–93; 106; 160; 177; 211; 236; 241–242; 244–245; 247; 249–252; 254; 261–262; 285; 290; 299; 306; 314; 346–347; 353; 374; 397; 404]. Их выводы состоят в безусловной необходимости расширения применения ИИ в правоохранительной деятельности, противодействии киберпреступности, а также отражают четкое убеждение в важности реализации решений на базе ИИ.

В рамках оценки состояния и перспектив использования технологий ИИ в задачах противодействия преступности следует подчеркнуть, что классическими путями развития являются как эволюционные, так и революционные процессы. На текущий момент преимущество имеют *эволюционные* векторы.

Исходя из данной точки зрения, обратим внимание на работы, в которых рассматривалось системное представление о применении ИИ правоохранительными структурами [72; 138; 149; 174; 181; 183; 284; 286–288; 311; 349–351].

В этой связи обратимся к работе И. А. Завьялова [166], где изложены результаты исследования мирового опыта использования ИИ и робототехники в раскрытии преступлений. Автор выделяет такие страны, как Великобритания, Германия, Израиль, Канада, Китай, Россия, Сингапур, США (более половины всех разработок мира), Франция, Швейцария, Южная Корея, Япония.

Как уже указывалось выше, относительно *сильного* ИИ, потенциально обладающего способностью заменить человека, пока что ведутся оценки его возможностей. То есть, фактически, еще нет четкого понимания перспектив его применения для решения оперативно-служебных задач раскрытия и расследования преступлений, создания стройной системы превентивной профилактики, обеспечения основных категорий пользователей и всего населения эффективными методическими рекомендациями и интеллектуальными программными

решениями автоматического противодействия типовым подходам организации и исполнения правонарушений в данной сфере.

Уровень же *слабого* ИИ представляет основную предметную область для проведения изысканий в рассматриваемой сфере. Получаемые при этом решения по затратным, организационным, логически обоснованным, технологическим и иным параметрам считаются вполне подходящими для различных сторон правоохранительной деятельности. Они перспективны для противодействия преступности при установлении логических, причинно-следственных, слеодообразующих связей, представляющих в итоге обоснование версий оперативного интереса, сбора ориентирующей, доказательственной, криминалистически значимой информации, а также формирования информационно-аналитической базы для обеспечения и организации различных направлений профилактической деятельности.

Выделяются основные направления использования возможностей ИИ в указанных приложениях:

- качественное совершенствование типовых операций сбора, хранения и обработки информации;
- выявление информационных связей оперативного интереса на основе аналитических и прогнозных моделей;
- обеспечение раскрытия, расследования, профилактики киберпреступлений посредством мониторинга цифровых следов, выявления «слабостей» ПО, определяющих потенциальные угрозы;
- поддержка сетевых коммуникаций и обеспечение взаимодействия с законопослушными гражданами в целях быстрого получения информации оперативного интереса.

Дадим краткую характеристику отмеченным направлениям применения ИИ.

1. Интеллектуальная поддержка типовых информационных операций.

Традиционным арсеналом полиции практически во всех странах мира являются типовые автоматизированные учеты: оперативно-розыскные, криминалистические и многие иные. Идея реализации *централизованных операционных* центров общественной безопасности с применением интеллектуальной обработки информации принадлежит США. Первый такой центр безопасности под патронажем полиции был открыт в 2007 г. в Нью-Йорке [164].

Информация о лицах (фотографии, голосовые данные, сведения с камер видеонаблюдения, патрульных машин, звонков в полицию, заявлений граждан, полицейских отчетов различной направленности, протоколов арестов и т. д.) поступает в центр в неструктурированном виде, где преобразуется по специальным алгоритмам в универсальный формат, упорядочивается и доводится инициаторам запросов. В результате внедрения данной технологии ИИ сразу на десятки процентов повысилась эффективность работы полиции.

Следует отметить, что аналогичный функционал реализован и в деятельности полиции России в Государственной информационной системе «Безопасный город» [91]. В ней, в частности, осуществляется работа комплекса биометрической идентификации (рис. 2.3) с использованием технологий ИИ.

В рамках информационно-аналитической системы обеспечения деятельности (ИСОД МВД России) продолжается тенденция объединения всех информационных учетов. Установочная, регистрационная, структурированная и неструктурированная информация об объектах оперативной заинтересованности подвергается соединению в общем центре аналитической обработки, что, в конечном итоге нацелено на создание нового класса интеграции поисковых сервисов – *метапоисковой системы* [83–84; 158; 215].

Подобная интеграция осуществляется в рамках проводимого в МВД России развития современных технологий идентификации личности с использованием биометрических данных.

В итоге планируется создание национальной системы биометрической идентификации личности (НС БИЛ) с двумя основных сегментами – правоохранительным и гражданским. Гражданский сегмент уже реализован в виде Единой биометрической системы персональных данных (ЕБС). Завершением правоохранительного сегмента будет Федеральная информационная система биометрических учетов (ФИС БУ).

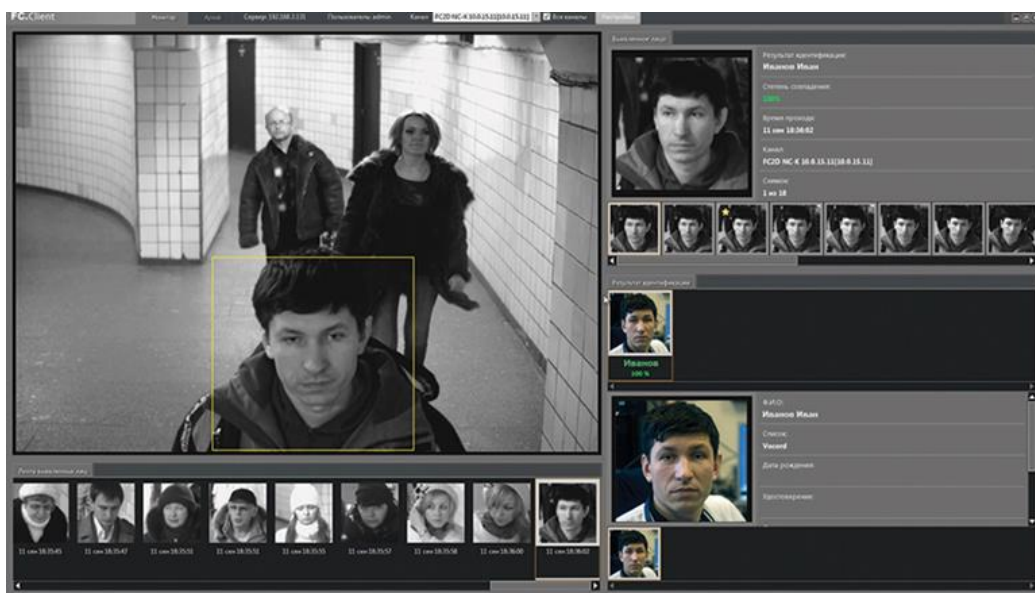


Рис. 2.3. Пример работы системы «Безопасный город» по лицу человека [124]

Данный сегмент будет осуществлять поиск по изображению лица, с учетом накопленных массивов фотографий граждан. В нем планируется объединить под единым аппаратно-программным управлением с привлечением технологий ИИ восемь видов учета:

– дактилоскопический модуль (ЦИАДИС-МВД России – централизованная интегрированная автоматизированная дактилоскопическая информационная система);

- системы распознавания голоса и изображений лиц;
- учет татуировок и их фрагментов;
- учет характеристик радужной оболочки глаза;
- система геномного учета («Ксенон-2»);
- учет поведенческих признаков и рисунка вен.

Создание единого центра и его внедрение в работу ОВД позволит значительно ускорить поиск лиц, причастных к подготовке и совершению преступлений, правонарушений и пропавших без вести, а также оптимизировать сбор, хранение и обработку биометрических данных граждан. Еще раз подчеркнем, что ведущей технологией в этой и в большинстве других современных правоохранительных систем автоматизированного учета и анализа данных является ИИ. Его применение в указанных информационных системах правоохранительных органов России обосновано необходимостью анализа больших данных, социальных сетей и других ресурсов, содержащих персональные данные.

Аналогичные функциональные возможности используются и в других системах. Например, поддержка интеллектуальным обеспечением применяется в решении *задач экспертно-криминалистической деятельности*.

Так, системы биометрического контроля доступа, учета, поиска и идентификации по лицам «Полифейс» и «Визирь» могут обрабатывать видеофайлы или сканировать лица пассажиров, персонала, сравнивая их с фотографиями клиентов, лиц, владеющих пропуском, разыскиваемых преступников или лиц, объявленных в розыск, из различных баз данных. К этому можно добавить возможности поиска по фотографиям в интернет-приложении сервиса «Фотопоиск» [114].

Некоторое представление о современном уровне в области использования интеллектуальных алгоритмов распознавания образов, а, конкретно – электронных изображений лиц в разных форматах – могут дать сведения, изложенные в работах А. А. Волкова [115; 218].

В сжатом виде можно отметить, что авторы провели актуально требуемое сравнительное исследование основных алгоритмов детекторов лиц на уровне традиционных (*Haar Cascades*, *HOG+SVM*, *Face Recognition*), так и перспективных нейросетевых решений (*MTCNN*, *RetinaFace*, *YOLOv11 Face*, *MediaPipe*, *SCRFD*). Особое внимание уделено использованию и разработке подходов интеллектуального имитационного моделирования: процессу нормализации, включая выравнивание по ключевым точкам и использование генеративно-состязательных сетей (*GAN*) для улучшения качества изображения. Показано влияние точности детектирования и нормализации на итоговую точность распознавания. Приведены результаты сравнительного

анализа различных алгоритмов на основе метрик *Precision*, *Recall* и *F1-score*, а также оценки их эффективности.

На рис. 2.4 приведен пример работы алгоритмов по восстановлению изображения лица программой *CodeFormer*.



Рис. 2.4. Пример работы алгоритма восстановления изображения лица программой *CodeFormer* [115]

Отметим возможности по восстановлению фотографических изображений специализированной нейросетью *Upscales.ai* [114], а также работу нейросетей *Kandinsky 2.2* и «Нейро-холст». Они позволяют по словесному описанию создать портрет человека.

Подобные технологии могут применяться для составления «первоначального» субъективного портрета. Этот объект, как показала практическая апробация, в последующем эффективно дорабатывается для получения большего сходства с разыскиваемым лицом, создавая реальные условия для проведения эффективных оперативно-поисковых мероприятий, что отмечается, например, в работе [172].

В целом применение технологий ИИ расширяет возможности поиска проверяемых лиц. В частности, широко используются действенные практические приемы: интегрировать фото- и видеоматериалы с учетами, объединять биометрические данные со сведениями из других систем, пополнять базы данных изображениями, фиксируемыми на потоковом видео с камер наблюдения, а также из видеофайлов, загруженных вручную.

Приведенная технология считается перспективной для производства судебной портретной экспертизы. В этих целях внедряется в экспертно-криминалистические подразделения страны специализированное программное обеспечение (СПО) «Фоторобот Сетка» [53].

Принцип сеточных функций основан на создании трехмерной модели лица с использованием нейронных сетей. Модель довольно точно определяет пространственное положение головы и узловые точки лица, на основе которых методом триангуляции строится сетка. Она позволяет изменять положение узловых точек для плавного (без разрывов) преобразование изображения. Задание новых значений углов обзора приводит к получению изображений другого ракурса. На рис. 2.5 поясняются возможности подобной нейронной сети.

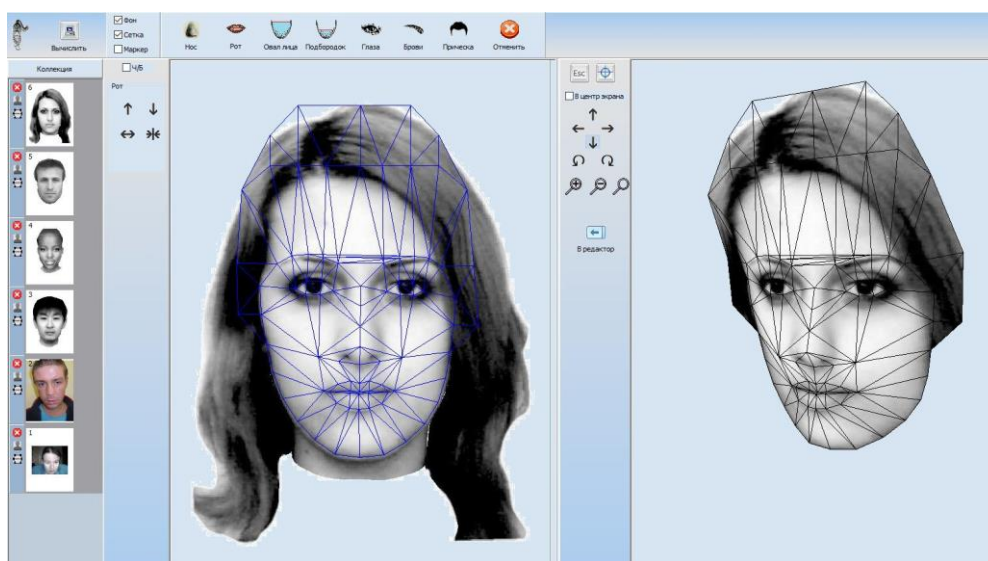


Рис. 2.5. Ракурсное преобразование изображения лица на базе СПО «Фоторобот Сетка» [53]

Покажем возможности применения технологий ИИ для обработки отпечатка пальца, приведенной на рис. 2.6 [491].

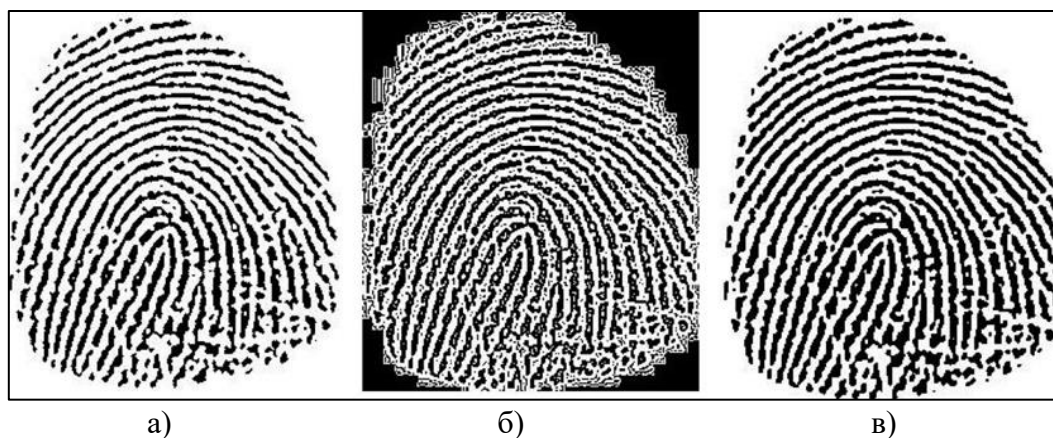


Рис. 2.6. Изображение отпечатка пальца, бинаризованное с помощью: ручной пороговой обработки (а), алгоритмов Niblack (б) и Otsu (в) [491]

Это пример из множества исследований, направленных на обеспечение интеллектуальной поддержкой экспертно-криминалистической деятельности. Они нашли активное развитие и являются, как и многое из выше представленного, самостоятельным направлением противодействия киберпреступности.

Приведем краткие сведения о СПО «Папилон-Нейро» [114]. Работа данной автоматизированной дактилоскопической системы (АДИС) осуществляется следующим образом.

АДИС формирует рекомендательные списки, которые далее становятся предметом рассмотрения СПО. Интеллектуальный алгоритм начинает процедуры выявления сходства объектов.

Особенностью является то, что сравниваются не математические модели отпечатков (дактилоскопические формулы), а *оригиналы дактилоскопических изображений*. При этом интеллектуальные поисковые алгоритмы, обученные на реальных дактилоскопических массивах, используют признаки папиллярных узоров (*минуции*): толщину, плотность, форму, изгибы папиллярных линий и т. д.

Нейросеть на основе индивидуальных признаков каждого отпечатка позволяет просматривать рекомендательные списки на любую заданную глубину. Объект-запрос сравнивается с найденными АДИС отпечатками и по результатам сравнения генерируется индекс совпадения – нейроиндекс.

Разработчики СПО «Папилон-Нейро» отмечают, что работа с модифицированными списками с нейроиндексами отличается от традиционной проверки по следующим характеристикам. На один искомый отпечаток в среднем приходится всего два несовпадающих (что характеризуется соотношением 1:2), а традиционная работа со списками идет в гораздо большем объеме – связана с просмотром до 100 несовпадающих отпечатков (соотношение – 1:100).

Нейросеть выполняет бóльшую часть работы эксперта по просмотру списков, но несравнимо быстрее.

Рассмотрим программный конструктор для судебно-почерковедческой экспертизы. Он создавался на основе технологий ИИ в качестве адаптивного инструмента, способного подстраиваться под текущую экспертную ситуацию и учитывать множество различных факторов.

Эффективность применения этой интеллектуальной системы, по мнению А. Н. Охлупиной, В. Ю. Федоровича, В. В. Устинова [304–305], основывается на ДСМ-методе автоматического порождения гипотез для проведения идентификационных и диагностических исследований рукописных записей, подписей. Интеллектуальная нейронная сеть, настроенная на офлайн-верификацию подписи, создана в Уральском государственном юридическом университете имени В. Ф. Яковлева.

Она позволяет дифференцировать две группы подписей – подлинные и выполненные с подражанием. При обучении использован метод сверточных искусственных нейронных сетей, когда сеть по интеллектуальным алгоритмам вырабатывает иерархическую систему существенных признаков [76].

Основной алгоритм работы системы состоит из следующих этапов:

- сканирование спорной подписи камерой смартфона;
- обрезка изображения для исключения лишних деталей;
- обработка изображения нейросетью для удаления лишних деталей;
- оценка нейросетью изображений подписей, определение вероятности выполнения их одним лицом;
- представление варианта решения нейросетью, оценка его экспертом и принятие им решения (рис. 2.7).

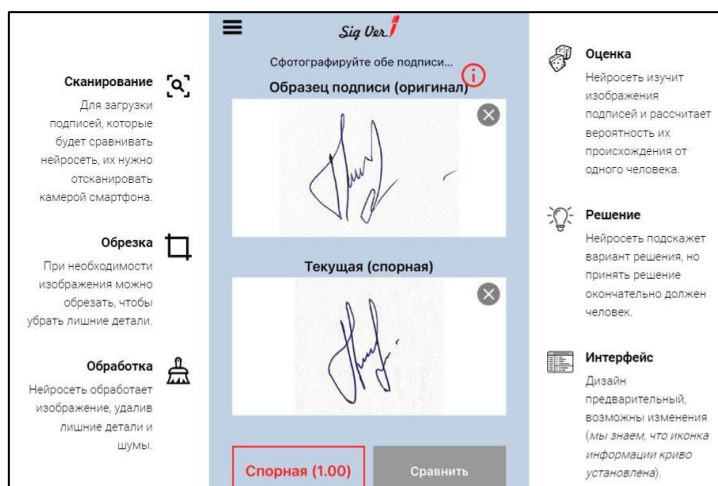


Рис. 2.7. Пример работы искусственной нейронной сети [114]

Распространение технологий ИИ привело к расширению их возможностей для решения многих задач судебных экспертиз. Например, для развития инструментальной одорологии, что позволит получить объективную информацию и создать физико-химические приборы, способные определять компоненты и представлять результаты в виде ольфактограммы [148].

2. Выявление информационных связей оперативного интереса на основе аналитических и прогнозных моделей.

Одной из первых моделей такого типа с использованием ИИ, является система *Blue CRUSH* (от англ. *Crime Reduction Utilizing Statistical History*) фирмы *IBM*.

Применение модели в Мемфисе, способствовало снижению уровня преступности на 30 %. Модель на основе аналитической обработки статистических данных о совершенных преступлениях, особен-

ностях местности и описании личности подозреваемого формировала прогнозные зоны возможного совершения преступлений и определяла предположительное время их совершения [210].

Основными шагами подобных интеллектуальных алгоритмов являются: поиск общих особенностей в неструктурированных объектах; распознавание лиц на базе анализа множества цифровых следов, получаемых доступными средствами; выделение оперативно значимых объектов из огромного объема неструктурированных данных.

Модель нашла применение в решении и других правоохранительных задач. Например, с помощью модели осуществлена оценка вероятности серийности совершаемых преступлений путем мониторинга контента из открытых источников – социальных сетей.

Методологическим аппаратом интеллектуальных процедур модели выступают математическая лингвистика и биометрия для идентификации, извлечения логических связей; статистическая оценка аффективных состояний и субъективной информации; методы исследования тональности при обработке текстов на естественном языке [160].

Системы, схожие с используемой в Мемфисе, внедрены во многих городах США. Так, в Лос-Анджелесе используется интеллектуальная технология *PredPol*, разработанная в Калифорнийском университете, которая после успешной апробации стала распространяться и за пределами страны.

Особенностью технологии ИИ, применяемой в полиции Чикаго, является оценка вероятности прогноза установочных данных как будущих убийц, так и их возможных жертв. Список, определенный по результатам работы модели, составил 1 тыс. 400 человек из общего числа 2,7 млн жителей города, по которым проведен анализ. Эффективность предсказаний модели определилась тем, что многие из указанного списка застрелены, а каждый 4-й стрелок значился в списке.

Важнейшим направлением рассматриваемой технологии в нескольких штатах стало ее использование для аналитической работы по профилактике и расследованию преступлений в режиме реального времени – система *RICAS (Real-time Intelligence Crime Analytics System)*. Результаты работы модели отображаются на карте с возможностью углубленного анализа криминогенной обстановки, групповой преступности, хода расследований преступлений.

Разработкой систем ИИ круга занимается компания *Palantir Technologies*. Для моделирования оперативной обстановки по линиям военных структур, спецслужб, включая правоохранительные органы она ориентирована на новые аналитические методы обработки разрозненных массивов данных.

Для решения соответствующих задач анализа оперативной обстановки системами, разработанными указанной компанией, отслеживались передвижения транспорта по номерным знакам, записи теле-

фонных соединений, потоки видеонаблюдения и т. д. Интеллектуальные модели обеспечивали выявление преступных сетей, готовивших террористические акты в различных странах мира, опасных преступных групп и даже обнаружение местоположения «террориста номер один» – Усамы бен Ладена [164].

Имеется опыт эксплуатации интеллектуальной системы предупреждения преступлений *DAS (Domain Awareness System)* в полиции Нью-Йорка. Модели подобного типа основываются на использовании систем технического зрения в режиме реального времени, наблюдениями за действиями подозреваемых, считывания номерных знаков транспортных средств в автоматическом режиме при мониторинге потоковой видеоинформации, выдачи изображений при включении режимов «следающих систем» за конкретными объектами оперативного интереса.

В этих целях в городе задействовано несколько тысяч видеокамер, специализированных датчиков и сенсоров. По принципу интеллектуальной поддержки в обработке реальной уличной информации ведется обслуживание оперативно-служебных задач правоохранительных органов.

Например, акустическая система детекторов выявления фактов выстрелов *ShotSpotter*, применяемая в десятках городов США, ориентирована на фиксацию и интеллектуальный анализ происшествия (определения места на карте города выстрелов из оружия, выдача результатов распознавания вида оружия, передача их в специальные приложения оповещения в полицейской связи). Другие приложения связаны с аналитическим обеспечением камер видеонаблюдения при выполнении охранных задач, распознаванием лиц и характерного поведения (в том числе – противоправного) в местах массового нахождения людей и в системах обнаружения оружия.

Нашли широкое распространение и другие прикладные решения интеллектуальной поддержки:

- распознавание лиц от корпорации *Amazon* в целях сканирования сетевых объявлений и теневого Интернета при поиске пропавших детей, выявления и ликвидации цепочек поставок детской порнографии и задержания похитителей детей, мониторинга по выявлению лиц, занимающихся похищением детей;

- известные разработки компании *BioLink* для автоматизированных систем идентификации личности по отпечаткам пальцев;

- автоматизированные многопрофильные системы биометрической идентификации (*AMBIS*, модульная переносная биометрическая система *MBU*);

- системы идентификации исследуемого огнестрельного оружия по штрих-коду;

- интеллектуальные системы мониторинга дорожного движения (программные комплексы *ANPR, RLVD, OSD, e-Challan*).

Можно отметить и другие примеры помощи полицейским на ба-

зе ИИ – интеллектуальные программы для автоматического распознавания, редактирования, фиксации речи в системах автоматизированной связи, автоматизации документооборота [160].

3. Интеллектуальное сопровождение задач обеспечения кибербезопасности, противодействия киберпреступлениям.

В области цифровых расследований одной из первых программных платформ использовалась интеллектуальная система *Nigel* от *Kimera Systems*. Ее основная особенность состоит в накоплении знаний и реакций в зависимости от контекстного оценивания материалов правоохранительной деятельности.

Другим примером выступает система *Mayhem*, созданная при соучастии компании *ForAllSecure* и Университета штата Пенсильвания. Ее функционалом является организация информационной защиты ПО на основании выявления в нем «слабых» мест.

Она используется для решения задач ФБР по распознаванию индивидуального «почерка» хакеров, выявления хакерских группировок, воздействий от хакерских атак. Алгоритмы системы в масштабе реального времени распознавали особенности вредоносного софта, обобщивали архитектуру возможных атак, которые недоступны для восприятия персоналом служб информационной безопасности.

4. Использование технологий ИИ для коммуникации и взаимодействия с гражданами, помогающих в привлечении последних в сборе информации оперативного интереса через социальные медиа (социальные сети, системы обмена мгновенными сообщениями или мессенджеры, сетевые форумы). Ведущее положение здесь занимает Китайская Народная Республика (КНР), где последовательно развивается система социального доверия и контроля за поведением граждан.

Наряду с очень значительными финансовыми вложениями в данный проект важной его характеристикой является и очень большой объем данных, который могут использовать правоохранительные органы из потока, генерируемого китайскими пользователями.

Прежде всего, это касается проекта *Police Cloud*, разворачиваемого с 2015 г. Архитектура проекта на уровне провинций страны базируется на создании облачных хранилищ полицейской информации. О значимости внедряемого подхода и ожиданий его эффективности говорит факт участия в разработке весьма значимых научно-практических организаций.

В их числе – первая национальная лаборатория, открытая в 2017 г., по разработке технологии «большого» ИИ, которая развернута в Китайском научно-техническом университете. Он известен лидирующей мировой ролью в создании очень перспективной технологии квантовой связи, в развитии «мозгоподобных» вычислений, развивающих представления об ИИ, и их приложений.

Интересными являются направления ее творческого взаимодействия. Данная лаборатория сотрудничает с такими знаменитыми

научными учреждениями, как Университет Фудань и Шэньянский институт автоматизации Академии наук Китая, а также с оператором крупнейшего в Китае сервиса Интернет-поиска – *Baidu*.

Глобальная система распознавания лиц компании *Cloud Walk* относится к известному примеру использования аналитических и прогнозных моделей ИИ. Она, в частности, базируется на 176 млн единиц видеокамер наблюдения (а перспективно планируется подключение еще 400 млн штук [84]).

Система тотально отслеживает самые разные стороны деятельности человека, в том числе – криминальной. Совокупность итоговых данных в системе включает оценку вероятности совершения правонарушений, соответствия деятельности установленным гражданским правилам и нормам и т. д.

Для представления возможностей данной системы можно привести пример с опытом эксперимента журналиста *BBC*. По его запросу поиск изображения персоны, включенной в список опасных лиц, при отслеживании ее передвижений в видеопотоках людей в Пекине занял 7 минут [84].

При этом система не является единственным аппаратно-программным комплексом тотального контроля под управлением технологий ИИ. Например, лица, часто путешествующие в другие страны, находятся под наблюдением системы от компании *UniView*.

В рамках излагаемого аспекта, наряду с передовым опытом КНР, отразим аналогичную деятельность в правоохранительных органах России. Наиболее показательно она представлена в информационно-аналитическом обеспечении работы ИСОД МВД России.

Подсистема поддержки взаимодействия с населением ИСОД предназначена для организации поступления оперативной информации, а также оказания услуг населению. Так, в целях решения указанной задачи к ИСОД подключены система централизованного учета оружия (СЦУО), единый банк данных архивной информации («Ретроспектива»), интегрированный банк данных (ИБД) [83].

Говоря о позитивном применении технологий ИИ, не стоит забывать и о развитии их негативных сторон, ориентируемых на осуществление противоправных деяний. Подчеркиваем данный тезис применительно к достижениям в сфере визуального распознавания личностей, как одной из ведущих технологий, используемых для обеспечения задач правоохранительных органов.

По этому поводу обратимся к аналитическому обзору коллектива ученых из Ростовского юридического института [188]. В своем исследовании авторы отмечают возможности технологий ИИ, которые, в первую очередь, способны повышать точность систем распознавания лиц с помощью обученных сверточных нейронных сетей *CNN* (*Convolutional Neural Networks*).

В то же время, рассматриваемые технологии ИИ обеспечивают,

к сожалению, и возможности фальсификации цифровых доказательств. В этих целях осуществляется обращение ко многим программным приложениям, способным подделывать фото-, видео-, аудио- контент, например, *DeepFake*-приложения и инструменты (*Doublicat, FaceApp, DeepFaceLab*), а также к технологии глубокой подделки *Zao* для платформ *Android, iOS*. Данное обстоятельство оказывает мотивирующее стремление киберпреступников к развитию методов обхода мер кибербезопасности.

Все это вызывает обоснованную тревогу по поводу возникновения и развития так называемой *синтетической социальной инженерии* со стороны средств массовой информации (СМИ). Ее основная цель – на базе дипфейков заставить жертву поверить в реальность доводимой информации, особенное влияние она имеет на тех, кто не знаком с особенностями современных технологий.

Для противодействия дипфейкам создаются аппаратно-программные комплексы, автоматически распознающие голосовые, фото- и видеообразы, синтезированные ИИ.

Например, это нейросеть *FakeCatcher*, одновременно снимающая показатели с 32 точек на лице и продемонстрировавшая в реальном времени точность распознавания дипфейков до 96 %. Ее принципиальное отличие от других систем – поиск параметров и признаков настоящего прообраза, а не отличий, выдающих обман.

Данный продукт имеет как свои достоинства, так и недостатки. Для деятельности же правоохранительных органов страны необходимо создание специализированного программного приложения.

Оно должно использовать технологии ИИ в своем функционале и ориентироваться на новые формы информационного обеспечения: содержать протоколы интеграции с биометрическими банками данных изображений, записей голоса и видеоматериалов, а также с сервисами ИСОД МВД России. Кроме того, данное приложение архитектурно должно быть представленным как распределенная мультиплатформенная вычислительная сеть.

Вновь обращаясь к опыту Китая, отметим, что, развивая единую информационную систему в стране, обеспечивающую и деятельность полиции, ее разработчики гармонично объединили многие профессиональные базы данных. Это системы видеонаблюдения с функционалом распознавания лиц по многим параметрам (в частности, по походке, начиная с первых успешных приложений, датируемых с 2018 г., с выделением в ходьбе человека до 24 параметров движения или даже по параметрам ступней человека), сотни мобильных приложений, интернет-ресурсы, платежные системы, базы социальных, дорожных и коммунальных служб.

На основе всей этой совокупности взаимосвязанных данных определяется социальный рейтинг каждого гражданина Китая. Учитываются три сферы жизни: государственная (налоги, счета, погашение кредитов и т. п.); общественная (соблюдение ПДД, норм рождае-

мости, честность в работе и успехи в образовании); поведение в сетевых ресурсах (культура общения, правовая чистота размещаемой информации, покупки в интернет-магазинах) [164].

Обратим внимание и на использование технологий ИИ другими странами, которые создают общее представление о спектре возможностей в сфере правоохранительной деятельности.

Так, японский опыт применения алгоритма раскрытия преступлений в городских условиях, реализованный компанией *Fujitsu Laboratories Ltd* совместно с Университетом электрокоммуникаций, базируется на использовании математического аппарата теории игр в описании технологии защиты и нападения.

Прогнозные модели ИИ разработчиков *Pre-Crime Observation System* по методологии схожи с описанными американскими подходами в обеспечении полицейской отчетности, принятой, например, в полиции Амстердама.

Следует подчеркнуть, что, наряду с положительным эффектом внедрения технологий ИИ в деятельность правоохранительных структур, имелись и негативные отзывы. Так, США стали первой страной, где запретили использование систем прогнозирования преступлений на основе ИИ (Санта-Крус, Калифорния, 2020 г.).

Аргументация властей Санта-Крус основывалась на том, что система шла «вразнос» в следующей практической ситуации. Находя особо криминогенный район, она привлекала туда дополнительные ресурсы полиции, поднимала, таким образом, в нем количество арестов. Как следствие, на данный район, становившийся еще более криминогенным со статистической точки зрения, обращалось еще большее внимание.

Поскольку в используемых моделях не учитывалась латентная преступность, которая при этом снижалась, формальная оценка состояния криминогенной обстановки по показателям регистрации преступлений становилась все хуже, что привело к отказу от продолжения пилотных проектов подобного плана в калифорнийских городах Маунтин-Вью и Пало-Альто. Как результат, «виноватым» оказался ИИ, а не непосредственные разработчики моделей, слабо разбиравшиеся в реальных процессах, имевших место в оцениваемом районе.

И в российских условиях заказчиков от правоохранительных подразделений не удовлетворяет непрозрачность в создании и эксплуатации профессионально ориентированных систем ИИ. У них из-за коммерческой защиты, сохранения авторских прав нет полного понимания и уверенности в том, кто разрабатывал эти системы, каковы недостатки используемых для обучения данных и с какими принципиальными проблемами может столкнуться заказчик [164]. Фактически использование созданных систем ИИ вписывается в кибернетическую идею применения «черного ящика», а именно, управляя только пара-

метрами входа и выхода технологии, выводы делаются без понимания структурных, а, следовательно, и функциональных составляющих.

Поэтому не редкость, когда возникают ложные срабатывания, формируется итоговая информации предвзятого характера, случайно образуются ошибки в исходном программном коде или нетиповые отклонения работы алгоритма модели ИИ.

К настоящему времени возникло своеобразное негативное явление – *AI bias* или «предвзятость искусственного интеллекта», встречающееся и при принятии ИИ-решений в правоохранительной сфере. В самом общем виде оно выражено в следующих положениях [67].

Технологии ИИ нередко принимают дискриминационные решения. Однако выявление причин указывает, что основная проблема данного феномена кроется в том, что ведущая роль в создании и использовании размеченных данных и их взаимосвязей отводится разработчикам ИИ. В результате в исходный материал непреднамеренно или преднамеренно попадают искаженные данные.

Таким образом, феномен *AI bias* следует считать результатом в определенном смысле недобросовестной деятельности разработчиков программно-аппаратных комплексов обучения ИИ. Истинные же причины связываются с *антропоморфизацией* – уподоблением ИИ человеку, наделением его человеческими качествами.

Поэтому в ведущих странах мира (США, Китай, Россия, государства Европейского Союза) ведется разработка и внедрение соответствующей законодательной базы, в рамках которой регламентируется формирование требуемых отношений в сфере ИИ, использование необходимых ресурсов, определение ответственности за негативные проявления со стороны интеллектуальных систем и противодействие им.

Изложенные сведения позволяют выделить основные направления и возможности использования технологий ИИ в раскрытии и расследовании преступлений, оперативно-розыскной и правоохранительной деятельности:

- интеграция в единую цифровую, интеллектуально поддерживаемую систему открытых и закрытых учетов всех видов;
- реализация мониторинга сетевых информационных ресурсов в целях выявления цифровых следов о совершенных преступлениях и разыскиваемых лицах. Этот функционал может быть выполнен на базе развития специализированных интеллектуальных систем поиска и анализа контента любого формата с привлечением средств и методов аутентификации и идентификации [84; 263];
- интеллектуальное обеспечение систем поддержки принятия управленческих и оперативно-розыскных решений, организация и планирование их реализации, усиление контроля за полицией со стороны общества;
- создание нового уровня аналитических систем общей, частной, профилактики преступлений и правонарушений;

- определение вариантов и форматов использования имеющихся систем ИИ для обеспечения целей оперативно-розыскной деятельности;
- обеспечение эффективной системы контроля, соблюдения конституционных прав и свобод человека, исключение утечки персональных и иных конфиденциальных данных, контроля процессов принятия решений, возложенных на системы ИИ.

В работе [164] о *перспективах развития полиции* при использовании технологий ИИ, отмечены те задачи, в решении которых начал реализовываться потенциал ИИ:

- противодействие киберпреступности в сфере криптовалюты и использования защитных возможностей технологии блокчейн;
- интеграция с глобальными навигационными системами для обеспечения правоохранительной деятельности;
- развитие нейронных сетей в области распознавания личностей, в том числе – при решении оперативно-поисковых задач;
- реализация розыскных и поисковых мероприятий (пропавшие, браконьеры, террористы, контрабандисты и иные правонарушители) на основе эксплуатации беспилотных воздушных средств;
- формирование нового класса интеллектуальных технологических решений, ориентированных на поддержку криминалистических исследований;
- аппаратно-программное обеспечение полиграфических процедур в интересах распространения ориентирующей информации.

2.2. Решения оперативно-тактических задач органов внутренних дел по борьбе с киберпреступностью

Приведем некоторые представления по ряду направлений правоохранительной деятельности, являющиеся довольно значимыми в общем объеме работы по расследованию и раскрытию киберпреступлений на основе применения технологий ИИ.

Цифровые следы Интернета – основа оперативно-розыскного поиска. Данное направление весьма широко представлено в различных источниках и результатах исследований. В них выражено довольно единодушное мнение, состоящее в интенсификации и углублении поддержки оперативно-розыскной работы за счет поиска и систематизации цифровых следов лиц и объектов оперативного интереса. Повышение эффективности этих процессов базируется на активном внедрении специализированных технологий ИИ.

Положения, изложенные А. Н. Поздняковым в статье [315], дают, по нашему мнению, тот срез решений, который составляет предметную область монографии. В статье делается попытка оценить состояние и перспективы задач оперативно-розыскной деятельности на основе ИИ при работе с Интернет-информацией в целях поиска ориентирующих и доказательственных сведений о преступлениях, соверша-

емых с использованием ИКТ. Прежде всего, автор выражается целесообразность создания в системе МВД России единой базы данных систематизированных сведений и результатов оперативно-розыскных мероприятий (ОРМ).

Речь идет о сведениях ОРМ, могущих помочь в организации противодействия преступлениям того или вида. В их числе определяются: круг лиц оперативного интереса; способы (почерк) совершения преступлений; виды и типы примененных программных продуктов и аппаратных средств; характеристика пострадавших физических или юридических лиц и т. д.

Типовым подходом российских пользователей интернета является работа в своем информационном поле или виртуальном пространстве – в доменной зоне. RU, которое находится под контролем правоохранительных органов. Но наличие определенных технологий открывает возможности перехода в информационные поля других государств. Аналогично осуществляются встречные информационные заходы и со стороны иностранных государств.

Возникновение такого рода информационных потоков сказывается на возникновении у правоохранительных органов страны и их оперативных подразделений проблем при раскрытии и расследовании преступлений, осуществленных с использованием ИКТ. Это встречается в случаях, когда, например, подозреваемым в мошенничестве является гражданин другого государства.

Рассматриваемые обстоятельства сформировали актуальность задачи разработки специализированных интеллектуальных программных продуктов в сфере противодействия киберпреступности. Их целевая направленность выражается в обеспечении надежной защиты от преступных действий со стороны граждан иностранных государств, а также российских криминальных сообществ, которые для совершения преступлений подобного рода обращаются к возможностям других государств.

Весьма показательным примером требуемого уровня разработки такого рода программно-аппаратного комплекса и эффективности его практического внедрения является интеллектуальная система, называемая «великий китайский файрвол» и развернутая правоохранительными структурами КНР [108].

В совокупности в указанной системе объединены несколько десятков специализированных инструментов, предназначенных для контроля, анализа, избирательной блокировки зарубежных сервисов, веб-сайтов и приложений.

Система находится в ведении китайской киберполиции. Основными видами ее функционала в целях выявления и пресечения незаконной деятельности являются: целенаправленная фильтрация трафика; контроль доступа к иностранным сервисам Интернет-полиции; от-

слеживание действий пользователей, анализ их сетевой активности; мониторинг контента сетевых платформ.

Учитывая возможности отмеченных мероприятий, цели контроля виртуального пространства закреплены как в ряде международных [3], так и российских национальных документов – Стратегия национальной безопасности РФ, Стратегия развития информационного общества в РФ, Доктрина информационной безопасности РФ [14–16].

В них отмечены довольно близкие нормативно-правовые нотации и подходы. Так, утвержденные регламенты российских документов направлены на организацию эффективного управления информационно-коммуникационными процессами в целях реализации и обеспечения защиты частных и публичных интересов личности, общества и государства.

Схожие с А. Н. Поздняковым позиции поддерживают и другие авторы, среди которых отметим работу А. А. Бабушкина [66], в которой определяются возможности внедрения системы оперативно-розыскного контроля за лицами, склонными к совершению преступлений. Для этого рассматриваются ее правовые принципы, организационно-тактические формы, информационно-аналитическое обеспечение, базирующееся на применении информационно-телекоммуникационных технологий, в том числе – на основе ИИ.

Подобного рода наработки представлены также в работах [95; 241; 243; 248–252; 298; 374; 398].

Полученные современные результаты в указанном направлении представлены в монографии [354], где раскрыта методика программно-интеллектуального выявления и анализа материалов оперативного интереса в социальных медиа.

Базовым в ней является положение о том, что сегодня любая человеческая деятельность оставляет после себя «цифровые» следы, отражающие действия пользователя в сети Интернет и в соответствующих микропроцессорных устройствах. Эти следы могут быть использованы в системе доказательств при раскрытии и расследовании киберпреступлений.

Методика выявления и анализа элементов «цифрового портрета» объекта оперативного интереса представляется как последовательность реализации этапов:

- получение установочных данных;
- выявление элементов «цифрового портрета»;
- определение перечня аккаунтов, подлежащих обработке;
- анализ «цифрового портрета» объекта интереса;
- выявление и анализ организованных сетевых структур.

Совокупность «цифровых следов» условно разделена на:

- *содержательные*, обладающие значимой информацией и, как правило, создающимся объектом интереса осознанно (личные фото-

графии и видео, тексты электронных сообщений и прикрепленных вложений);

- *сопутствующие*, формирующихся без участия объекта интереса и являющихся метаданными (адреса сетевых устройств, данные геолокации, биллинговая информация и т. д.).

На технологическом и функциональном уровне социальные медиа выступают как средство связи и как среда взаимодействия, где пользователи, проявляя сетевую активность, оставляют следы своего пребывания. Важной особенностью «цифровых следов» объектов оперативного интереса является то, что они постоянно изменяются. Отсюда и следует целесообразность непрерывного сбора изменяющейся информации, ее профессионального мониторинга.

В рамках мониторинга с помощью информационно-аналитических систем выявляются и собираются сведения о сетевых фактах и характерных проявлениях пользователей, включая их метаданные:

- о сетевой активности (посты, репосты, комментарии, обсуждения и т. д.);
- изменение профилей, анкетных данных, географического положения, аватаров;
- характерной текстовой информации (лексика; сетевые, финансовые реквизиты и установочные данные; другие характеристики контента объектов интереса);
- характерных изображений (лица; символика; текст на изображениях; фотографии геолокаций);
- связях с объектами оперативного интереса.

Ориентирующая информация может добываться с помощью информационно-аналитической системы, например, ПС СЕУС. Информация в ней доступна в режиме *on-line*, однако полнота и достоверность сведений зависит от данных, размещенных владельцем социальных медиа.

Они в целом определяются возможностями используемой информационно-разведывательной системы. Но полученная информация требует дополнительного процессуального доказательства.

Доказательственная информация базируется на применении установленного порядка взаимодействия уполномоченных органов с организаторами распространения информации. Информация доступна только после получения официального, но далеко не всегда оперативного ответа от организаторов. Обязательным при этом является необходимость использования механизма оперативно-служебного документирования оперативных данных об объекте интереса.

Поэтому при решении реальных оперативно-служебных задач и оценке конкретных обстоятельств требуется определение необходимости выбора отмеченных вариантов сбора сведений, а может и их комбинирование.

В работе К. А. Кузьминой [212], связанной с рассмотрением нейросетевых моделей мониторинга социальных медиа для выявления деструктивного контента, указано, что ведущим трендом в задачах оперативно-розыскного поиска в киберпространстве является использование технологий ИИ.

Для исследования выбраны медиа с объемом пользовательской аудитории порядка 75 млн:

- Telegram (61 %);
- ВКонтакте (21 %);
- Одноклассники (8 %);
- прочее (10 %).

Поисковые задачи ориентированы на поиск контента с пропагандой идеологии терроризма, порнографических материалов; касающихся незаконного оборота специальных технических средств, запрещенных веществ и многого другого.

Для реализации подобного подхода компанией Т-АВИАС разработан специализированный интеллектуальный программный комплекс *41ChAT*, архитектура которого приведена на рис. 2.8, а *QR*-код этого программного продукта, ориентированного, в том числе на обеспечение систем защиты информации беспилотных авиационных систем представлен на рис. 2.9.

Интеллектуальный программный комплекс *41ChAT* обеспечивает аналитические отчеты о возможности решения задач:

- попарного анализа изображений;
- текстового анализа ключевых тем и выявления важной оперативной информации;
- обобщения результатов анализа изображений и текстов, принятие решения о вредоносности рассматриваемого канала.

Подчеркнем, что реальная оперативная и процессуальная работа, проводимая в области исследования сетевых цифровых следов на основе технологий ИИ, ориентирована и на решение задач предупреждения и профилактики киберпреступлений, о которых будет рассказано ниже.

Противодействие серийным преступлениям. Преступления данного типа считаются одними из самых сложных в раскрытии и расследовании. Они требуют высокопрофессиональных подходов и умений у оперативно-розыскного и процессуального персонала, штатно обеспечивающего реализацию данного функционала, обладания ими на требуемом уровне методами и подходами тактики в процессах поиска, сбора и обоснования информации о выдвигаемых версиях.

Эффективную помощь в этой деятельности могут оказать подходы и методы использования специализированных технологий ИИ. Особенности внедрения в практику подобного инструментария можно проследить, например, в работе [113].

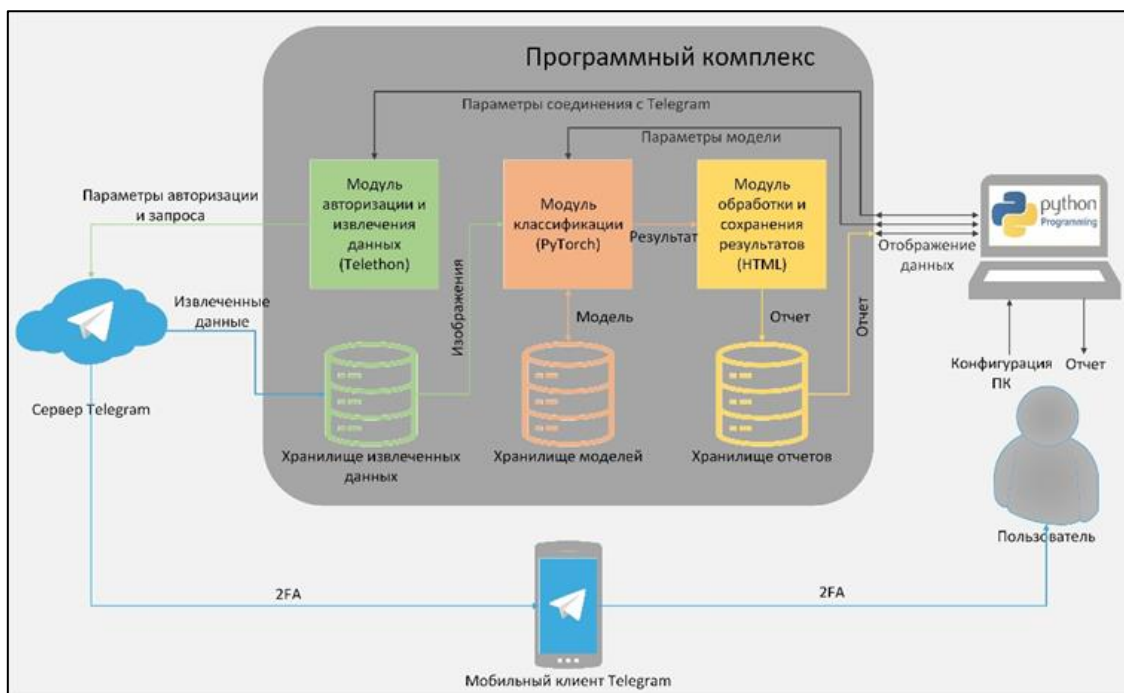


Рис. 2.8 Архитектура программного комплекса мониторинга социальных медиа для выявления деструктивного контента [212]

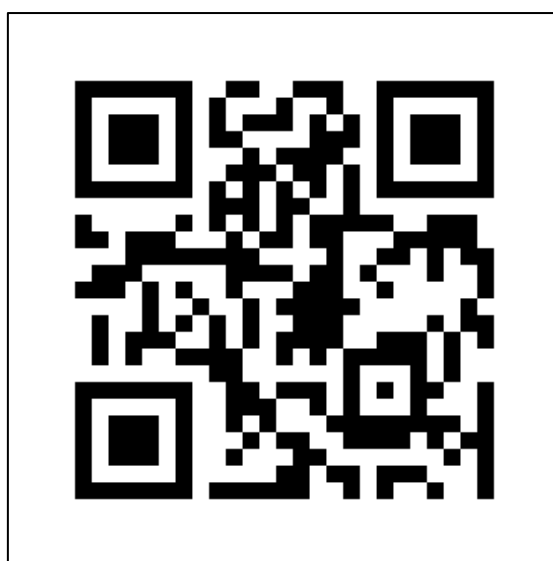


Рис. 2.9. QR-код программного комплекса 41ChAT

В ней рассмотрены результаты научно-исследовательской работы (НИР) под шифром «СЕРИЯ». В проведенной исследовано машинное обучение, как один из методов ИИ анализа данных в целях выявления признаков серийности определенных категорий преступлений.

Основу эмпирической базы проведения НИР составили систематизированные обращения к совокупности данных по раскрытым и оконченным расследованиям серийных преступлений против личности. В частности, анализировались 370 эпизодов по законченным расследованиям, подследственными в которых были довольно известные

фигуранты или наименования серий преступлений – Чикатило, Ряховский, Табардин, Миргород. В качестве характеристик, сформировавших особенности представления серийных преступных эпизодов, оценивались 76 параметров: тип преступления, место и время их совершения, наличие сопутствующих деяний и т. д.

Целевая установка применения технологий ИИ в решении поставленной задачи заключалась в разработке и апробации пилотного образца специального интеллектуального программного обеспечения. Алгоритм программы тестировался на возможность определения и выделения отдельных эпизодов в серийные версии совершенных преступлений.

Общий, достаточно высокий результат точности предложенного алгоритма составил 72,5 % от выводов расследования реальных серийных преступлений против личности. Так, для серии под названием Миргород реально доказано 16 эпизодов преступлений, а модельный результат составил 14 эпизодов (87 %), когда система ИИ сгруппировала их в общую версию (карта систематизации приведена на рис. 2.10). Результат для серии Бондаренко изображен на рис. 2.11.

Успешность проведенного исследования указала на перспективность приложений модели ИИ. Но, выявлены и негативные нюансы, связанные с процедурами отнесения преступлений к их предполагаемой серии.

По мнению авторов исследования, такие недостатки связаны, прежде всего, с неполнотой заполнения исходных учетных и регистрационных карт, отсутствием единого, системного подхода в описании типовых информационных объектов в правоохранительных базах данных. То есть, сказывается влияние человеческого фактора из-за недобросовестности внесения необходимых сведений и отсутствие надежного программного контроля такого рода ситуаций. А самое главное, по нашему мнению, существующая применительно к профессиональным базам данных *разница в терминологическом описании одних и тех же объектов учета*.

Подобные исследования проводились и в Московской академии Следственного комитета Российской Федерации имени А. Я. Сухарева. Там коллективом ученых разработано ПО «Портрет серийного убийцы *PorSerO*». Программа формирует цифровую криминалистическую модель преступления в виде формализованной электронной системы криминалистически значимых признаков и их связей между собой в виде числовых данных и в итоге создает поисковый портрет серийного преступника [27].

В целом отмеченный подход вполне применим не только к общеуголовной преступности, но и может быть реализован и для решения задач противодействия киберпреступлениям. Для этого требуется практическая адаптация метода, создание удобных интеллектуальных программных приложений и их методического обеспечения.

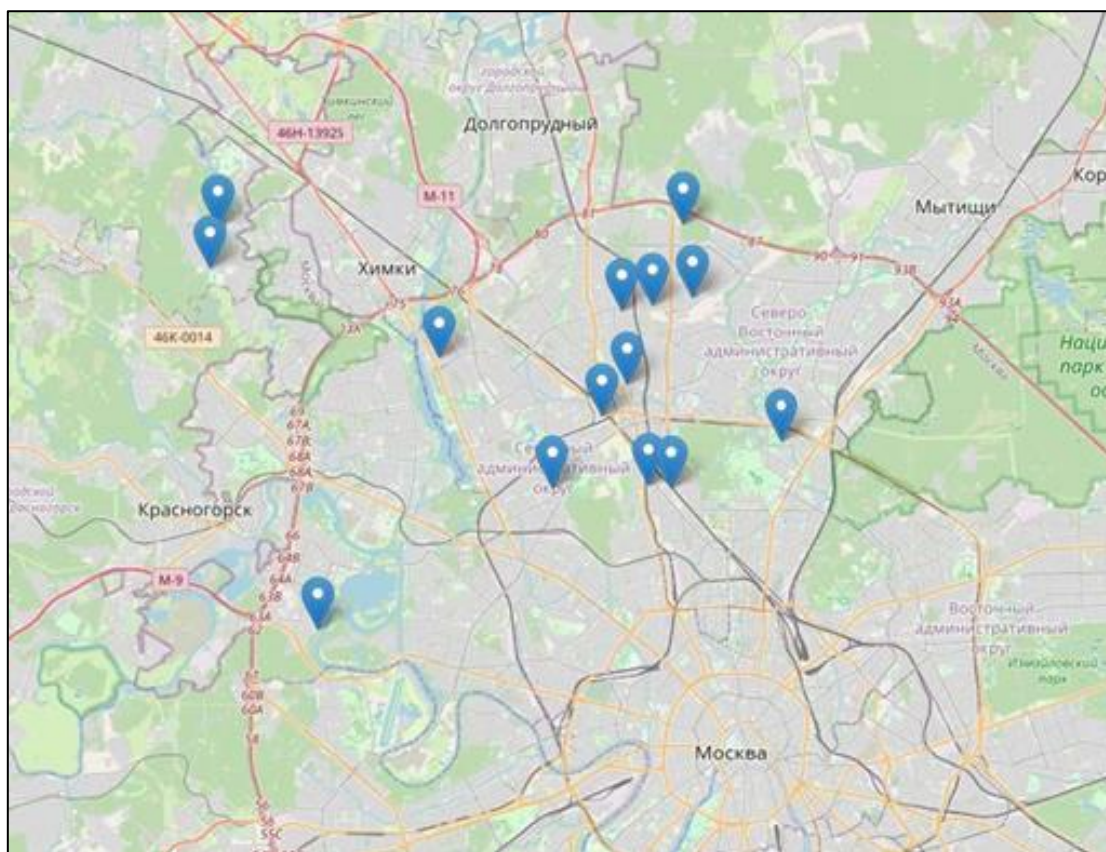


Рис. 2.10. Карта выявления эпизодов серии преступлений Миргород на основе модели ИИ [113]

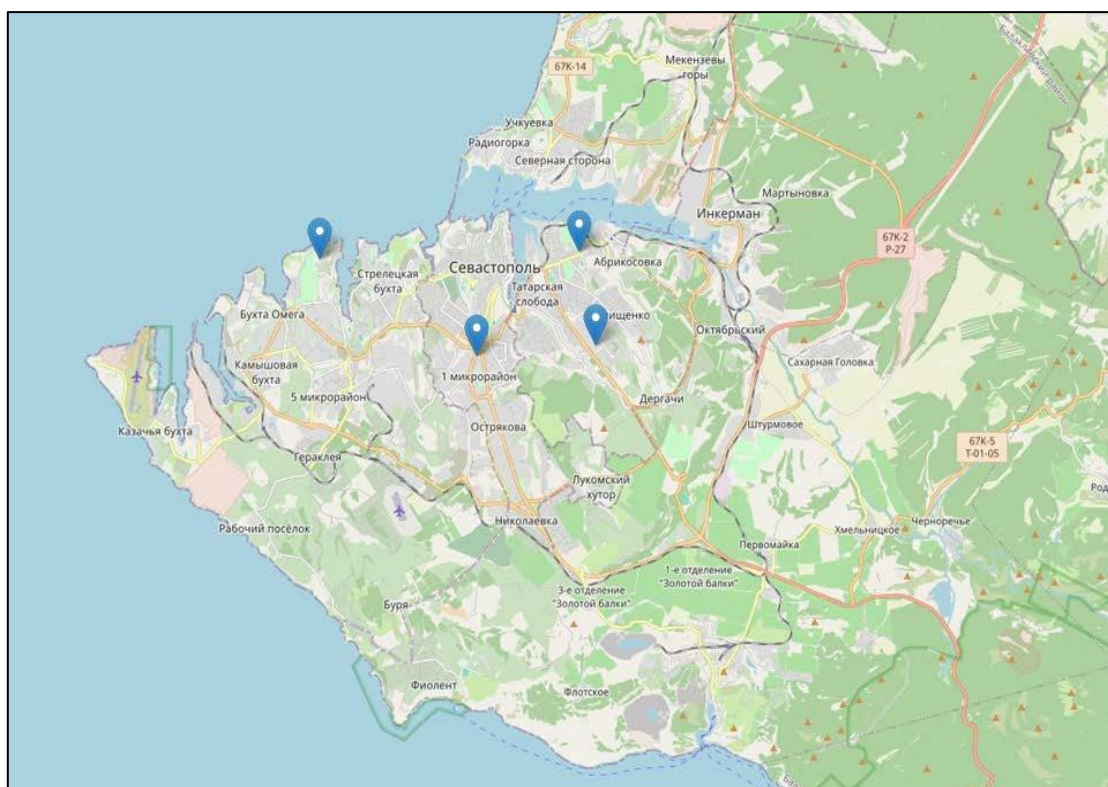


Рис. 2.11. Результаты выявления моделью ИИ эпизодов в серии Бондаренко [113]

Экономическая безопасность и противодействие коррупции (ЭБиПК). В указанной сфере имеются определенные наработки в области применения ИИ. Вместе с тем, отмечается и ряд проблемных вопросов.

В частности, Р. Г. Искалиев указывает в работе [180], что одна из них и довольно противоречивая состоит в том, что данный интеллектуальный инструмент даже не упоминается в нормативно-правовой регламентации указанной деятельности. Об этом свидетельствует, например, анализ текста Основных направлений дальнейшего развития единой системы информационно-аналитического обеспечения деятельности МВД России до 2024 г. [25].

В то же время, реальная практика говорит о достаточно активном использовании технологий ИИ в деятельности полиции. Речь идет, прежде всего, о таких системах, как ИСОД МВД России, автоматизированные информационные системы (АИС) «Карта криминальности», аппаратно-программный комплекс (АПК) «Безопасный город», подсистема «Дистанционное мошенничество» ПТК (программно-технический комплекс), «ИБД-Ф» (федеральный интегрированный банк данных), «Следопыт-М», СПО «Паутина» с включением массивов данных от АПК «Розыск-Напо», робототехнический комплекс «Сфера», «Крибрум», «Зеркало» («Верблюд»), Автоматизированная система обработки инцидентов «ФинЦЕРТ» и многих других.

Можно также отметить и другие приложения. Так, хорошо зарекомендовало себя российское приложение *PolyAnalyst*. Оно является программным продуктом компании Мегапьютер, представляя собой аналитическую среду разработки интеллектуальных решений для проведения глубокого анализа данных на предмет выявления оперативно значимой информации, обоснования розыскных версий и сбора доказательств, информационной взаимосвязи фактов из открытых и закрытых баз данных.

Подобного рода система *Zero Trust* (КНР, эксплуатация с 2016 г.) имеет доступ к 150 государственным, финансово-кредитным базам данных с информацией о деятельности и социальной жизни государственных служащих, используя *модель безопасности с нулевым доверием – ZTA*. Данная архитектура отражает стратегию проектирования и внедрения IT-систем, ориентированных на решение задач правоохранительных органов. Концептуально она реализует принцип – «никогда не доверять, всегда проверять».

Профилактика преступлений в киберпространстве. Основа данного научно-практического подхода, определенная, в частности, в исследованиях В. Ю. Федоровича [412–417] по созданию теории криминалистической (экспертной) профилактики может быть выражена рядом следующих положений. Они сформулированы автором на основании интеграции современного нормативно-правового регулирования задач профилактической деятельности правоохранительных

органов и результатов целенаправленных изысканий в этой предметной области.

Нормативно-правовая сторона данного подхода выражена, например, в Федеральном законе «Об основах системы профилактики правонарушений в Российской Федерации» [10], приказе МВД России от 11.01.2009 № 7 (с изм. от 09.03.2023) «Об утверждении Наставления по организации экспертно-криминалистической деятельности в системе МВД России» [26].

На фоне современных общественных изменений важно отметить необходимость дальнейшего развития учения о криминалистической (экспертно-криминалистической) превенции преступлений с учетом теории криминалистики и судебной экспертизы и теории информационно-компьютерного обеспечения криминалистической деятельности [396; 413]. Текущие условия применения ИИ предъявляют повышенные требования к технико-криминалистическим средствам предупреждения высокотехнологичных преступлений, выявления информации о готовящихся преступных деяниях, защите объектов от преступных посягательств и создания условий для формирования доказательственной информации.

На взгляд автора, использование ИИ в правоохранительной деятельности зависит от потенциала технико-криминалистических средств для решения указанных задач, уровня методического обеспечения и готовности субъектов профилактики к применению технико-криминалистических средств. Создание единой информационно-аналитической платформы различных субъектов профилактики (экспертно-криминалистических, следственных, оперативно-розыскных и других подразделений) позволит актуализировать системный обмен информацией в целях решения профилактических задач [412].

Интеллектуальные системы способны выявлять аномальное поведение пользователей, автоматизировать оперативное реагирование на инциденты и строить прогнозные модели. Так, внедрение XDR-платформ (*EXtended Detection and Response*) обеспечивает интегрирование данных из различных источников (системные журналы, трафик, поведение пользователей) и оперативное выявление сложных угроз.

Современный уровень технологий делает актуальным противодействие фальсификации цифровых данных. Так, в рамках сотрудничества Сбербанка и МВД России осуществляется разработка и внедрение технологии выявления и нейтрализации дипфейков, активно используемых в мошеннических схемах обмана граждан.

Эффективное решение современных экспертно-профилактических задач сегодня базируется на применении технологий ИИ при обработке криминалистически значимой информации в целях предупреждения и предотвращения преступлений. Для этого совершенствуется взаимодействие при совместной работе специалистов в сфере криминалистики и судебной экспертизы, а также специальных субъектов

профилактики, развитие теоретических основ криминалистической превенции на основе применения технологий ИИ.

Базовые позиции здесь выражаются в решении оперативно-служебных задач ОВД и обращении к информационной поддержке посредством обработки больших данных в процессах интеллектуального автоматизированного мониторинга криминалистических и иных учетов, использования технологий *OSINT*. В результате до заинтересованных исполнителей доводятся выявленные ориентирующие и доказательственные материалы. Речь идет о сотрудниках ОВД, задействованных в решении конкретных оперативно-служебных задач или заинтересованных в указанных материалах. Данная информационная поддержка позволяет исполнителям формировать развернутое представление о правонарушениях, вычленять в них очевидные и скрытые закономерности, обосновывать свои решения.

Совокупность полученных материалов способствует выработке типовых рекомендаций по противодействию преступлениям и правонарушениям, с учетом оригинальных или повторяющихся особенностей их проявлений, а также по формированию специфических для сферы киберпреступности профилактических мероприятий [58; 65; 80–81; 101; 412; 417].

Основные пути осуществления данной работы видятся: в выявлении условий, способствующих совершению преступлений; организации прогнозирования возможных способов совершения преступлений, включая потенциал технологий ИИ; использовании возможностей технологий криминалистического характера в предупреждении преступлений.

Возможно участие в работе общественных советов (оперативных штабов) по мониторингу ИТ-преступности в целях выработки политики предупреждения преступных посягательств, а также принятия мер профилактического характера. Для распространения и продвижения профилактического контента предусмотрено использование СМИ, социальных сетей, активизация кибердружин и представителей волонтерского движения [18]. Отмеченные положения должны обеспечить меры профилактического воздействия при возможных аналогичных происшествиях.

В дополнение обратимся к работе О. В. Русецкого [367]. В ней освещены принципы профилактики преступлений в кибернетическом пространстве. Данный вид преступности, характерный для киберпространства, опирается на новые противоправные средства и способы, специфическую техническую и технологическую среду их реализации, качественные изменения общественного сознания, образа жизни населения.

Современные процессы информационной модернизации социума в то же время значительно определяют характеристики криминального поведения:

– реализация достижений информационных технологий в детской среде. На основе увлекательного, яркого и динамичного удовлетворения потребностей детей в познании мира гаджеты становятся близким «другом», постоянным помощником. В криминологическом плане именно развивающаяся серьезная привязанность несовершеннолетних к информационно-коммуникационной среде формирует проблемы их социализации, а затем и активного взаимодействия с противоправными процессами;

– воздействие на сознание детей посредством создания искусственной реальности на основе игрового подхода способно обеспечить редукцию значимых элементов мировоззрения пользователя и довести его до возникновения иллюзорного чувства реальности. Все это реально уменьшает вероятность адекватной оценки событий, рождает неуверенность в будущем, фрустрацию, приводят к анархическим настроениям. В конечном итоге, подобные, «вновь сформированные личности» неадекватно воспринимают реальную возможность уголовного преследования и последующего наказания;

– формирование зависимости от сетевого воздействия и информационно-коммуникационных технологий. Наличие данного вида зависимости подтверждается в исследованиях психологов, социологов, медиков. Они предлагают ее внесение в перечень поведенческих зависимостей как нового вида, порожденного интернетом и информационно-коммуникационными технологиями.

Уже не секрет, что такая зависимость способна создавать реальные условия для реализации противоправных видов поведения. Кроме того, обосновывается влияние рассматриваемой зависимости на снижение нормальных процессов социализации конкретных личностей;

– влияние сетевых и информационных технологий на возможности достижения деструктивных политических целей, организации и осуществления противоправных деяний в области киберпреступлений.

В современном обществе стало значительным возникновение противоречий новых видов. Например, интенсивное освоение информационных технологий и низкий уровень компьютерной грамотности; отставание внедрения и правового регулирования информационных технологий по сравнению с высоким технологическим уровнем их разработки; повышение виктимогенности населения в условиях новых кредитно-финансовых отношений и активизация применения мошеннических алгоритмов и схем посягательства на них.

Рассмотрим основные направления предупреждения преступности в киберпространстве:

– создание условий для максимально безопасного развития информационных технологий на основе нового уровня взаимодействия в кибернетическом пространстве, формировании более совершенной нравственной и правовой культуры, правильного изменения и поддержания ценностной и мировоззренческой ориентации по восприя-

тию виртуальной реальности, в первую очередь, среди несовершеннолетних и в молодежной среде;

– снижение действия социальных и личностных факторов, которые определяют в информационно-кибернетическом пространстве криминальное поведение пользователей.

Детализируем аспект, связанный с возможностями интеллектуальных технологий в противодействии кибермошенничеству. При рассмотрении соответствующих направлений и инструментов сошлемся на работу [220].

В ней проведена оценка, показавшая, что ИТ-система Сбербанка в 2024 г. предотвратила 72,2 млн мошеннических операций, то есть вдвое больше, чем в предыдущем году. В этих целях разработано и использовано около сотни моделей ИИ для разных вариантов осуществления противоправных деяний.

Интересно отметить, что ручная проверка в банковском или биржевом секторе – KYC (*Know Your Customs*) – для одного клиента оценивается от 500 до 5 тыс. рублей, а при автоматизации снижается до 90–200 рублей. Да и работа по автоматизированному выявлению мошенничества существенно дешевле по сравнению с затратами на традиционное расследование и возмещение причиненных убытков.

Наконец, преимущественным выступает адаптируемость ИТ-систем к изменяющимся условиям рынка и появлению новых видов кибермошенничества. Однако нужно учитывать при этом и, как правило, более быструю адаптацию преступных схем и привлечение технологий ИИ для осуществления кибермошенничества криминальной средой. Что требует, в свою очередь, ускорения решения задач повышения технической и правовой грамотности сотрудников правоохранительных органов, занимающихся раскрытием и расследованием кибермошенничества.

Сегодня изысканиями причин и условий совершения киберпреступлений, их криминологического прогнозирования на основе технологий ИИ, а затем выработки мер их предупреждения занимаются многие исследователи.

Так, В. О. Давыдов [147] изучает специфический вопрос *оценки вероятности использования систем ИИ криминалитетом* в целях разработки сценариев развития криминальных событий, а также формирования комплекса методов и средств эффективного проведения их расследования.

Статья Н. И. Старостенко [384], базируясь на анализе способа совершения *мошеннических действий с использованием интеллектуальных DeepFake-технологий*, рассматривает принципы формирования прогностического подхода в целях расследования хищений в сфере информационно-телекоммуникационных технологий.

В работе А. П. Суходолова и А. М. Бычковой [386] авторы обращаются к опыту применения ИИ для анализа различных сторон пре-

ступности – прогнозная психометрика преступного сообщества – COMPAS; система прогнозирования преступлений *PredPol*; система *ePOOLICE*; программные продукты *Palantir*; российская система «Искусственный интеллект».

Можно указать еще на ряд исследований, раскрывающих применение технологий ИИ в решении задач правоохранительных органов:

- о международной организации противодействия киберпреступности ведут свои рассуждения И. Е. Лапшина, Л. К. Зеленкова [219], исследуя вопросы функционирования *уголовной полиции Интерпола*. Исследование связано с правовым регулированием данной организации, а также с основными направлениями ее деятельности в условиях цифровизации общественных отношений. Авторы подчеркивают перспективу развертывания в Интерполе служб, обеспечивающих расследование и раскрытие киберпреступлений;

- оценка *перспектив внедрения ИИ в деятельность ОВД* проводится З. С. Гельмановой и Т. К. Бакаевым [126]. Авторы обращаются к опыту анализа больших данных, прогнозирования преступлений, распознавания лиц оперативного интереса, управления центрами правовой информации, обеспечения кибербезопасности, международного сотрудничества;

- исследование путей *совершенствования автоматизированных информационных систем* в целях обеспечения расследований преступлений проводит Е. А. Астахова [62]. Автор отмечает продолжающееся *развитие интеллектуальной поддержки* алгоритмического и программного обеспечения; *формирование новых видов систем* – характеризующих преступления (цифровые следы, способы совершения киберпреступлений, параметры внешности, психики, навыков и иных особенностей личности преступников), связанных с появлением новых видов и групп преступлений (по сферам, субъектам и объектам совершения); *создание единых баз данных*;

- вопросы реализации *административной функции правоохранительных органов* на основе разработки, внедрения и применения специализированных технологий ИИ стали предметом исследования А. Р. Атабекова [63]. Автором намечены пути решения нормативно-правовых вопросов, нацеленных на предиктивные возможности в области предупреждения правонарушений граждан;

- С. В. Расторопов и В. А. Прорвич [358] обратили внимание на формирование информационных основ уголовно-правовой *защиты субъектов цифровой экономики и финансов*, используя технологии ИИ. Авторы рассматривают проблемно-ориентированные интеллектуальные средства обработки информации при выявлении и раскрытии преступлений в сфере цифровой экономики и финансов;

- оценивая возможности *нейросетевых технологий*, А. В. Лагуточкин [217] указывает на их инновационную основу *в сфере проведения оперативно-розыскной деятельности*. При этом особая роль им

отводится противодействию киберпреступности в молодежной среде. Он анализирует причины активного вовлечения молодых людей в этот вид антисоциальной деятельности, приводящей их в конечном итоге в число ее инициаторов и организаторов.

Речь идет, в том числе, о таких сетевых явлениях, мотивирующих повышенный интерес детской, подростковой, молодежной среды. Заметными и отрицательно известными в мировой практике стали, например, «Синий Кит» и подобные опасные увлечения – «Тихий дом», «Море Китов», «Разбуди меня в 4:20» и других, склоняющих пользователей к суицидальным действиям; «Арестантский уклад един»; «Секстинг»; «Грумминг»; «Зумбобинг». В организации должного противодействия, необходимого оперативно-розыскного прикрытия, предупреждения и пресечения данных киберпреступлений автор видит возможности применения нейросетевых технологий;

– отметим работу А. В. Соколовой [378], которая рассматривает возможности применения технологий ИИ в осуществлении судебно-баллистической экспертизы. Это – одно из множества исследований, направленных на обеспечение экспертно-криминалистической деятельности поддержкой ИИ, активно развивающейся в системе МВД России.

Читателям, желающим расширить свои представления об использовании ИИ в противодействии киберпреступности, рекомендуем обратиться также к работам: [78–79; 106; 149; 174; 181; 183; 284–288; 299; 314; 349–353; 404].

До текущего момента в разделе отражены общие, систематизированные положения, относимые к *эволюционному подходу* в развитии применений ИИ в решении оперативно-служебных задач правоохранительных органов. Однако немаловажно уделить внимание и *революционным*, по сути, тенденциям, которые, на первый взгляд, казались не обладали заслуживающим внимание потенциалом в формировании новых подходов, технологических решений, востребованностью практических приложений ИИ.

Первая такая тенденция связана с организацией движения *беспилотных транспортных средств* (БТС), управления ими, а главное – практическими приложениями во всём их технологическом богатстве, начиная от хозяйственного применения и до обеспечения безопасности в широком смысле. Все это требует разработки, внедрения и использования ИИ.

В настоящем монографическом исследовании авторы в большей мере будут выделять *БТС воздушного направления*. Другими их синонимами, которые также встретятся ниже, являются беспилотные воздушные суда – БВС, беспилотные авиационные системы – БАС, беспилотные летательные аппараты – БПЛА. Общие представления о парке современных воздушных средств, их основных тактико-технических характеристик дает, например, работа [376].

Обращение к данной технологии в тех или иных целях насчитывает достаточно значительный исторический период, начиная с наступления XX в., когда в 1916 г. британский инженер Арчибальд Лоу разработал первый прототип БВС. В 1930-х гг. развитие БАС получило новый импульс, благодаря поискам способов улучшения разведки в разных сферах.

В современный период ряд факторов резко изменил развитие БАС, в том числе и для решения задач правоохранительных органов. С начала 2000-х гг. оно продолжает ускоряться, основываясь на новых достижениях в области ИИ, машинного обучения и сенсорных технологий.

Сегодня БАС представляют собой, прежде всего, высокотехнологичные системы. Они способны выполнять широкий спектр задач с минимальным участием человека.

К факторам интенсификации применения БАС относятся: технико-политические, политико-организационные условия ускорения развития человеческой цивилизации; существенные ресурсные вливания государств в совершенствование технологий, в том числе – в связи с обострением международной обстановки, усилением военно-политического противостояния мировых держав; появление новых сфер использования технологических решений. Более подробно к оценке всех имеющихся при этом целей, задач, имеющихся противоречий обратимся в главах 3 и 4.

На текущий момент укажем только общие направления использования воздушных БТС, в том числе под управлением технологий ИИ, применительно к деятельности ОВД. Они отражаются в следующем функционале [164]:

- оперативно-служебное и профилактическое видеонаблюдение. Например, при обеспечении безопасности массовых, представительских, протестных мероприятий; выполнение мероприятий «безопасного города»; предотвращение террористических актов и устранение их последствий;

- розыскные мероприятия;
- организация оперативной связи;
- поддержка проведения оперативно-следственных мероприятий (задержания, проведение операций, пресечение нелегальной миграции; осмотры мест происшествий, особенно со сложными и опасными условиями, требующими 3-D видеоотчетов);

- видеонаблюдение за наземными и морскими линиями регулярных сообщений; транспортными потоками; транспортом, угнанным или представляющим оперативный интерес; анализ причин и последствий ДТП;

- противодействие морскому пиратству;
- фиксация незаконной разработки недр, хищения биоресурсов, выращивания наркотикосодержащих растений и т. д.

При этом не следует забывать, что использование технологий БТС проявилось, к сожалению, в активном интересе у представителей так называемой высокотехнологичной преступности. Противоправными формами деяний в этой сфере выступают: террористическая деятельность, посягательство на жизнь; несанкционированное исследование различных объектов, фиксация результатов и их применение для организации последующих преступлений; слежка за людьми и наблюдение за объектами; контрабанда запрещенных предметов (оружие, наркотики, средства связи, денежные средства и т. д.), доставка их в режимные зоны; отслеживание действий правоохранительных органов и организация сокрытия следов преступлений, выхода из критических оперативных ситуаций; реализация киберпреступлений, руководство их осуществлением [386].

Организация должного противодействия негативным явлениям, связанным с БТС, подразумевает поиск эффективных решений. Опыт показал, что их требуемый уровень обеспечивают как раз технологии ИИ, применяемые в различных приложениях.

Ведущая роль в противодействии киберпреступлениям в МВД России отведена Управлению по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России (УБК МВД России). Оно создано в структуре центрального аппарата приказом МВД России от 11 октября 2022 г. № 747 [281].

УБК МВД России реализует функции головного подразделения по борьбе с преступлениями, совершёнными с использованием (в сфере) ИКТ, а также в области противодействия распространению противоправной информации в интернет.

Основные задачи Управления связаны с предупреждением, выявлением, пресечением и раскрытием преступлений и иных правонарушений в сфере ИТ-технологий, а также координацией этой деятельности в системе МВД России.

Основным направлением деятельности Управления является анализ данных информационно-коммуникационных сетей в целях выявления запрещённого контента, поиска и фиксации ориентирующей и доказательственной информации о противоправных действиях в этой сфере. На него же возложено обеспечение организации взаимодействия подразделений ОВД с государственными органами, органами власти субъектов РФ, учреждениями финансово-кредитной сферы и иными участниками информационного обмена.

По инициативе УБК МВД России решается вопрос создания единого реестра адресов электронных ссылок на официальные сайты хозяйствующих субъектов, добросовестно осуществляющих свою деятельность посредством сети. Цель проекта – выявление и блокирование фишинговых сайтов, используя интеллектуальные алгоритмы.

Сегодня один из путей организации мошенничеств – использование абонентских номеров, вовремя не отвязанных от портала «Госуслуги». Кроме того, злоумышленники широко используют технологии подмены номеров на официальные телефоны банков и государственных структур.

Автоматизированная система «Антифрод» Роскомнадзора предназначена для блокирования таких соединений. Реакция злоумышленников на такую деятельность последовала достаточно быстро – организация новых вариантов коммуникации через специальное оборудование для массовой рассылки, приёма коротких сообщений, активации сим-карт и преобразования международного телефонного трафика в российские сети.

Постоянной задачей правоохранителей в этой связи выступает обнаружение и изъятие такого оборудования. В частности, в 2024 г. подобные ОРМ были проведены на территории 29 регионов.

Результатом их явилось изъятие более 600 единиц специального оборудования сим-банков, более 120 тысяч сим-карт различных операторов сотовой связи, а также привлечены к уголовной ответственности 17 лиц, организующих и реализующих мошеннические операции.

Предполагаемая профилактическая оценка может выражаться различными характеристиками. Так, с помощью изъятых технических устройств у мошенников была возможность совершать до 30 млн звонков в сутки.

Нужно отметить и проблему низкой правовой и финансовой грамотности граждан, несоблюдения ими правил цифровой гигиены, пренебрежения ими информацией о наиболее распространенных видах мошенничества, постоянно доводимой до населения правоохранительными органами.

Для повышения профилактики дистанционных мошенничеств УБК МВД России постоянно ведёт телеграмм-канал «Вестник киберполиции России» (https://t.me/cyberpolice_rus). На нем регулярно выставляются публикации о новых видах мошенничеств, правилах соблюдения цифровой гигиены, о совершении преступлений в сфере информационно-коммуникационных технологий, в том числе в интернете.

Среди опубликованных там видеоматериалов выделяется тематика: треш-стриминга; рассылки ложных сообщений об экстремистских актах; особенностей мошеннических действий с использованием социальной инженерии; преступлений против половой неприкосновенности несовершеннолетних; кибербуллинга; антинаркотического характера и т. д.

Реальное воздействие на население выполняется через социальные сети и мессенджеры с территорий недружественных стран, в том числе – с Украины. Работа Управления по профилактике отмеченных групп преступлений характеризуется большим объемом конкретных

мероприятий, например, в 2024 г. это привело к блокированию более 5 тыс. интернет-ресурсов с запрещённой информацией.

Расширение трансграничного характера киберпреступлений привело к необходимости усиления УБК МВД России в создании гармонизированных международных правовых механизмов. Эта деятельность позволила согласовать в августе 2024 г. значимый на международном уровне документ «Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определёнными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьёзным преступлениям».

Эффективное противодействие ИТ-преступности базируется на минимизации коммуникаций злоумышленников с их потенциальными жертвами, а также на разрушении системы вывода похищенных денежных средств. Для этого Управление совместно с заинтересованными государственными органами разрабатывает и реализует политику в сфере профилактики и противодействия ИТ-преступности.

Рассмотрим направления противодействия киберпреступности, в том числе – с привлечением технологий ИИ.

Первое направление связано с обеспечением безопасности граждан путем максимального снижения ущерба от дистанционных происков кибермошенников. При анализе рассмотренных выше вариантов организации данного противоправного деяния напрашивается простой вывод. Его смысл состоит в том, что не так важно, с помощью каких ухищрений и аргументов осуществляется воздействие, но, если оно в своей основе направлено на финансовое состояние атакуемого, то это – однозначно мошенники, и их необходимо опасаться. А вот здесь нужно понимать очевидное – без надежного привития населению элементарных правил безопасного финансового поведения не следует надеяться на помощь от любых высокотехнологичных решений, в том числе – со стороны ИИ. Поэтому, несмотря на возможные нетактичные элементы поведения по отношению к незнакомому абоненту, главным принципом атакуемого должно быть – «не верь глазам и ушам своим».

Определенную страховку от мошеннических случаев можно предусмотреть, рассчитывая на помощь потенциальным жертвам при использовании автоматизированной системы обработки инцидентов «ФинЦЕРТ», разработанной Банком России с подключением всех банков страны [419].

Ее функционал направлен на мониторинг событий на финансовом рынке, их анализ, и предназначен для обмена информацией с МВД России. Система имеет возможность блокировать денежные операции в случае наличия данных об их совершении без согласия клиента.

Важным этапом является обязательная фиксация в «черном» списке дропперов информации о владельце счёта, куда направлены похищенные средства. Регламент действий системы исключает у него опции дистанционного управления всеми своими счетами, открытыми в кредитных организациях. Применение этой технологии в противодействии дропперам довольно эффективно: ежедневно блокируется до 20 тыс. подобных сомнительных операций.

Кроме того, профессионалы рекомендуют работникам банковской системы на этапе принятия решений о выдаче кредитов и при общении с потенциальным клиентом шире использовать возможности целенаправленного профайлинга (от англ. *profiling* – профилирование) – метода анализа поведения и личностных характеристик, чтобы предсказать намерения человека или действия.

Требуют выполнения и другие рекомендации. Например, работникам связи необходимо соблюдать условие внесения достоверных данных о лицах, с которым заключаются договоры услуг связи. Четкое выполнение данного условия способно обеспечить исключение из оборота серых сим-карт. Но, к сожалению, недобросовестность некоторых работников связи благоприятствует сокрытию истинной информации о мошенниках.

Второе направление отражает особенности работы экспертов-криминалистов и применения технологий ИИ в процессе расследования ИТ-мошенничеств. Эта деятельность базируется на том физическом принципе, что невозможно подготовить и совершить преступление с использованием электронных устройств, при этом не оставив никаких следов в цифровом пространстве.

Конечно, стремясь скрыть свою противоправную деятельность, мошенники предпринимают различные технические и технологические ухищрения. Поэтому электронные носители, которые принадлежат подозреваемым в кибермошенничестве и попадают на криминалистические исследования, нередко имеют специальные цифровые следы, отражающие факты сокрытия, зашифровывания, преобразования, удаления отдельных информационных элементов.

Противодействовать этому и осуществлять эффективные действия по получению требуемых доказательств (последовательность работы банковских приложений, управляющих электронными кошельками, историю посещения интернет-ресурсов и т. д.) возможно лишь на основе применения специальных технических и аппаратно-программных средств (в том числе интеллектуальных), состоящих на вооружении экспертно-криминалистических подразделений.

Отметим ряд направлений их работы по расследованию ИТ-мошенничеств [206]:

– *компьютерные экспертизы*. Например, в одной из экспертиз исследовался ноутбук с зашифрованным разделом на носителе информации. При этом мошенниками применен тактический прием –

«матрешка», заключающийся в том, что в некоторой файловой системе создается ряд автономных функциональных систем. Интеллектуальный анализ данного, фактически виртуального внутреннего компьютера, позволил доказать, что вся мошенническая переписка в интернете осуществлялась именно через него (рис. 2.12);



Рис. 2.12. Инструмент для вскрытия «матрешки» [206]

– *исследование мобильных телефонов*. Память этого гаджета, как показывает экспертная практика, очень часто наполнена крайне полезной оперативной информацией. Естественно, кибермошенники предпринимают различные воздействия на мобильный телефон в целях устранения цифровых следов.

Но не всегда наличие даже сложного пароля, повреждение экрана, поломка аккумуляторной батареи или интерфейсного порта, криптостойкое шифрование данных и прочие ухищрения будут являться препятствием для получения доступа к внутренней памяти мобильного телефона. И в этом случае экспертно-криминалистические подразделения обладают требуемым набором программно-аппаратных инструментов;

– *фоноскопическая экспертиза*. Авторы настоящей монографии подробно обращались к этой теме, представив результаты в [84]. Здесь лишь подчеркнем, что направление «Выявление признаков использования специальных программных средств для изменения голоса» является одним из актуальных в современных экспертных исследованиях [142] при расследовании кибермошенничеств.

Для эффективного применения данного инструментария изучались алгоритмы изменения, имитации голоса. Исследования позволили сформировать корпус эталонных фонограмм (более 1 000 записей) и создать методическое приложение по осуществлению фоноскопических экспертиз для выявления кибермошенничества (рис. 2.13).

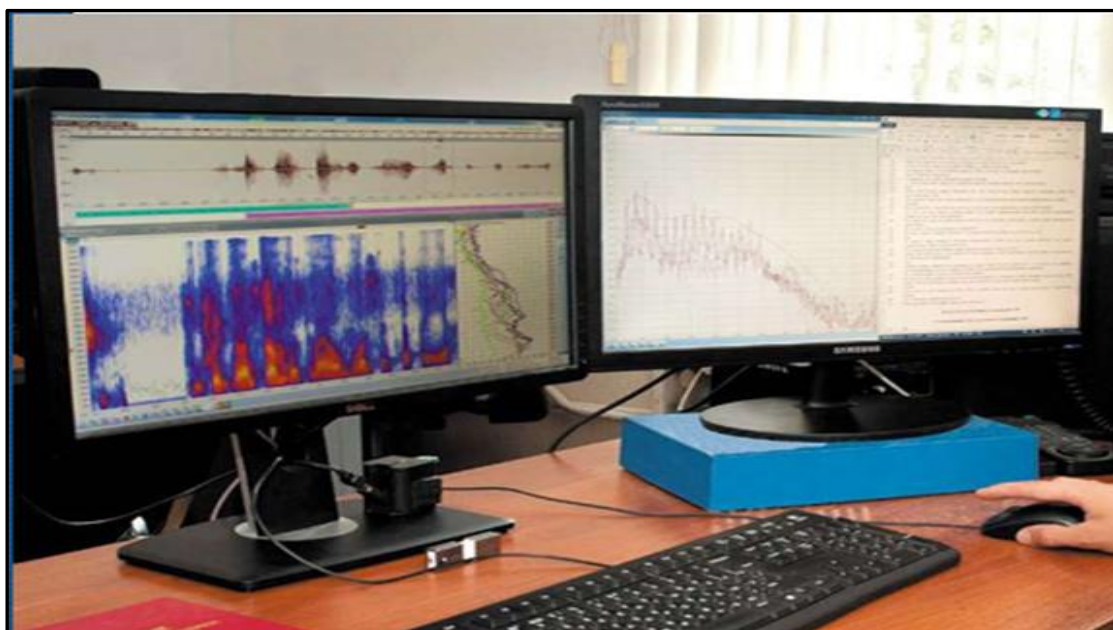


Рис. 2.13. Компоненты фоноскопического исследования имитации голоса [142]

Таким образом, задача извлечения информации из различных электронных устройств требует постоянных разработок новых и совершенствования уже имеющихся аппаратно-программных комплексов. Важным объектом при этом является компьютерная информация, которая размещается в облачных хранилищах (национальных или за пределами страны).

При этом следует отметить наличие у правоохранительных органов развивающихся методических подходов и аппаратно-программных средств для изучения облачных хранилищ и сетевых устройств. Важным моментом является возможность их применения в рамках производства следственных действий и ОРМ.

Третье направление связано с интеллектуальным сервисом обеспечения охраны общественного порядка (СООП), который реализован в ИСОД МВД России. Его задача – комплексная автоматизация деятельности подразделений по вопросам миграции и охраны общественного порядка территориальных органов и подразделений полиции на транспорте (окружной, межрегиональный, региональный и районный уровни).

Архитектурно СООП имеет модульную структуру. Текущая версия содержит модули: «Административная практика», «Административный надзор», «Инспектор ПДН», «Участковый», «Изолятор» и «Иные подразделения». Сервис доступен участковым уполномоченным полиции и сотрудникам патрульно-постовой службы непосредственно в ходе наружной работы, что повышает её качество и эффективность.

2.3. Выводы по главе 2

1. Современная оперативно-служебная деятельность по противодействию киберпреступности все в большей степени начинает опираться на интеллектуально-аналитическую поддержку правоохранительных структур, что соответствует общим мировым тенденциям. Текущее состояние указанных процессов характеризуется эволюционными и революционными аспектами, определяющими перспективы от возникающих новейших методов, средств и приложений.

2. Эволюционное направление связано с двумя тенденциями:

- общего характера – интеллектуальная поддержка типовых информационных операций; реализация новых возможностей в выявлении информационных связей оперативного интереса на основе современных прогностических моделей; интеллектуальное сопровождение задач обеспечения кибербезопасности, противодействия киберпреступлениям; использование сетевых возможностей для коммуникации и взаимодействия с гражданами;

- частного характера, отражающего современную практику – цифровые следы в Интернете как основа оперативно-розыскного поиска; противодействие серийным преступлениям; экономическая безопасность и противодействие коррупции; профилактика преступлений в киберпространстве и др.

2. Революционное направление затронуло процессы:

- использования беспилотного транспорта и функционального набора его возможностей, в реализации которых все большее место отводится технологиям ИИ. Нужно отметить, что особенностью их эксплуатации является, к сожалению, не только активный интерес к ИИ, но и его применение высокотехнологичной криминальной средой;

- противостояния, борьбы или, если хотите, «войны» технологий. Речь идет, фактически, об использовании технологий ИИ для подготовки и непосредственного совершения киберпреступлений. Это обстоятельство, в свою очередь, требует от правоохранительных органов нового уровня организации мероприятий по противостоянию в данной сфере.

ЧАСТЬ II. ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ УПРАВЛЕНИЯ БЕСПИЛОТНЫМ ТРАНСПОРТОМ

Приведем ряд положений, которые сформировали содержание второй части монографии. Первая часть работы отражала особенности использования технологий ИИ в организации противодействия со стороны правоохранительных органов распространению киберпреступлений. В ней показано, что разнообразие киберпреступлений и их абсолютное число имеют четкую тенденцию нарастания, определяющую значимую социальную напряженность.

В сообщении *Cybernews* [436] указано, что одна из групп хакеров слила 16 млрд паролей аккаунтов *Apple*, *Google* и других сервисов. Как отмечалось выше, это было обусловлено несколькими факторами.

Основное влияние связано с цифровизацией человеческого существования. В этой связи приведены систематизированные сведения о теоретических изысканиях и практических приложениях, которые создают представление о существующем положении и перспективах противодействия киберпреступности на основании применения технологий ИИ.

Далее внимание обращено на оценку революционных проявлений в технологических прорывных направлениях. К ним относятся БТС в их различных вариантах реализации (воздушных, наземных, водных).

Активизация этих процессов вызвала необходимость создания в России войск беспилотных систем, о чем заявил Президент РФ В. В. Путин в июне 2025 г. [355]. Актуальность такого решения подтверждается хотя бы одним следующим фактом – российский оптоволоконный *FPV*-дрон «Князь Вандал Новгородский» в зоне специальной военной операции (СВО) от начала применения этой боевой технологии с августа 2024 г. уничтожил различную военную технику НАТО на сумму более \$2 млрд [157].

Дроны, управляемые по оптоволоконному кабелю, среди специалистов считаются революционным оружием. Данный способ управления неуязвим для средств радиоэлектронной борьбы (РЭБ).

Однако следует отметить, что применение такого рода развитой технологии, к сожалению, не только углубляет позитивные достижения в различных сферах (на текущий момент, в основном, в боевом применении). Но отмеченный технологический эксплуатационный спектр, выражающий в настоящее время положительные решения для государственной, правоохранительной, хозяйственной и иным видам деятельности, ведет, к сожалению, в том числе, и к появлению новых противоправных деяний. Данный фактор, в конечном итоге, расширяет и возможности киберпреступлений.

Основу движения в сторону негативных «достижений» во многом определяет еще не изведанный потенциал возможностей техноло-

гий БАС, имеющий как положительные, так и отрицательные аспекты. Отмеченные тенденции, в частности, отмечены в работе В. А. Минаева, А. В. Мокшанцева, А. С. Толпыгина, А. О. Фаддеева [363], отражающей применение технологий ИИ, БАС в топливно-энергетическом комплексе (ТЭК) России.

Речь в ней идет, в том числе, о киберугрозах, которые связаны с проблемами управления беспилотным транспортом. Они могут повлечь негативные последствия – катастрофы, нарушение нормального функционирования критических инфраструктур.

Именно поэтому расширение применения технологий БАС (в том числе, в новом научно-практическом объединении – интеллектуальные транспортные системы – ИТС) делают разработку и создание эффективной системы обеспечения их кибербезопасности остро актуальной задачей, опирающейся на применение технологий ИИ.

Изложению ведущих положений, сформулированных авторами в ходе научно-практических исследований и апробирования предлагаемых подходов и методов, посвящена глава 3. Для более детального ознакомления с ними можно ознакомиться в работах [20; 60; 254–260; 263–264; 363; 399–402].

Их лейтмотивом является обоснование и разработка системы моделей и технологий безопасного управления БАС. Теоретическая проработка указанной предметной сферы позволила сформулировать базовые требования, определившие концептуальную схему единой цифровой платформы БАС.

В главе 4 представлены решения некоторых задач ОВД на основе эксплуатации БАС с применением технологий ИИ. При этом интеллектуальная составляющая акцентируется как метод поддержания системы управления БАС, так и противодействия киберугрозам, направленным на срыв ее нормального функционирования в процессе решения конкретных задач.

Дело в том, что преступный мир серьезно нацелен на использование достижений ИИ для поддержания и сопровождения не только обычных, но и киберпреступлений:

- многие обычные преступления в процессе подготовки или непосредственной реализации, а также удаления или модификации их следов используют несанкционированный доступ к информационным ресурсам и системам управления БТС;

- оптимизация маршрутов БТС для контрабанды и перевозки запрещенных грузов. При этом сбор сведений о расположении патрулей, камер слежения, проводимый программой ИИ, из различных информационных систем обеспечивает работу модели по обходу контрольно-пропускных пунктов и таможенных зон;

- разведка через сеть Интернет с одновременным привлечением БТС для определения оптимальных путей отхода при совершении

краж, грабежей, разбегов, побегов, нахождении «слепых зон» для движения угнанных автомобилей;

- использование дронов для доставки наркотиков и оружия по рассчитанным ИИ маршрутам в обход контролируемых зон или зон с подавлением сигналов возле охраняемых объектов;

- решение задач уклонения от слежки при реализации анти-трекинга маршрутов, подмены координат и генерации ложных маршрутов (метод *GAN – Generative Adversarial Networks*), отправки ложных *GPS*-сигналов для введения в заблуждение систем правоохранительных органов;

- организация криминального контроля за ходом выполнения правоохранительных операций путем взлома систем городского наблюдения, атак на его камеры и датчики. Более того, специально сконструированный ИИ способен генерировать видео для подмены в системах оперативного и наружного видеонаблюдения;

- организация преступлений с использованием аналитической оценки с помощью технологий ИИ и БТС при анализе данных о перевозчиках, клиентах, пассажирах, грузах, районах патрулирования, графиках дежурств и интервалах пересменки, средствах охраны и видеонаблюдения, скорости их реагирования, чтобы найти уязвимые технологические недоработки, выбрать момент и место для совершения преступления.

Совокупность указанных угроз и рисков злоупотреблений выражается: кражами, несанкционированной слежкой, нарушением границ охраняемых зон, доставкой запрещенных грузов и контрабандой, шпионажем и провокационными акциями. Не исключается, что описываемая платформа может стать базой и для других видов преступлений, которые по своему статусу относятся к группам большей тяжести и пока что не нашли распространения в преступной среде.

Рассмотрим пару из них более детально:

- кража личных данных. Для идентификации БАС часто используются персональные данные владельца или оператора транспортного средства: имя, адрес проживания, номер телефона и другие личные сведения. Если они попадут в руки злоумышленников, реально их использование в преступных целях;

- манипуляции с идентификационными метками способны изменять их у беспилотных устройств путем взлома ПО. Это позволяет преступникам, подделывая регистрацию беспилотника, скрываться от ответственности.

Приведенные примеры противоправных деяний в отношении систем управления БАС, к сожалению, не исчерпывают их перечень. Далее рассмотрим еще ряд киберпреступлений в данной сфере.

Глава 3. Система моделей и технологий безопасного управления беспилотным транспортом

3.1. Моделирование киберугроз системам искусственного интеллекта в управлении беспилотным транспортом

В главе приводятся ключевые положения по формированию системы моделей и технологий безопасного, интеллектуального управления беспилотным транспортом [60; 254–260; 263–264; 363; 399–402]. Систематизированы базовые требования к созданию указанной системы, проведена оценка ресурсного обеспечения, обсуждено построение единой цифровой платформы БТС.

Основные цели изложения связаны с формированием систем моделей:

- киберугроз ИИ, участвующему в управлении беспилотным транспортом;
- киберустойчивости и управляемости флотом БТС;
- математической поддержки систем защиты информации БАС.

Как уже отмечалось, всепроникающее использование БТС, к сожалению, не исключает негативные стороны данного процесса. Это касается, прежде всего, активной заинтересованности криминалитета по созданию удобных условий подготовки и совершения различных преступлений.

Создание подобных условий, нередко, обусловлено бесконтрольным применением БТС. В совокупности они могут способствовать реализации широкого спектра противоправных актов – от криминальных эксцессов в сфере киберхулиганств и киберкраж, до опасных деяний террористической, шпионской и диверсионной направленности.

Естественно, что отмеченные особенности и проявления должны быть учтены при формировании комплексного подхода к управлению беспилотным транспортом, призванного обеспечить безопасность, надежность и эффективность транспортных операций.

Возникающие нарушения в процедурах функционирования систем управления (СУ) БТС требуют регулирующих влияний, способных корректировать параметры траекторий и целевого функционала. Пути современных решений таких сложных задач должны быть ориентированы на все более развитые алгоритмические подходы и, в конечном итоге, возлагаются на технологии ИИ.

Вместе с тем, следует помнить, что любая СУ БТС, в том числе выполненная на основе использования ИИ, имеет *уязвимости*. Они могут стать логической или физической основой для создания угроз кибербезопасности.

Сформулируем подход к рассматриваемой проблеме.

Угрозы кибербезопасности – совокупность условий и факторов, создающих потенциальную опасность потери управления БТС, штатного функционирования или получения несанкционированного доступа к нему из-за целенаправленных вредоносных программно-аппаратных воздействий на СУ беспилотного транспорта [254–255; 402].

Как отмечено, в современных условиях важную роль в СУ БТС играют технологии ИИ. Интеллектуальный ресурс используется для обработки информации, подготовки и принятия решений, непосредственного управления транспортным средством. Кроме того, ИИ может использоваться для обучения моделей и алгоритмов, участвующих в СУ БТС.

Вместе с тем, реалии привели к необходимости учитывать уязвимости и формирующиеся на этой основе киберугрозы инфраструктуре, необходимой для СУ беспилотным транспортом. В самом общем виде СУ интегрирует в себе подсистемы связи, хранения и обработки данных, организации и управления движением. В совокупности они обеспечивают ориентирование БТС в пространстве и корректное движение по маршруту.

В качестве подхода для формирования первичного перечня актуальных угроз кибербезопасности в рассматриваемой предметной сфере предлагается ориентироваться на Банк данных угроз (БДУ) ФСТЭК России (ubi.fstec.ru). Включение в указанный перечень типовых угроз для СУ БТС и определение их для каждого этапа ее жизненного цикла создает основу для создания и описания *базовой модели угроз* (БМУ). Исходя из обозначенного подхода, сформирован перечень, содержащий более 30 угроз, которые могут иметь значительный уровень влияния в рамках анализируемых процессов.

Примерами таких угроз являются:

- УБИ.006: Угроза внедрения кода или данных;
- УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации;
- УБИ.011: Угроза деавторизации санкционированного клиента беспроводной сети;
- УБИ.023: Угроза изменения компонентов информационной системы;
- УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию;
- УБИ.031: Угроза использования механизмов авторизации для повышения привилегий;
- УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными;
- УБИ.036: Угроза исследования механизмов работы программы;
- УБИ.047: Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке;

- УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;
- УБИ.069: Угроза неправомерных действий в каналах связи;
- УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;
- УБИ.074: Угроза несанкционированного доступа к аутентификационной информации;
- УБИ.075: Угроза несанкционированного доступа к виртуальным каналам передачи.

Полный перечень угроз формируется путем добавления киберугроз, специфичных для СУ конкретных типов БТС.

Общий алгоритм формирования множества угроз кибербезопасности СУ БТС включает следующее.

1. Начальное формирование перечня киберугроз безопасности информации, циркулирующей в СУ БТС.
2. Структурно-логический анализ множества угроз, систематизация и конкретизация.
3. Верификация множества угроз, опираясь на опыт создания и эксплуатации СУ БТС.
4. Дополнение множества угроз, применяя методы экспертных оценок (полноты множества угроз и причинно-следственных связей).
5. Верификация угроз и дополнение их множества методами имитационного моделирования.
6. Дополнение множества угроз путем применения методов экспертных оценок.
7. Верификация угроз и дополнение множества с применением натуральных экспериментов.
8. Формирование системы киберугроз безопасности защищаемой информации.

Основа построения подобного алгоритма показана в виде последовательного перехода. Но, на самом деле, в процессе его работы возможны и циклические повторы с организацией определенного количества итерационных действий. Они помогают перебрать возможные и представляемые варианты особенностей развития ситуаций в данной предметной области.

Выполнение процедур анализа и обобщения привело к выделению следующих условных групп угроз кибербезопасности БТС.

1. *Безопасность данных:*
 - несанкционированный доступ к данным СУ БТС;
 - фальсификация или подмена данных, связанных с принятием решений по управлению движением БТС (например, маршрутное задание, данные об окружающей среде);
 - внедрение вредоносных программ, которые могут влиять на СУ и приводить к сбоям или утечке информации.

2. Безопасность связи:

- подделка сигналов связи между БТС и СУ;
- внедрение вредоносных программ, нарушающих работу систем связи с целью перехвата управления БТС.

3. Безопасность СУ:

- ошибки в ПО, которые могут привести к сбоям или уязвимостям в СУ;
- ошибки идентификации БТС и элементов, взаимодействующих с СУ;
- уязвимости в аппаратном обеспечении, потенциально допускающие получение несанкционированного доступа к СУ БТС.

4. Инфраструктурные угрозы безопасности, которые могут отражать недостатки в системах:

- организации и управления движением, которые способны создавать сбои или уязвимости в СУ флотом БТС;
- связи, реализующиеся в их потере между БТС и внешней СУ.

5. Безопасность систем ИИ:

- внесение некорректных данных в целях манипуляции системой ИИ, преднамеренного искажения результатов работы и нарушения функционирования СУ БТС;
- ошибки различной природы в моделях обработки данных;
- получение конфиденциальной информации путем обмана системы ИИ;
- закладки в моделях в целях получения несанкционированного доступа к конфиденциальной информации, воздействия на результаты работы системы ИИ.

Естественно, приведенные обобщающие сведения не исчерпывают всего многообразия возможных типов и видов угроз. Поэтому в монографии далее будут выделены и иные частные проявления реальных и потенциальных угроз кибербезопасности.

К сожалению, информационная война, в состоянии которой вынужденно находится Россия, незаконная санкционная политика Запада осложняют доступ к международным базам уязвимостей и индикаторам компрометации, источникам данных об угрозах. Это частично приводит к «ослеплению» средств киберзащиты и не позволяет организовать их оптимальную систему.

Кроме того, к этому добавляются факторы эксплуатации зарубежного ПО и ресурсов Интернет, а также отказов в технической поддержке ИТ-оборудования и обновления ПО со стороны недружественных государств. Очевидно, в этих условиях возрастает вероятность реализации кибератак на СУ, а ее обеспечение необходимой защитой становится иногда непростой задачей.

Поскольку уязвимости в СУ БТС могут быть внесены до начала эксплуатации, ее защиту необходимо обеспечить на всех этапах жизненного цикла:

- формирование требований;
- проектирование;
- разработка;
- ввод в действие;
- эксплуатация;
- вывод из эксплуатации.

В целях учета и систематизации всех факторов угроз безопасности СУ БТС и сфер проявления угроз необходимо разрабатывать модели угроз для каждого конкретного вида и класса БТС. С переходом на новые уровни автономности (УА) транспортных средств появляются новые уязвимости и новые угрозы в СУ. Их обобщенная характеристика объединена в табл. 3.1 [255].

Для учета всех возможных факторов и проявлений угроз безопасности СУ БТС необходимо разработать и поддерживать в актуальном состоянии модели угроз кибербезопасности для каждого вида и класса БТС, с учетом УА БТС. Подчеркнем, как указано в [298], что «информационная безопасность» выступает более широким понятием по отношению к понятию «кибербезопасность», отражающего, прежде всего, воздействия компьютерных атак.

В целях обеспечения системности и единства подходов к решению вопросов кибербезопасности беспилотного транспорта разработана система моделей угроз (МУ) информационной безопасности, адаптированных к конкретным видам, типам и уровням автономности БТС.

Предлагаемая система МУ безопасности включает в себя три вида моделей:

- базовую МУ безопасности информации беспилотного транспорта, основанную на иерархии УА БТС;
- типовые МУ безопасности составных частей СУ БТС;
- частные (по видам БТС) модели угроз (ЧМУ).

Структурная схема системы МУ безопасности для БАС приведена на рис. 3.1. Обозначим типы и классы БАС, приведенные там.

Типы БАС:

- С – самолетный;
- В – вертолетный;
- М – мультироторный;
- К – конвертоплан;
- Г – гибридный.

Классы БАС:

- СЛ – сверхлегкий (до 4 кг);
- Л – легкий (4–30 кг);
- С – средний (30–500 кг);
- Т – тяжелый (свыше 500 кг).

БМУ предназначена для управления информационной безопасностью на стратегическом уровне. Предполагается, что подобное регулирование должно быть юридическим предметом для федерального

органа исполнительной власти, ответственного за безопасность беспилотного транспорта в РФ.

Таблица 3.1

**Угрозы кибербезопасности интеллектуальной системе
управления в зависимости от уровня автономности
транспортного средства [255]**

УА БТС	Характеристика уровня автономности	Угрозы СУ
УА-5	Полная автономность БТС. Пилот не требуется	Уровень 4. Угрозы, связанные с потерей контроля над системами ИИ
УА-4	Полные возможности самостоя- тельного вождения. Пилот кон- тролирует и управляет удаленно по радио- каналам	Уровень 3. Угрозы, связанные с перехва- том управления. Угрозы искажения данных, от ошибок в данных, закладки в моделях ИИ
УА-3	Ограниченные возможности са- мостоятельного вождения, БТС контролируется и при необ- ходимости управляется пилотом	Уровень 2. Угрозы, связанные с возмож- ным влиянием на корректность работы бортовых систем по ка- налам связи
УА-2	Частичная автоматизация и по- мощь водителю. Транспортным средством управляет компьютер	Уровень 1. Угрозы, связанные с работой бортового компьютера, ошиб- ками ПО, уязвимостями аппа- ратных средств
УА-1	Ассистенты пилота помогают в сложных условиях движения, при этом пилот контролирует всё (не предусмотрено автоматизирован- ных систем вождения)	Уровень 0. Угрозы, связанные с некор- ректной работой ассистентов пилота
УА-0	Функций автоматизации и по- мощников нет. Транспортное средство полностью контролиру- ется и управляется пилотом	Угрозы, связанные с работой внешних систем организации и управления движением: светофоры, информационные табло

В определенном, организационном смысле БМУ является мето-
дической основой для:

- разработчиков БТС и разработчиков средств защиты инфор-
мации для БТС;
- организаций, выполняющих работы по проектированию си-
стем контроля и управления беспилотным транспортом;

– организаций, осуществляющих работы по оценке соответствия беспилотного транспорта требованиям защиты информации и его сертификации по требованиям регуляторов.

БМУ содержит описание объекта защиты в части структуры и функциональных характеристик СУ БТС, соответствующих им угроз безопасности информации и модели нарушителя, а также методические рекомендации по разработке типовых и частных МУ. Модель охватывает все стадии жизненного цикла БТС, в том числе – порядок разработки (проектирование, изготовление опытного образца и испытания), производства, эксплуатации и утилизации. Кроме того, она определяет порядок и условия разработки:

- типовых моделей угроз безопасности центров контроля и управления движением для типовых элементов в СУ БТС;
- частных (по видам БТС) моделей угроз объектов (элементов) СУ БТС.



Рис. 3.1. Основы систематизации моделей угроз кибербезопасности беспилотного транспорта [255]

Для поддержания моделей угроз всех видов в актуальном состоянии необходимо проводить их регулярное уточнение при:

- выявлении новых угроз, появлении новых способов и средств их реализации;
- при модернизации системы контроля и управления беспилотным транспортом, изменении структуры и (или) конфигурации ее инфокоммуникаций.

3.2. Моделирование киберустойчивости и управляемости флотом беспилотных транспортных средств

В разделе продолжим представление иерархии моделей, являющихся основой для разработки единой цифровой платформы безопасного интеллектуального управления БТС в современных условиях. После отражения уязвимостей и определения угроз кибербезопасности интеллектуальной поддержки СУ БТС перейдем к основам моделирования процессов киберустойчивости и управляемости, системно расширяемых от единичных экземпляров до флота БТС.

Для оценки способности реагировать и противостоять угрозам кибербезопасности, поддерживать приемлемую функциональность, применяют условную меру, определяемую как *киберустойчивость*. Устойчивая система должна снижать риски кибербезопасности и, в самом общем смысле, минимизировать негативные последствия кибератак [200]. Исходя из данной установки, приведем известное понимание киберустойчивости, а затем дадим его интерпретацию для адаптации к задаче эффективного управления флотом БТС.

Киберустойчивость – это способность компьютерной системы сохранять во времени в установленных пределах значения всех параметров, характеризующих ее способность выполнять свои функции в условиях компьютерных атак, не допускать несанкционированного доступа к вычислительным ресурсам, нарушения целостности информации и нарушения доступности информационных сервисов.

Выразим особенности математического моделирования киберустойчивости и управляемости флотом БТС.

Говоря формальным языком, речь в данной задаче идет о системе θ , состоящей из m объектов (элементов) ϑ_j . Каждый из объектов имеет набор из n свойств (параметров) и характеризуется вектором показателей [402]:

$$Y_{\langle n \rangle}^j = \langle y_1^j, y_2^j, \dots, y_n^j \rangle; i = 1, \dots, n; j = 1, \dots, m. \quad (3.1)$$

Система θ будет считаться киберустойчивой, если выполняется правило:

$$G: \bigcap_{i=1}^n (y_i^j \in \{y_i^d\}) \cong U, \quad (3.2)$$

где $\{y_i^d\}$ – множество допустимых значений показателя качества y_i^j , U – достоверное событие, при условии, что:

$$y_i^j = f(i, j; t) * g(i, j; t), \quad (3.3)$$

где функции $f(i, j; t)$ – противодействие кибератаке, $g(i, j; t)$ – кибератака, в отношении j -го объекта, направленная на изменение его -го параметра (свойства).

При этом система достигает целей W^θ , а также не теряются эмерджентные свойства системы Q^θ , т. е.:

$$\begin{cases} W^\theta = \max_t P_{\text{дц}}(Y_{\langle n \rangle}^j; t) \\ Q^\theta(t) = Q^\theta(t_0) = \text{const} , \\ Q^\theta \neq \sum_{j=1}^m Y_{\langle n \rangle}^j \end{cases} \quad (3.4)$$

где t_0 – начало эксплуатации системы, $P_{\text{дц}}$ – вероятность достижения поставленной цели.

Определив формальное описание, обратимся к пониманию системы контроля и управления флотом (СКУФ) БТС. Она, по-нашему мнению, имеет иерархическую структуру с тремя уровнями управления (табл. 3.2).

Таблица 3.2

Иерархия объектов системы СКУФ БТС

Уровень	Органы управления
Стратегический	Федеральный центр контроля и управления
Тактический	Региональный (ведомственный) центр контроля и управления
Оперативный	Стационарные и подвижные пункты контроля и управления. Группировка БТС. БТС

В современных условиях развития транспортной отрасли особую значимость приобретает вопрос *безопасного управления* беспилотным транспортом. Создание эффективной системы моделей и технологий для управления БТС на основе использования достижений ИИ становится ключевым фактором успешного внедрения инновационных решений в транспортную инфраструктуру.

Принципиальным инновационным направлением считается потребность государства (рис. 3.2) в обосновании, разработке, финансировании и создании распределенной защищенной автоматизированной системы контроля и управления движением беспилотных транспортных средств (АСКУД БТС) [399].



Рис. 3.2. Иерархия построения центров и пунктов контроля и управления БВС [399]

Эмерджентные свойства системы в данном случае – способность выполнять функции управления флотом БТС на каждом уровне управления, $Q^{\theta} = \{Q^C, Q^O, Q^T\}$.

Приведем краткую характеристику основных составляющих отмеченных уровней управления в целях понимания функциональных особенностей и их вертикальных взаимосвязей.

На *стратегическом* уровне управления $Q^C = \{Q_1^C, Q_2^C, \dots, Q_{\|Q^C\|}^C\}$, $\|Q^C\|$ – мощность множества Q^C , это:

- установление стандартов и правил эксплуатации БТС;
- мониторинг и анализ данных о состоянии движения БТС в масштабах страны;
- координация работы региональных центров контроля и управления движением;
- реагирование на чрезвычайные ситуации масштаба страны, связанные с беспилотным транспортом;
- взаимодействие с международными организациями и странами по вопросам беспилотного транспорта;
- разработка и внедрение новых технологий и инноваций в сфере беспилотного транспорта.

На *тактическом* уровне управления $Q^O = \{Q_1^O, Q_2^O, \dots, Q_{\|Q^O\|}^O\}$, $\|Q^O\|$ – мощность множества Q^O , это:

- мониторинг и анализ данных о состоянии движения БТС в регионе;
- регулирование движения БТС в соответствии с региональными правилами и нормами;
- координация работы мобильных пунктов управления воздушным движением;

- организация взаимодействия между различными ведомствами и службами в регионе, связанными с беспилотным транспортом;
- реагирование на чрезвычайные ситуации регионального масштаба, связанные с беспилотным транспортом;
- взаимодействие с федеральным центром контроля и управления движением по вопросам координации и обмена информацией;
- разработка и внедрение региональных программ и проектов в области беспилотного транспорта;
- организация и проведение научных исследований и испытаний новых технологий и инноваций в сфере беспилотного транспорта на региональном уровне;
- оказание технической поддержки и консультаций региональным операторам беспилотного транспорта.

На *оперативном* уровне управления $Q^T = \{Q_1^T, Q_2^T, \dots, Q_{\|Q^T\|}^T\}$, $\|Q^T\|$ – мощность множества Q^T , это:

- контроль и управление движением БТС на определенном маршруте;
- обмен данными и информацией с участниками движения, включая другие БТС и стационарные пункты управления;
- выполнение команд и распоряжений от вышестоящих органов управления;
- дистанционное управление отдельными БТС в экстренных ситуациях и в случаях необходимости;
- диагностика и устранение неполадок в работе БТС;
- обеспечение безопасности совместного движения БТС;
- контроль соблюдения правил движения и требований операторов беспилотного транспорта.
- своевременное оповещение вышестоящих органов управления о возникновении аварийных ситуаций или других происшествий.

Естественно, приведенные перечни функций СКУФ БТС не являются исчерпывающими, а в конкретных СУ определяются множеством ресурсных и эксплуатационных факторов.

Обозначив подходы к формированию моделирования киберустойчивости и управляемости флотом БТС, расширим представление о возможностях дальнейшего изыскания. В частности, принимаем во внимание, что кибератака – это подготовленное мероприятие.

Оно с силу этого имеет цель, объект и сценарий атаки, средства реализации и последствия, носит процессно-функциональный характер. Поэтому, для оценки киберустойчивости СКУФ БТС могут применяться *методы функционального моделирования*.

Рассмотрим последовательно все аспекты обеспечения кибербезопасности в контексте процесса подготовки и реализации атаки. В общем виде указанная атака может быть представлена совокупностью фаз и мероприятий, которые объединены в табл. 3.3.

**Фазы и мероприятия подготовки и реализации
кибератаки на ИИ СКУФ БТС**

№	Фаза	Мероприятия
1	Разведка	Сбор данных, анализ уязвимостей, идентификация и выбор объекта атаки
2	Оснащение (вооружение)	Выбор средств реализации атаки, подготовка вредоносного ПО (ВПО – <i>Malware</i>) средств вычислительной техники и зараженных файлов, носителей информации, разработка сценария атаки
3	Доставка	Донесение вредоносного контента до объекта атаки по сети (почтовое сообщение, <i>web</i> -сайты и т. д.) или на носителе информации
4	Заражение	Запуск вредоносного кода, используя уязвимости объекта атаки, с последующим заражением компьютера или всей вычислительной сети
5	Установка (внедрение)	Открытие удаленного доступа для скрытного получения обновлений ВПО, обновление ВПО
6	Получение управления	Получение обновлений ВПО извне, получение управляющих команд для достижения поставленных целей
7	Выполнение неправомерных действий – атака	Перехват управления, реализация замысла нарушителя, кража информации, шифрование файлов, подмена или порча данных
8	Удаление следов Несанкционированного воздействия	Удаление и очистка журналов событий
9	Удаление следов заражения	Удаление ВПО, закрытие портов

Уточним определение *объекта защиты*.

К *объектам защиты*, определяемым согласно [9], относятся:

- информация, содержащаяся в СКУФ БТС;
- данные информационного и командно-сигнального трактов взаимодействия;
- аппаратные технические средства;
- средства и системы связи и передачи данных;
- технические средства обработки информации;
- программные средства и обеспечение;
- информационные технологии;
- средства защиты информации.

Цель атаки определяется намерениями нарушителя, которым может быть иностранное государство, организация, физическое лицо. Каждая категория нарушителей имеет различные потенциальные воз-

возможности проведения атаки. Цель атаки определяет порядок реализации и средства.

События кибербезопасности, приводящие с высокой вероятностью к угрозе потери управления БТС, рассматриваются как инциденты кибербезопасности. Для них определены следующие фазы [45] (табл. 3.4).

Таблица 3.4

Фазы и мероприятия подготовки и реализации кибератаки

Фаза	Мероприятия
Идентификация	Идентификация инцидента. Категоризация инцидента
Локализация	Предотвращение распространения
Уничтожение	Устранение угрозы
Восстановление	Восстановление работоспособности
Пост-анализ	Расследование: установление фактов и хронологии. Документирование, занесение в базу знаний

Меры воздействия и противодействия составляют функциональную модель процессов обеспечения киберустойчивости и управления флотом БТС. На основании указанного подхода сформирована система математических моделей (ММ) (рис. 3.3). Здесь каждой ММ в соответствие должна быть поставлена ключевая метрика.

В соответствии с этой системой строится методика сохранения управляемости флотом БТС, которая позволяет оптимизировать свойства системы и повышать киберустойчивость за счет:

- повышения скорости реакции на кибератаку;
- повышения гибкости и адаптивности системы;
- минимизации негативных последствий кибератаки;
- повышения надежности и скорости восстановления.

Состояние киберустойчивости не постоянно во времени. Кибератаки в любой момент могут дестабилизировать функционирование СУ БТС. Поэтому основная задача киберзащиты состоит в том, чтобы сохранять управляемость БТС и флотом БТС на базе системного подхода к защите информации и инфраструктуры СУ БТС от киберугроз.

Предложенная система моделей киберустойчивости позволяет проводить оценку рисков, защищенности системы, последствий кибератак и управлять кибербезопасностью. Для этого она должна быть интегрирована в качестве аналитического инструмента во множество

мероприятий процесса совершенствования системы защиты информации в рассматриваемой сфере, восстановления после сбоев, системы предотвращения вторжений.

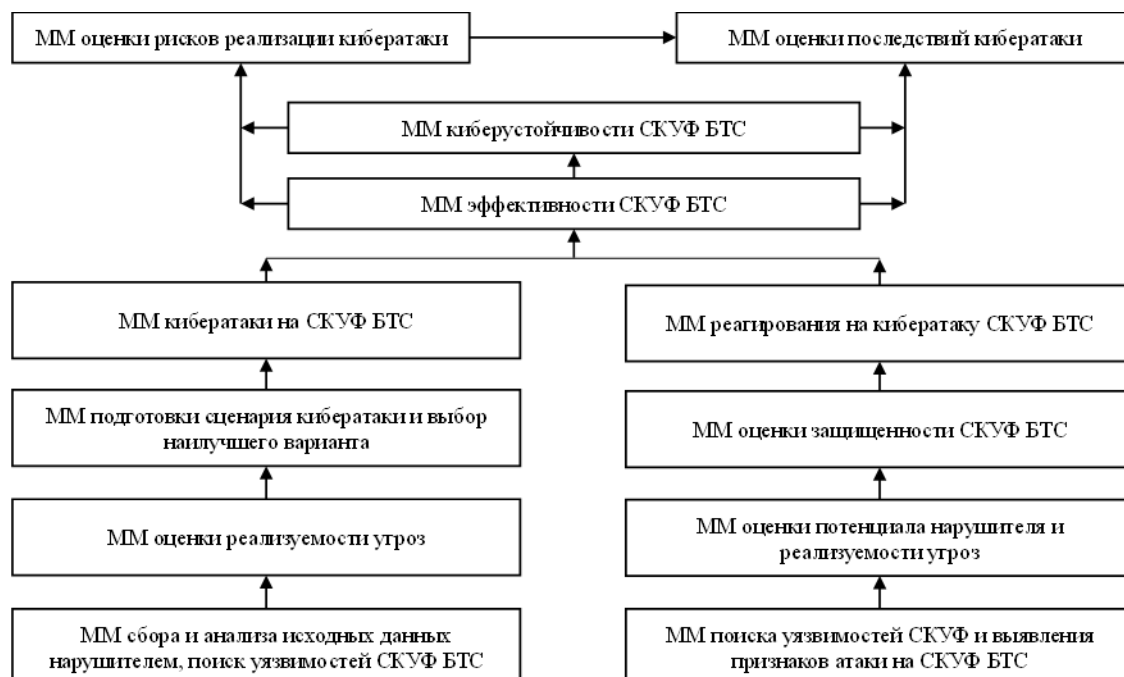


Рис. 3.3. Система математических моделей оценки киберустойчивости СКУФ БТС [255]

3.3. Классификация моделей безопасного управления беспилотным транспортом

В современных условиях особую значимость приобретает вопрос *безопасного управления* беспилотным транспортом. Создание эффективной системы моделей и технологий управления БТС на основе использования достижений ИИ становится здесь ключевым фактором успешного внедрения инновационных решений в транспортную отрасль. Как уже отмечалось, инновационным направлением при этом выступает создание распределенной защищенной автоматизированной системы контроля и управления движением беспилотных транспортных средств (АСКУД БТС) [399].

Оценка этой задачи дает основание отнести ее к уровню глобальной, имеющей самостоятельные направления, которые объединяться в целях достижения интегрального замысла.

Принципиально важную часть такого замысла составляет *функционал защиты информации, реализованный на использовании технологий ИИ*. Данный функционал на физическом, логическом и технологическом уровне напрямую определяет эффективность и качество работы всего комплекса АСКУД БТС.

Разработкой и созданием ядра обозначенной глобальной системы занялся объединенный творческий коллектив Московского университета МВД России имени В. Я. Кикотя, МГТУ имени Н. Э. Баумана и компании «Тактические авиасистемы» (Т-АВИАС), направив свои усилия на построение *цифровой платформы контроля и управления движением БТС со встроенными средствами защиты информации*. Далее рассмотрим основные результаты, полученные указанным коллективом, их апробации на ведущих форумах страны.

Система моделей и технологий управления беспилотным транспортом реализуется в комплексном исследовании, направленном на обеспечение безопасности, надежности и эффективности его операций. Ключевыми аспектами функционирования такой системы являются:

- безопасность движения – минимизация рисков аварий и предотвращение внештатных ситуаций;
- надёжность управления – обеспечение бесперебойной работы в различных условиях эксплуатации;
- оптимизация процессов – эффективное планирование маршрутов и снижение ресурсных затрат;
- технологическая интеграция – использование современных решений в области ИИ и кибербезопасности;
- адаптивность системы – возможность масштабирования и подстройки под различные типы транспорта;
- нормативное соответствие – соблюдение стандартов безопасности и упорядочение сертификации.

Создание системы включает этапы:

- 1) определение целей и требований к управлению;
- 2) разработка иерархической системы моделей;
- 3) интеграция современных технологий;
- 4) формализация и стандартизация решений при реализации моделей и технологий;
- 5) тестирование и валидация;
- 6) внедрение и эксплуатация.

Разработка и внедрение системы моделей и технологий для безопасного управления беспилотным транспортом представляет собой стратегически важное направление развития транспортной отрасли. Комплексный подход к созданию такой системы позволяет обеспечить гибкое, надёжное и эффективное управление БТС, что открывает новые возможности для развития современной транспортной инфраструктуры.

Важной при построении системы безопасного управления беспилотным транспортом является задача классификации методов и технологий, решаемая в целях:

- обеспечения комплексного подхода к проектированию СУ;
- упрощения выбора оптимальных технических решений;

- стандартизации требований к безопасности;
- ускорения процесса разработки перспективных СУ.

Сделаем попытку систематизировать базовые критерии и признаки классификации.

Методы и средства управления:

- автономность – управление осуществляется без участия оператора на основе алгоритмов ИИ и обработки данных сенсоров;
- дистанционность – управление производится оператором через каналы связи;
- гибридность – сочетание автоматического и дистанционного управления с их выбором в зависимости от ситуации.

Функциональная направленность методов:

- планирование маршрутов и навигации;
- обнаружение и предотвращение столкновений;
- мониторинг и диагностика состояния;
- обеспечение кибербезопасности.

Технологии обеспечения безопасности:

- использование сенсорных систем – лидары, радары, камеры;
- алгоритмы ИИ при обработке данных и подготовке решений;
- резервные, отказоустойчивые системы;
- системы кибербезопасности – шифрование, аутентификация.

Уровень автоматизации (автономности):

- полностью автономные системы – транспортное средство самостоятельно решает все задачи по управлению;
- частично автономные системы – БТС выполняет самостоятельно ограниченный набор функций;
- дистанционное управление.

Технологическое обеспечение:

- сенсорные технологии (лидары, радары, камеры);
- коммуникационные технологии (V2X, 5G);
- вычислительные платформы;
- технологии ИИ.

Области применения:

- воздушный транспорт;
- наземный транспорт;
- водный транспорт;
- подводный транспорт.

Степени интеграции:

- монофункциональные системы;
- комплексные интегрированные системы;
- модульные системы.

Основные задачи классификации включают:

- систематизацию существующих методов управления;
- выявление взаимосвязей между различными технологиями;
- определение перспективных направлений развития;

- формулировку требований к каждой категории систем;
- разработку рекомендаций по выбору оптимальных решений.

Практическая значимость классификации заключается в создании унифицированной системы описания методов управления, упрощении процесса разработки новых систем, повышении эффективности внедрения беспилотного транспорта, улучшении стандартов безопасности и ускорении процесса сертификации СУ.

Системная классификация методов и технологий безопасного управления беспилотным транспортом позволит создать методологическую основу для развития отрасли, совершенствования существующих СУ, создания новых технологических решений и обеспечения высокого уровня безопасности эксплуатации беспилотного транспорта. Предназначение классификации – служить инструментом для разработчиков, исследователей и регуляторов в процессе создания и внедрения СУ беспилотным транспортом нового поколения.

Определим принципы систематизации знаний, проведем классификацию множества моделей и технологий безопасного управления беспилотным транспортом. Основным предположением является: структура СУ предполагает управление миллионами БТС, имеет иерархическую структуру, на каждом уровне которой свои методы и технологии.

Для выделения признаков и определения критериев отнесения объектов к конкретным классам, определим множества *объектов классификации*. Они включают в себя:

- объекты управления;
- субъекты управления;
- средства управления;
- средства контроля достижения целей управляющих воздействий;
- ресурсное обеспечение.

Далее на базе указанных представлений обратимся к основным результатам математического моделирования интеллектуального обеспечения безопасности информации БТС.

3.4. Моделирование защиты беспилотных авиационных средств

Приведем основные этапы создания математической модели, ориентированной быть инструментальным средством для анализа угроз и выработки стратегии защиты информации, циркулирующей в контурах: между БВС, БВС и пунктами управления. Модель должна служить обоснованием при выработке комплекса мер по снижению вероятности несанкционированного вмешательства в СУ БАС и проведении количественной оценки принятых мер [264].

Говоря о флоте (группировке) БАС, подчеркнем, что обеспечение и поддержание его устойчивой, слаженной работы должно опираться на надежное интеллектуальное обеспечение информационной безопасности БАС. При этом в контур защиты должны входить такие элементы СУ, как [258]:

- различные данные;
- программные ресурсы и приложения;
- каналы связи и коммуникации;
- оборудование бортовых комплексов и наземных пунктов управления (НПУ).

Обобщенная модель системы защиты информации.

Общими целями моделирования процессов и системы защиты информации (СЗИ) выступают:

- достижение наибольшей эффективности механизмов безопасности;
- соблюдение баланса между организационными и техническими мерами защиты;
- оптимальные выбор и применение технических средств (ТС) и ПО при построении СЗИ;
- детальная проработка структуры СЗИ для охвата процедурами безопасности всей информации, хранимой и циркулирующей в бортовых информационных системах БАС, а также средствах вычислительной техники НПУ;
- определение основных технико-экономических показателей СЗИ с учетом изменяющихся требований к мерам защиты и для различных вариантов эксплуатации БАС.

Основными классификационными признаками, которые учтены при построении модели, были следующие:

- характер и особенности моделируемых процессов;
- способ моделирования;
- масштаб модели.

Приведем самую общую модель процесса защиты информации в информационной системе в терминах теории графов. В основе модели лежит изначальное положение о необходимости рассмотрения, по крайней мере, двух множеств:

$T = \{T_j\}$ – множество угроз;

$O = \{O_i\}$ – множество объектов защиты.

Они формируют множество отношений угроза-объект $\{T, O\}$. Цель защиты заключается в перекрытии всех возможных рёбер в этом графе. Для этого вводится СЗИ, состоящая из элементов множества $D = \{D_l\}$ [167].

В результате получаем трёхдольный граф $\{T, D, O\}$ (рис. 3.4).

На рис. 3.4 приняты следующие обозначения:

$\{T_j\}$ – j -я угроза информационной безопасности, дестабилизирующий фактор воздействия на объект защиты;

$\{O_i\}$ – i -й объект защиты (информация);

$\{D_l\}$ – l -е средство защиты информации;

P_{ijk} – вероятность негативного воздействия j -й угрозы на i -й объект в его k -м состоянии без применения средств защиты;

P_{ijlk} – вероятность негативного воздействия с учётом нейтрализации воздействия j -й угрозы на i -й объект в его k -м состоянии с применением l -го средства защиты;

P_i – вероятность требуемой (гарантируемой) защиты i -го объекта.

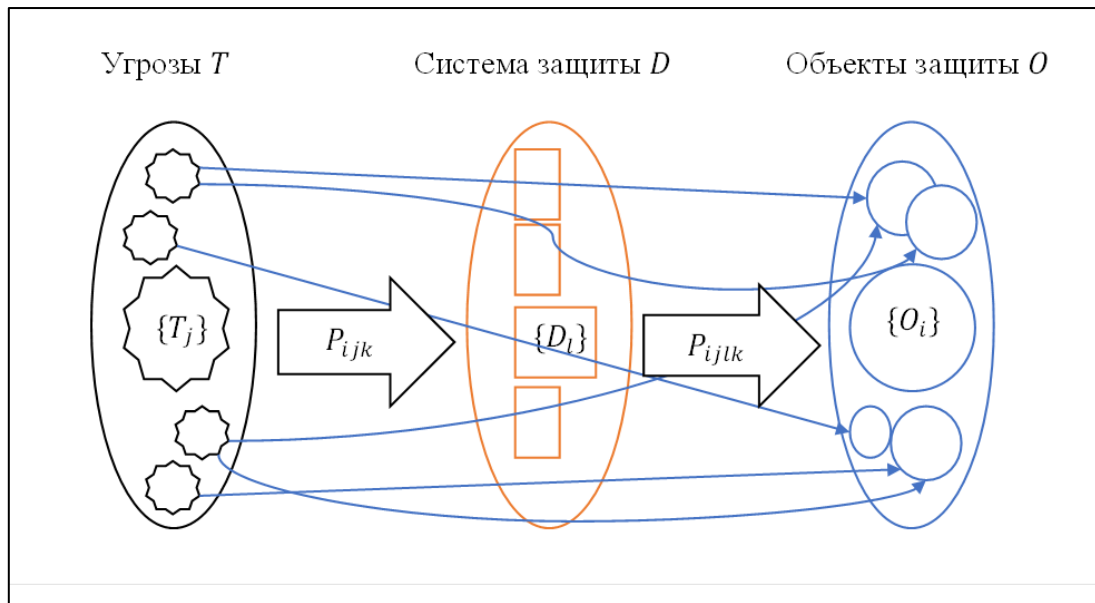


Рис. 3.4. Обобщенная модель процесса защиты информации [264]

Итак, в соответствии с особенностями рассматриваемой модели [167] обработка информации на объекте $\{O_i\}$ осуществляется в условиях воздействия угроз (дестабилизирующих факторов) $\{T_j\}$. Для противодействия угрозам информации могут использоваться средства защиты $\{D_l\}$, оказывающие нейтрализующее воздействие на дестабилизирующие факторы.

В общем случае на объект защиты в любом его состоянии может воздействовать множество угроз. При этом характер и уровень воздействия одних факторов может не зависеть от других. Однако могут существовать и взаимозависимые факторы.

Точно также и средства защиты могут быть как независимыми, так и взаимозависимыми.

Конечно, при разработке моделей процессов защиты информации необходимо учитывать не только воздействие угроз и средств защиты, но и их взаимное влияние друг на друга. Для этого нужна разработка более детальной модели.

Однако и частные модели могут хорошо служить для изучения безопасности отдельных элементов или процессов. К их числу можно отнести модели:

- описывающие конкретные угрозы и их совокупное негативное воздействие;

- нарушителей для различных способов реализации атак;

- информационных потоков, циркулирующих в системе.

Преимущество формального описания заключается в том, что оно минимизирует возможность возникновения противоречий в политике безопасности.

Частные модели способствуют выявлению ключевых характеристик в обеспечении безопасности информации и систем их обработки. К таким характеристикам относятся:

- важность информации, которая определяется уровнем значимости в случае её раскрытия или потери;

- степень опасности угроз, которая позволяет определить как актуальные, так и наиболее критичные угрозы;

- уровень угрозы со стороны нарушителя, позволяющий выявить наиболее опасного злоумышленника;

- уровень защищённости отдельных компонентов, который позволяет обнаружить и контролировать наиболее уязвимые элементы систем обработки данных или наименее надёжные механизмы защиты;

- эффективность политики безопасности информационной системы, которая позволяет сравнить их и определить оптимальную.

Дальнейшее развитие модели включает введение двух дополнительных элементов [167]:

- $V\{V_m\}$ – множество уязвимостей;

- $B\{B_n\}$ – множество барьеров.

Таким образом, модель будет состоять из пяти элементов $\{T, O, D, V, B\}$ (рис. 3.5).

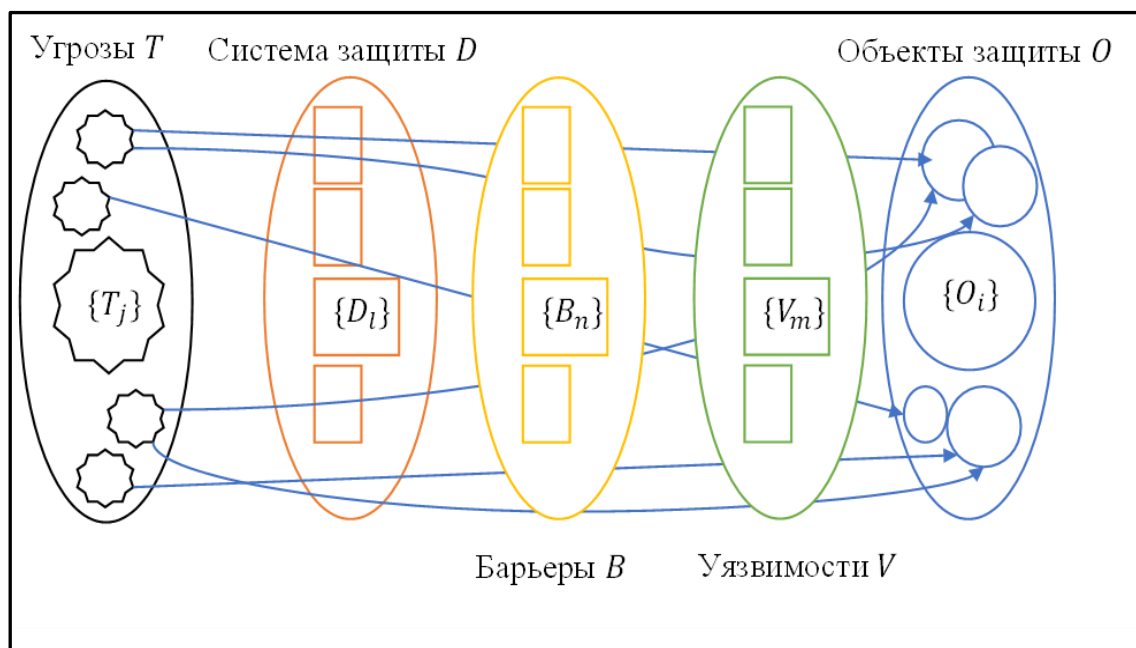


Рис. 3.5. Уточненная модель с учетом уязвимостей [264]

Оценка эффективности системы защиты информации.

Практический интерес вызывает понимание того, какой результативности достигают принятые меры защиты информации. Соответствующую оценку эффективности системы защиты можно осуществить, следуя алгоритму (рис. 3.6).

Шаг 1: Оценка актуальных угроз информационной безопасности.

Шаг 2: Оценка устойчивости системы защиты от угроз информационной безопасности.

Шаг 3: Вычисление коэффициента эффективности.

Шаг 4: Уточнение модели угроз/доработка системы защиты.

Процесс, изображенный на рис. 3.6, является циклическим, который можно ограничить количеством итераций по поиску решения на основе существующих средств и мер защиты. Выполнение выраженных при этом требований является обязательным условием для последующего перехода к разработке новых средств защиты, соответствующих актуальным угрозам и требованиям.

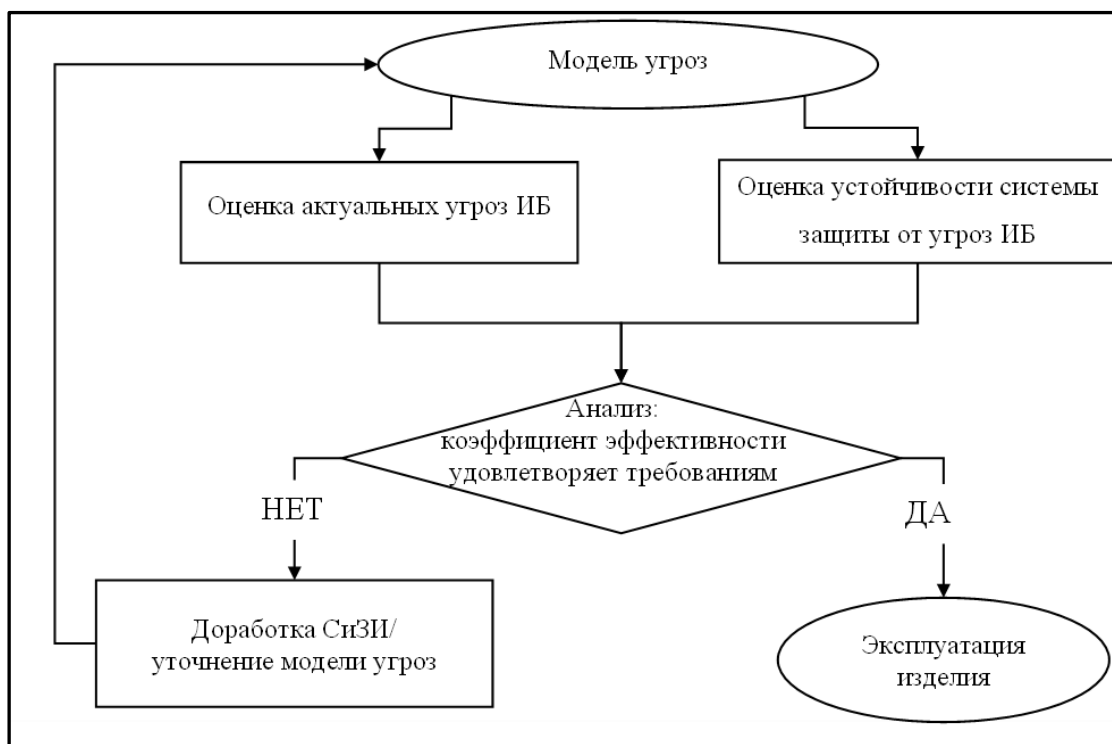


Рис. 3.6. Алгоритм оценки эффективности систем защиты информации [264]

Реализуемость требований, предъявляемых к системе защиты информации, характеризуется вероятностью достижения цели – $P_{ДЦ}^{ВТ}$. Она включает полный набор средств защиты от потенциальных угроз, или достаточный (соответствующий набору актуальных угроз) критерий пригодности $G: P_{ДЦ}^{ТР} \leq P_{ДЦ}^{ВТ}$.

Здесь и далее индексы оценки вероятностей:

- ДЦ – достижение цели;
- ВТ – выполнение требований;
- ТР – требуемый уровень вероятности ДЦ.

Для проведения оценки реализуемости требований необходимо определить вероятность достижения цели $P_{ДЦ}^{ВТ}$, с учетом возможностей производства, научно-технической и ресурсной базы.

Согласно формуле полной вероятности, имеем:

$$P_{ДЦ}^{ВТ} = P(ГН|ГФ \cap ГП)P(ГФ \cap ГП), \quad (3.5)$$

где ГФ – готовность финансово-экономической, ГН – научно-технической и ГП – производственно-технологической базы.

Математическая модель обеспечения безопасности информации БАС позволяет обеспечить системный подход к формированию мер противодействия.

Рассмотрим систему управления БАС как объект с входными и выходными сигналами, подверженный возможным атакам. Пусть:

$X(t)$ – вектор входных команд управления в момент времени t ;

$Y(t)$ – вектор выходных состояний БАС;

$A(t)$ – вектор возможных атак.

Общий вид модели можно представить как:

$$Y(t) = F(X(t), A(t)), \quad (3.6),$$

где F – функция перехода системы.

Для обеспечения безопасности необходимо минимизировать влияние $A(t)$ на выходную переменную $Y(t)$.

Цель системы защиты – минимизация вероятности перехода в состояние компрометации безопасности.

Методы защиты.

Исходя из анализа угроз и с учётом математической модели обеспечения безопасности, приведём основные мероприятия, проведение которых поможет минимизировать угрозы информационной безопасности БАС.

1. Защита коммуникаций.

Шифрование данных.

Для защиты информации, передаваемой между самими БАС, БАС и НПУ необходимо применять современные алгоритмы шифрования, например, такие как AES-256 и RSA.

Защита радиоканала.

Чтобы предотвратить глушение и подмену сигнала, необходимо применять частотное сканирование и смену частот (*frequency hopping*).

Для проверки подлинности отправителя данных следует использовать протоколы аутентификации, такие как *Kerberos*, *CHAP*, *SSH* и *TLS/SSL*.

Сети Mesh и Ad-hoc.

В таких сетях важно внедрить криптографические ключи, динамическое управление топологией сети и механизмы обнаружения аномалий.

2. Аутентификация и контроль доступа.

Многоуровневая аутентификация.

Для доступа к СУ БАС необходимо использовать сертификаты, пароли и двухфакторную аутентификацию (2FA).

Роли и права доступа.

В зависимости от роли оператора (например, администратор, наблюдатель) предоставляется соответствующий ограниченный доступ к управлению группировкой.

Бортовая идентификация.

Для исключения возможности подключения посторонних устройств необходимо использование механизмов взаимной аутентификации между БАС.

3. Защита ПО.

Обновление ПО.

Необходимо регулярное обновление ПО СУ БАС для устранения уязвимостей. Для проверки подлинности обновлений необходимо применять цифровые подписи.

Антивирусные меры.

Прошивки и сторонние модули должны проверяться на наличие вредоносного кода.

Безопасная разработка.

При разработке ПО для управления группировкой необходимо использовать принципы безопасного программирования, например, OWASP (Open Worldwide Application Security Project).

4. Защита данных.

Шифрование данных на борту.

Данные, хранящиеся в бортовых информационных системах БАС (например, полетное задание, навигационные и картографические данные, фотографии, видео), должны быть зашифрованы.

Безопасное удаление данных.

В случае захвата дрона данные должны быть уничтожены автоматически.

Облако или локальные серверы.

Данные, полученные БАС, должны храниться в защищённом облаке или на локальном сервере с доступом через защищённые каналы.

5. Противодействие атакам.

Обнаружение и предотвращение атак (IDS/IPS).

Для мониторинга трафика между БАС необходимо внедрить системы обнаружения и предотвращения атак.

Противодействие глушению GPS.

Инерциальные навигационные системы (INS) и альтернативные методы позиционирования, такие как визуальная или радионавигация позволяют обеспечить навигацию при обнаружении глушения сигналов геопозиционирования.

Защита от подмены сигнала (spoofing).

Для защиты применяются средства криптографии – электронной подписи сигналов GPS или других данных позиционирования.

Анализ поведения.

Для выявления аномальных действий в поведении БВС используются алгоритмы машинного обучения.

6. Физическая безопасность.

Необходимо ограничить физический доступ к БВС и их компонентам, установить датчики, фиксирующие попытки вскрытия корпуса БВС. При несанкционированном вскрытии корпуса БВС автоматически должно производиться уничтожение данных.

7. Мониторинг и аудит системы.

Регистрация (логирование) событий и анализ логов.

Все действия в системе необходимо автоматически фиксировать в специальном журнале событий, который в дальнейшем анализируется на предмет подозрительных событий. Необходим периодический анализ логов для выявления подозрительных действий.

Мониторинг в реальном времени.

Используются системы непрерывного наблюдения за состоянием сети и дронов.

8. Планирование на случай инцидентов.

Планы реагирования.

Для всех операторов разрабатываются четкие инструкции на случай кибератак, потери связи или захвата БАС.

Резервные системы.

На случай отказа основной СУ создаются резервные каналы связи и механизмы управления.

Регулярно проводятся тесты на устойчивость системы к различным типам атак.

В завершении раздела отметим, что предложенный подход создает эффективную основу для аналитического исследования, комплексной оценки рисков и последующей выработки решений. Они направлены на минимизацию вероятности несанкционированного вмешательства в управление БАС, которое в очень динамично меняющихся современных условиях становится особо актуальным из-за активного применения в боевых обстоятельствах, подготовки и совершения различных видов правонарушений. Таким образом, применение данной модели способствует повышению уровня информационной безопасности и снижает риски эксплуатации БАС в условиях современных киберугроз.

3.5. Цифровая платформа беспилотных транспортных средств

Как отмечено выше, логическим завершением научно-практических изысканий является разработка и создание ядра системы *безопасного управления* беспилотным транспортом – АСКУД БТС. Ядро системы обозначено как *Цифровая платформа контроля и управления движением БТС со встроенными средствами защиты информации*.

Основные установки выполнения проекта в целом направлены на обеспечение:

- полного контроля трафика БТС в границах зон социальных объектов, защищаемых объектов критической инфраструктуры;
- киберустойчивости БТС и защиты от их неправомерного применения;
- контроля выполнения маршрутных (полетных) заданий;
- выявления и предотвращения аномалий в поведении БТС;

– соответствия БТС законодательству РФ и требованиям регуляторов по безопасности их применения.

Для этого требуется создание сети центров контроля и управления движением БТС, обеспечивающих ситуационную осведомленность и поддержку управленческих решений.

Обратимся к изложению основных теоретических и прикладных положений, разработанных указанным выше коллективом авторов в целях создания отмеченной Цифровой платформы. Существо полученных при этом результатов можно представить, например, в следующих работах [60; 254–260; 263–264; 363; 399–402].

Один из основных нормативно-правовых документов страны в рассматриваемой области – «Стратегия развития беспилотной авиации Российской Федерации на период до 2030 года и на перспективу до 2035 года» – предусматривает [21]:

– разработку скоростных транспортных БАС для региональных и межрегиональных перевозок, в том числе – применительно к условиям Арктики;

– развитие сетевой структуры разработки и производства БАС;

– создание системы идентификации, контроля и управления БАС;

– формирование системы обеспечения комплексной безопасности применения БАС и их ключевых компонентов, включая системы ИИ;

– интеграцию систем управления БАС с системами управления пилотируемой авиации.

Для решения указанных задач требуется создать инфраструктуру, обеспечивающую полеты БАС, разработать стандарты и нормативные документы, заместить импортное оборудование и ПО, зачастую не сопрягаемые друг с другом.

Возникает необходимость создания системы контроля и управления [255], основой которой выступает Цифровая платформа БАС, обеспечивающая:

– создание и запуск в практическую деятельность типовых центров контроля и управления БАС;

– интеграцию БАС с информационно-управляющими системами пилотируемой авиации;

– создание федеральной системы контроля и управления движением БВС;

– интеграцию циркулирующих данных с системами учета БАС, планирования полетов БАС;

– создание маркетплейса, где участники могут оформить свои отношения друг с другом: приобрести (взять в аренду) БАС, сдать (продать полетное время) БАС; застраховать БАС и ответственность перед третьими лицами; подать заявку в подразделение организации воздушного движения и согласовать полет; узнать об ограничениях движения в воздушном пространстве;

- регистрацию и идентификацию БАС, расчет оптимального плана полета и согласование полетного задания;
- кибербезопасность БАС, защиту информации и персональных данных участников информационного взаимодействия;
- контроль исполнения полетного задания;
- моделирование поведения БАС и воздушной обстановки с применением цифровых двойников.

По прогнозам [278], в 2026 г. в воздушном пространстве будет постоянно находиться более 2 млн БВС. Бесконтрольное применение БВС создает риски возникновения чрезвычайных ситуаций и совершения противоправных действий, включая проявления терроризма, многих киберпреступлений.

Таким образом, цифровая платформа становится центральным элементом, который:

- обеспечит построение федеральной сети центров контроля и управления БАС на единых системотехнических принципах;
- объединит указанные центры в общую информационно-аналитическую систему контроля и управления беспилотным транспортом.
- обеспечит быстрое создание, запуск и масштабирование системы, интеграцию с существующими интеллектуальными системами управления транспортом, построение единого пространства кибербезопасности.

Важность решения указанных задач возрастает в связи с появлением полностью автономных или управляемых БАС с минимальным участием оператора. Киберустойчивость таких БАС в достаточной мере не изучена, чтобы гарантировать их безопасное применение в современных мегаполисах и защиту критически важных объектов.

В ходе авторских исследований, направленных на формирование требований к цифровой платформе и научно-технического задела для ее создания, решены задачи анализа:

- существующих и перспективных технических средств и информационных систем контроля и управления движением БАС, перечня критически важных технологий, необходимых для создания цифровой платформы БАС;
- систем и средств организации защищенного информационно-технического взаимодействия (ИТВ) и обеспечения киберустойчивости БАС и инфраструктуры;
- систем ИИ для управления БАС и выявления аномалий в их поведении;
- нормативно-правовых актов и нормативно-методической документации в области кибербезопасности БАС;
- угроз кибербезопасности БАС;
- модели угроз, а также нарушителей кибербезопасности БАС;
- мер по защите от угроз кибербезопасности БАС;

- построения кроссплатформенного (в отношении аппаратных и операционных систем) ядра цифровой платформы БАС;
- создания макета типового центра контроля и управления движением БАС;
- разработки технического задания на опытно-конструкторскую работу по исследованию и созданию сети центров контроля и управления движением БАС;
- правового регулирования в области кибербезопасности БАС.

Важнейшими задачами выступают также:

- разработка моделей и методов ИИ для выявления аномалий в движении БАС;
- организация управления крупными скоплениями БАС в реальном времени;
- обеспечение обнаружения и идентификации БАС с использованием нейронных сетей;
- управление воздушным движением БАС, подготовкой принятия решений;
- повышение уровня безопасности полетов БАС.

С учетом изложенного определим триединую цель разработки цифровой платформы БАС:

- обоснование инструментария для создания типовых центров контроля и управления движением БАС;
- построение распределенной защищенной информационно-аналитической системы контроля и управления движением БАС;
- интеграция системы контроля и управления БАС с системами управления пилотируемой авиации.

Для создания системы защиты информации цифровой платформы определены:

- ее архитектура и функциональные подсистемы;
- уровень конфиденциальности обрабатываемой информации, хранящейся в них;
- интерфейсы взаимодействия.

Средства защиты информации предусмотрены на уровне интеграционной шины – ядра платформы. Она обеспечивает объединение всего множества беспилотных средств, типовых пунктов контроля и управления БТС в единую интегрированную сетевую вычислительную среду (ИСВС), в рамках которой обеспечивается решение перечисленных задач (рис. 3.7).

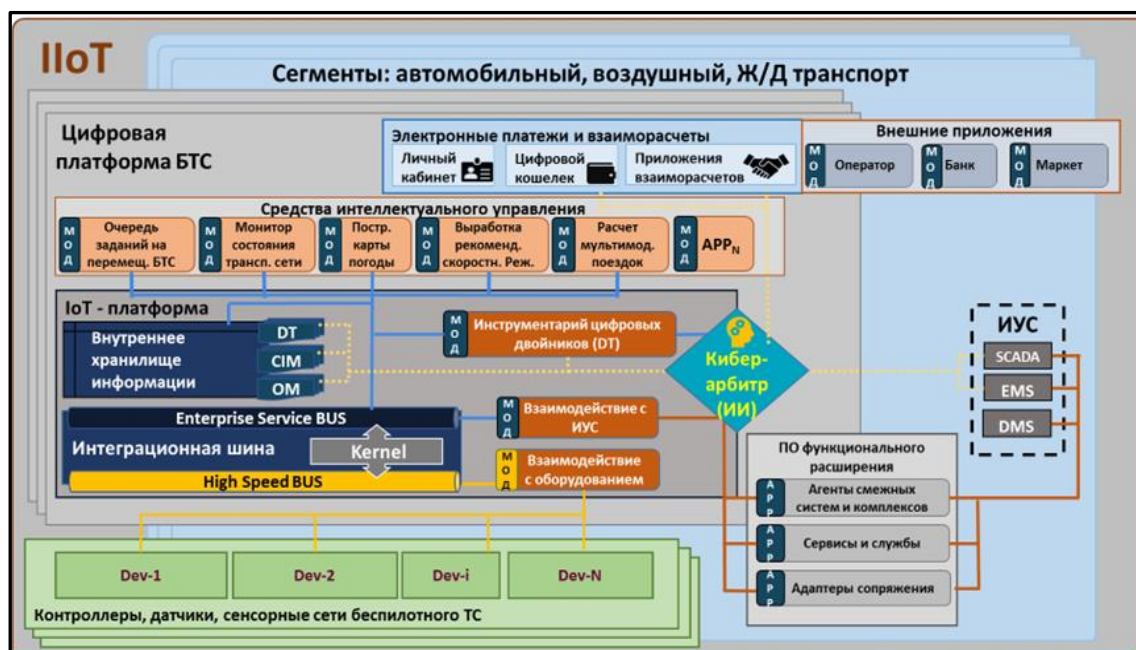


Рис. 3.7. Архитектура платформы БТС (БАС) [258]

Цифровая платформа содержит следующие элементы.

1. *Интеграционная шина.*

Ее назначение состоит в обеспечении взаимодействия всех компонентов системы и решении следующих задач:

- создание единого адресного и информационного пространства на множестве узлов гетерогенной вычислительной сети, состоящей из центров управления и бортовых комплексов БАС различных производителей;
- управление всеми процессами, зарегистрированными в соответствии с общесистемными требованиями;
- высокоскоростной обмен данными по сервисной шине (*High Speed Bus*) для взаимодействия с бортовыми системами БАС со скоростью обмена не менее 250 Кб/с;
- маршрутизация данных, гарантированное доведение информации, в том числе – по каналам с потерями и низкой пропускной способностью, гарантированная обработка информации получателем;
- гарантированное хранение данных во внутреннем хранилище и управление источниками данных, в том числе – внешними;
- разграничение доступа к информационным ресурсам, каналам передачи данных, средствам ввода/вывода информации;
- контроль действий всех субъектов (люди/роботы), привилегированные пользователи;
- бесшовная интеграция с внешними информационными системами и предоставление для них шины для обмена информацией.

2. *Комплекс программ интеллектуального управления БАС.*

Он включает модули мониторинга и интеллектуального управления, которые обеспечивают:

– начальную проверку, включение и контроль параметров работы модулей БАС;

– сбор, анализ и передачу результатов контроля модулей;

– управление электропитанием и параметрами работы модулей;

– обслуживание и управление конфигурацией модулей.

3. Интегрированное хранилище информации.

Хранилище включает банки данных первичной (собираемой) и вторичной (обработанной) информации. В результате обеспечивается хранение данных и предоставление доступа к ним, документам, моделям и алгоритмам обработки данных.

4. Модуль, реализующий инструментарий цифровых двойников.

Инструментарий цифровых двойников позволяет перенести в вычислительную среду сложившиеся представления (знания) о состоянии всей системы управления и объективизировать их на уровне концептуальной модели предметной области (КМПО), обладающей, в том числе и темпоральными свойствами [373].

5. Модуль искусственного интеллекта (киберарбитр) [141].

Модуль реализует алгоритмы интеллектуальных вычислений с применением нейронных сетей для обработки сигналов, больших данных, разрешения конфликтов субъектов информационного взаимодействия. На БАС предусмотрены модели машинного зрения.

В условиях быстро изменяющейся воздушной обстановки и переменного состава группировки в воздухе обеспечивается динамическое распределение вычислительных ресурсов флота БАС, повышается энергоэффективность.

6. Модуль взаимодействия с бортовыми информационными системами БАС предыдущих поколений и сторонних разработчиков [170; 368–370].

Модуль позволяет решать проблемы интеграции разнородных БПЛА и БАС и обеспечить их взаимодействие на основе унифицированных протоколов.

7. Модуль взаимодействия с информационно-управляющими системами пилотируемых воздушных судов.

Модуль обеспечивает интеграцию БАС в единое информационное пространство воздушного движения.

Исходя из сказанного, укажем принципы, положенные в архитектуру цифровой платформы, и которые позволяют:

– производить реконфигурацию системы и ее составных частей без изменения архитектуры;

– унифицировать и типизировать модули технического конструктива, а также библиотеки базовых алгоритмов;

– гибко изменять состав встроенного и системного ПО;

– работать с любыми операционными системами реального времени и обеспечивать кроссплатформенность;

– резервировать аппаратные и программные компоненты и обеспечивать требуемую кибербезопасность, надежность, отказоустойчивость БАС.

Функционирование ПО цифровой платформы предполагается на отечественных аппаратных средствах Эльбрус и Байкал. Используемые подходы и методы позволят создать класс технологий для построения унифицированной ИСВС, которая в дальнейшем будет взаимодействовать со всеми используемыми и перспективными БТС.

Состав ядра цифровой платформы и встроенных средств защиты информации. Ключевым элементом цифровой платформы БАС является *интеграционная шина*. Она предназначена для организации вычислительного процесса на множестве распределенных в пространстве гетерогенных программно-аппаратных средств БАС. Рассмотрим подробнее устройство структурно-функциональной схемы интеграционной шины (рис. 3.8) [258].

По своей сути она является так называемой канонической схемой организации защищенной обработки данных средствами интеграционной шины в составе автоматизированной системы управления (АСУ) беспилотным транспортом. Совокупность используемых при этом элементов относится к классу общесистемного программного обеспечения (ОСПО) и призвано обеспечить организацию совместного функционирования доверенных компонентов автоматизированных информационно-управляющих систем (АИУС) для каждого узла.

В составе интеграционной шины предусматривается пять функциональных подсистем:

- организации и управления вычислительным процессом – ядро интеграционной шины;
- интегрированное хранилище информации (базирующееся на технологиях систем управления базами данных – СУБД);
- комплекс средств защиты информации;
- транспортная служба передачи данных;
- мультипротокольный сервис интеграции информационных систем (специального назначения и обеспечивающих).



Рис. 3.8. Структурно-функциональная схема интеграционной шины – ядра цифровой платформы БАС [258]

В составе интеграционной шины для рассматриваемого и предлагаемого нами класса задач должны быть сосредоточены пять функциональных подсистем:

- организации и управления вычислительным процессом – ядро интеграционной шины;
- интегрированное хранилище информации (базирующееся на технологиях систем управления базами данных – СУБД);
- комплекс средств защиты информации;
- транспортная служба передачи данных;
- мультипротокольный сервис интеграции информационных систем (специального назначения и обеспечивающих).

Обратимся вначале к общему описанию ядра цифровой платформы БАС. Перечисленные задачи могут быть решены средствами интеграционной шины – *ESB-шины*. Интеграционная шина включает в свой состав кроссплатформенные средства интеграции, хранения, обмена данными и комплекс средств защиты информации. Указанная унифицированная или каноническая схема вычислительного процесса для доверенных компонентов ОСПО является инвариантной по отношению к различным программно-аппаратным платформам и воспроизводится на каждом узле локальной вычислительной сети (ЛВС) АСУ беспилотным транспортом.

Каноническая схема содержит набор коммуникационных приложений (транспортных задач). Транспортные задачи, с одной сторо-

ны, обеспечивают интерфейс подключения узла к интеграционной шине, а, с другой – транспортный диспетчер – к ОСПО.

Все интерфейсы взаимодействия между доверенными компонентами унифицируются на уровне ОСПО таким образом, что симметричное взаимодействие распределенных (на одной или различных программно-аппаратных платформах) приложений сводится к композиции локальных обращений к интеграционной шине и взаимодействию их между собой по внутреннему защищенному протоколу шины.

Ключевым элементом является ядро, которое решает задачу организации вычислительного процесса на множестве гетерогенных программно-аппаратных средств. Модуль инициализации системного окружения ядра обеспечивает для всех зарегистрированных в интеграционной шине приложений (сервисов, адаптеров, прикладных задач) функционирование в рамках единого информационного пространства. В созданном едином пространстве данные становятся доступными всем авторизованным приложениям и пользователям вне зависимости от их локализации и организационной подчиненности.

Ядро интеграционной шины обеспечивает для каждого процесса ведение очереди с возможностью приоритетной обработки передаваемых сообщений, в зависимости от их важности, и маршрутизацию сообщений (передачу в очередь специализированным обработчиком), в зависимости от вида и формата передаваемых в них данных.

При передаче данных между процессами по каналам связи средствами «Транспортной службы» обеспечивается предварительное сжатие и контроль целостности, а со стороны «Ядра интеграционной шины» контроль доведения до получателя и обработки на приемной стороне соответствующим обработчиком.

Выполнение всех операций доступа к информационным ресурсам, функциям и каналам связи в интеграционной шине производится под контролем комплекса средств защиты информации. Комплекс средств защиты обеспечивает:

- контроль целостности и неизменности всех исполняемых модулей и файлов конфигурации перед каждым запуском интеграционной шины;
- управление полномочиями субъектов доступа;
- проверку полномочий субъектов при допуске к работе в интеграционной шине и при доступе субъектов к данным;
- фиксацию всех инцидентов нарушения безопасности и штатного режима функционирования в журналах регистрации системных событий.

Интеграция с внешними информационными системами обеспечивается посредством «Многопротокольного сервиса интеграции информационных систем», а также сервисов и адаптеров, которые могут разрабатываться в дополнение к нему. На приведенной схеме (рис. 3.8) видно, что функциональность интеграционной шины может

наращиваться добавлением новых модулей, для разработки которых в интеграционной шине реализуется и предоставляется программный интерфейс для разработки новых программных расширений.

В настоящее время описанное решение реализовано в Цифровой платформе «Атлант-БАС» (разработчик – ООО «Т-АВИАС»), прототип которой создавался при грантовой поддержке Фонда НТИ.

Таким образом, существующие заделы обеспечивают реализацию любой задачи передачи данных во внешние ИС. В связи с этим фокус внимания должен быть перенесен на подготовку информации для обмена: повышение качества первичных данных, обеспечение их точного соответствия стандартизированным концептуальным моделям и массивам нормативно-справочной информации.

Интеграционная шина обеспечит гарантированную доставку данных до абонентов (задач) с ретрансляцией информационных потоков и шлюзованием различных протоколов обмена данными при работе по различным сетям связи общего пользования, а также по прямым (выделенным) открытым и закрытым ведомственным каналам связи.

Выполнение обозначенного функционального комплекса и многих сопутствующих операций в настоящее время все больше приобретает черты интеллектуальной поддержки и возлагается на СПО, по замыслу своему разрабатываемому для решения узкоспециализированных задач в определённой области деятельности. Указанная методология обусловлена использованием именно в профессиональной среде, где стандартные программные решения не всегда подходят из-за требований и условий эксплуатации.

Можно отметить совокупность основных ПО, которые рассматриваются как система обеспечения в управлении БАС и предназначены для автоматизации таких операций, как:

- регистрация планируемого к эксплуатации парка;
- идентификация и аутентификация;
- управление парком беспилотников на жизненном цикле;
- планирование маршрутов;
- управление полетом;
- обеспечение систем связи;
- контроль состояния на маршруте;
- картография и поддержание взаимодействия с геоинформационными системами;
- поиск и распознавание объектов;
- предупреждение столкновений.

Кроме того, перечисленный состав должны дополнять СПО, реализующие симуляторы и тренажеры, среды разработки ПО БАС и т. д.

Естественно, что рамки монографии не позволяют привести подробные особенности научной, конструкторской, технологической и иных этапов деятельности Т-АВИАС по созданию предлагаемой цифровой платформы БАС. Основной задачей при этом выступает

обеспечение совместимости между собой всех компонент комплекса ПО АСУ БАС, в который входят следующие.

1. *ОС*. Главный принцип выбора ОС – обеспечение совместимости всего множества аппаратных и программных средств. Отметим некоторые из этих функционально оцененных платформ:

- *ROS (Robot Operating System)* – для роботизированных систем и автономных транспортных средств;

- проприетарная ОС от *DJI* – осуществляет работоспособность «из коробки», но ограничит в возможности развития функциональности;

- *ArduPilot* и *PX4* – открытые платформы для полетных контроллеров, используются в *DIY*-проектах (*Do It Yourself*);

- *POK (Partitioned Operating Kernel)* – для надежных контроллеров, поддерживает *AADL*-моделирование (*Architecture Analysis & Design Language*);

- *Arduino* – для создания собственных программ полетных контроллеров, например, с помощью пропорционально-интегрально-дифференциальных регуляторов (ПИД-регуляторов).

2. *СУБД*. Они обеспечивают хранение, поиск и быстрый доступ, а также анализ огромных объемов данных, генерируемых системами БАС: телеметрия, геопространственные данные, изображения и т. д. Например, на борту БАС применяют «лёгкие» системы (*SQLite* – запись данных о полёте в полётных контроллерах с прошивками *ArduPilot* или *PX4*). В центрах обработки данных (ЦОД) объёмы информации, получаемой от БАС, измеряются сотнями ТБ. Там нашли применение *PostgreSQL* или *MongoDB*. А задачи фотограмметрии обуславливают необходимость геопространственных СУБД, таких как *PostGIS* – создание подробных карт или *3D*-модели местности.

3. *СПО*. Например, для БАС квадрокоптерного типа принципиально важны: *полётные контроллеры* (*ArduPilot* и *PX4* – управление датчиками и стабилизация полёта); *приложения для мобильных и стационарных комплексов управления полетом* (*DJI Fly* – удобные интерфейсы для выполнения полетных заданий).

Завершая небольшой экскурс, подчеркнем, что, выполняя непосредственные производственные задачи, описываемое программное изделие (ПИ) «Комплект сервисов цифровой платформы БАС», осуществляет и взаимодействие с другими программными платформами. В частности, по сетевому протоколу прикладного уровня HTTP поддерживается связь с следующими браузерами: Яндекс Браузер; *Google Chrome*; *Chromium*; *Firefox*; *Safari*.

Пользователь взаимодействует с ПИ через веб-приложение, отправляя запросы на сервер, и ожидает ответ. Сервер обрабатывает запрос, аутентифицирует пользователя через *JWT* сервис, проверяет права доступа в каждом запросе, после чего позволяет получить доступ к необходимым полям, например, учет или план полетов БВС. Сервер возвращает данные в виде *HTTP*-ответа (рис. 3.9).

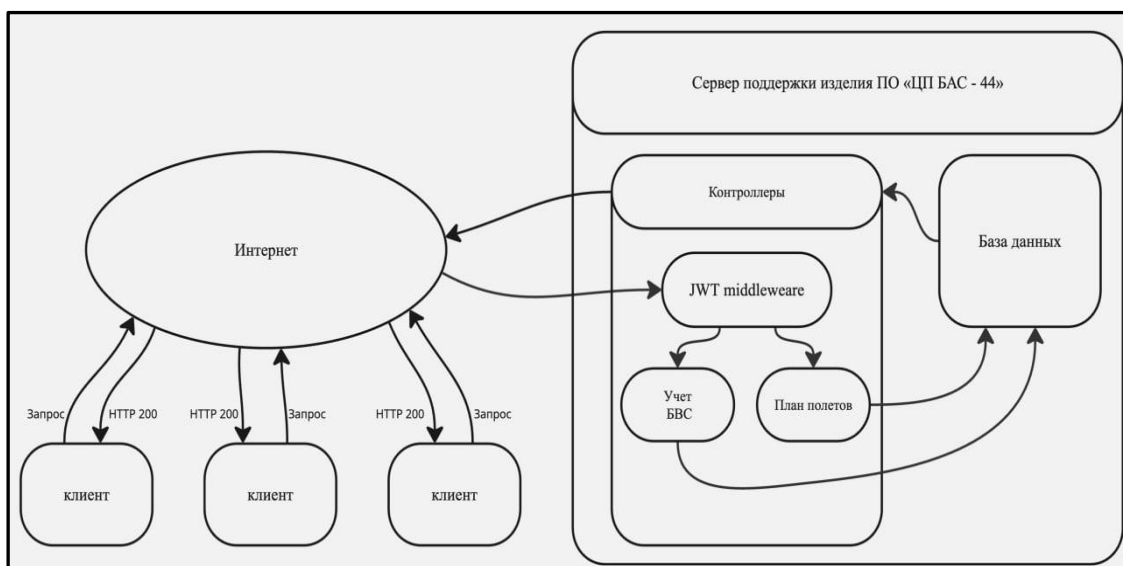


Рис. 3.9. Схема взаимодействия между пользователем и сервером

Кроме того, еще в качестве иллюстрации для понимания некоторых нюансов цифровой платформы БАС обратимся к краткому пояснению технологических подходов аутентификации пользователей, отраженных на рис. 3.10. Изображение представляет собой общую логическую схему аутентификации пользователей, которая поддерживается в цифровой платформе БАС.

В самом общем виде на схеме показано описание технологии данной реализации на основе использования *JWT*-сервис. Для этого на поле рисунка отмечены вспомогательные пакеты, такие, например, как: *pkg/authentication* и *pkg/hash*.

Они содержат в себе возможности методов для реализации основных функций аутентификации. Среди них, например:

- хэширование и проверка пароля и ключа (*GenerateHash Password*, *ValidatePassword*);
- генерация токенов доступа и обновления (*GenerateAccessToken* и *GenerateRefreshToken*);
- проверка корректности ключа (*ParseAccessToken* или *ValidateRefreshToken*).

Кроме того, отмечены пакеты для взаимодействия с базой данных: *repository/tokenRefresh* и *repository/user*. Они поддерживают методы получения и изменения данных, например, создания токена и пользователя (*CreateToken* и *CreateUser*), поиск токена, используя его хэш-строку (*GetTokenByHash*). Эти пакеты участвуют в реализации бизнес-логики: *SignUp*, *SignIn*, *Logout*, *AccessTokenUpdate*.

Перед тем, как запрос достигнет обработчика, используется промежуточный обработчик *Middleware*, который проверяет все необходимые поля: *cookies*, тип токена, его пригодность. После этого дается разрешение на дальнейшую работу сервиса или отказ пользовате-

лю, например, на основании, что время действия его токена доступа истекло.

Для обработки запросов и возврата ответов реализован пакет *Hadler*, который проверяет запрос, преобразовывает запрос (*JSON*) во внутреннюю бизнес-модель, вызывает методы *service: SignIn, SignUp* и другие, обрабатывает ошибки, устанавливает параметры, например, сохранение пары ключей в *cookies*, формирует и возвращает ответ.

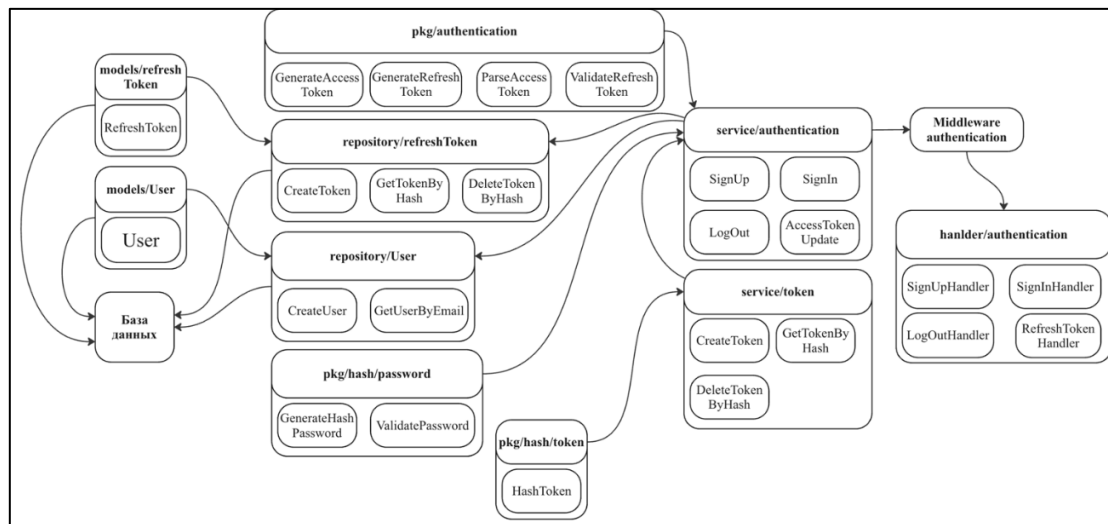


Рис. 3.10. Логическая схема аутентификации пользователя, поддерживаемой цифровой платформой БАС

После теоретических положений, приведем характеристику некоторых возможностей функционала ядра интеграционной шины.

Модуль инициализации системного окружения, находящийся в составе ядра, обеспечивает единое адресное пространство на всем множестве узлов (вычислительных установок, логических модулей) и задач, а также единую среду функционирования для приложений, выполняющих общесистемные соглашения. К приложениям относятся сервисы, адаптеры сопряжения и различное ПО, решающее прикладные задачи. При инициализации системного окружения логический модуль получает системные переменные, справочники и классификаторы информации, адресные таблицы, правила обработки документов и сообщений, данные об организации вычислительного процесса на объекте автоматизации, матрицу разграничения доступа к информационным ресурсам и каналам передачи данных.

Модуль управления очередями сообщений интеграционной шины для каждого зарегистрированного процесса обеспечивает ведение очереди сообщений с установкой приоритетов их обработки. Обеспечивается асинхронный режим взаимодействия между процессами.

Маршрутизация данных выполняется *модулем маршрутизации* в зависимости от формата данных передаваемых сообщений и документов.

В функциональные возможности шины заложена возможность работы на низкоскоростных каналах (до 1 200 бод) с потерями. Интеграционная шина контролирует целостность передаваемых данных, квитируются доведение и обработка данных специальным обработчиком на приемной стороне.

Модуль управления средствами защиты информации обеспечивает управление встроенным комплексом средств защиты информации (КСЗИ), включающим средства:

- управления профилями и полномочиями пользователей;
- управления доступом к информационным ресурсам, каналам передачи данных и устройствам ввода/вывода информации;
- ведения журналов регистрации системных событий;
- контроля целостности;
- контроля действий всех субъектов (люди/роботы), в том числе контроль действий привилегированных пользователей (администраторы, руководители с высокими рангами полномочий).

В функции *модуля управления доступом* входит контроль выполнения всех операций доступа к информационным ресурсам и каналам связи производимых субъектами доступа средствами цифровой платформы БАС.

Модуль управления профилями пользователей обеспечивает управление полномочиями субъектов. Поддерживаются мандатная, дискреционная и ролевая модели управления доступом.

Все инциденты, нарушения информационной безопасности и штатного режима функционирования фиксируются в журнале регистрации системных событий КСЗИ.

Развитие системы защиты информации видится в обеспечении кибербезопасности платформы с функциями ИИ, защиты ее от угроз, приводящих:

- к ошибкам в моделях обработки данных;
- несанкционированному получению конфиденциальной информации путем обмана модели ИИ;
- преднамеренному внесению некорректных данных с целью манипуляции ИИ и искажения результата работы системы ИИ;
- переусложнению системы ИИ.

Взаимодействие БАС и цифровой платформы реализуется посредством многопротокольного сервиса интеграции, а также разрабатываемых по мере необходимости адаптеров сопряжения.

Инструментарий цифровой платформы БАС позволяет разработчикам ПО реализовывать любые дополнительные механизмы обеспечения ИТВ с внешними информационно-управляющими системами БАС. Обязательными условиями являются выполнение общесистемных требований, определенных в эксплуатационной документации на цифровую платформу БАС. Для включения новых элементов и ресурсов в вычислительный процесс и единый информационный

контур необходимо выполнить процедуру регистрации задачи согласно руководству системного программиста. Это позволяет в дальнейшем производить централизованное управление, предоставление доступа к данным и обеспечивать защиту информации.

Технологическая зрелость цифровой платформы. ПО в составе цифровой платформы характеризуется следующими свойствами:

- исходные коды являются оригинальными и не имеют заимствований из Интернет и других открытых источников;
- ПО авторизовано – за каждой строчкой кода есть ответственный автор – резидент РФ;
- высокая степень готовности ядра цифровой платформы и ее компонент;
- разработка ориентирована на сертификацию по требованиям МО, ФСБ, ФСТЭК РФ;
- технологический цикл выстраивается в соответствии с требованиями, предъявляемыми [46].

Уровень зрелости технологий и продуктов в составе цифровой платформы представлен в табл. 3.5. В поле «статус» указан условный уровень зрелости технологии, продукта:

- PRO – промышленное исполнение продукта (изделия), имеются внедрения и накоплен опыт применения в реальных условиях;
- MVP (Minimum Viable Product) – минимально жизнеспособный продукт, для которого подтверждена бизнес-ценность;
- ADV TECH – уровень зрелости, при котором разработан и протестирован в реальных условиях экспериментальный образец или работающий прототип изделия;
- TECH – технология или продукт протестированы на макетах в рамках инициативных НИР.

Уровни зрелости, примененные для оценки составных элементов цифровой платформы, можно условно отождествить с уровнями готовности технологий (УГТ), определенными ГОСТ Р 58048-2017. В табл. 3.6 представлено соотнесение с условными ограничениями, обусловленными особенностями технологического цикла разработки ПО цифровой платформы и наличием доступных действующих аналогов.

Отметим некоторые особенности. Разработка рассмотренной цифровой платформы ведется без заимствования зарубежных технологий, в том числе – из открытых источников. Отдельные компоненты платформы прошли сертификацию по требованиям безопасности информации во ФСТЭК России, Минобороны России, ФСБ России в составе систем и изделий, эксплуатируемых в государственных организациях.

Технологии, реализуемые на уровне ядра цифровой платформы, позволяют снять ряд ограничений при построении информационно-управляющих систем БАС, а именно:

- использование различных опорных сетей связи и передачи данных;

- работа в низкоскоростных, неустойчивых каналах связи;
- возможность взаимодействия с системами управления других видов беспилотного транспорта: автомобильного, морского, речного, а также роботами;
- организация мультимодальных перевозок;
- киберустойчивость БАС.

Таблица 3.5

Уровень зрелости технологий и продуктов в составе цифровой платформы

Технологии, продукты	Статус
Интеграционная шина - Enterprise Service BUS. Технологическая платформа интеграции приложений - High Speed BUS. Технологическая платформа для взаимодействия с терминальными устройствами в режиме реального времени - Служба гарантированной доставки данных и контроля обработки данных на принимающей стороне	PRO
Система операционного управления - Служба управления распределенной вычислительной инфраструктурой - Служба мониторинга бизнес-процессов	MVP
Конструктор цифровых двойников технических объектов и бизнес-процессов	ADV TECH
Система интеллектуального управления бизнес-процессами - Очередь заданий на перемещение БТС - Монитор состояния транспортной сети - Построение карты погоды - Выработка рекомендаций скоростного режима - Расчет мультимодальных поездок	TECH
Интегрированное хранилище информации и объединенный коммуникационный центр консолидации данных от разнородных источников	ADV TECH
Агентство доступа к первичным сетям передачи данных	ADV TECH
Интерактивный экспресс-анализ данных Служба экспресс-анализа серий данных	TECH

Таблица 3.6

Соответствие уровня зрелости технологий и продуктов УГТ по ГОСТ Р 58048-2017

УГТ по ГОСТ Р 58048-2017		Уровень зрелости элементов ЦП БАС
УГТ	Описание	
УГТ-4	Компонент и/или макет испытан в лабораторных условиях	<i>TECH</i>
УГТ-6	Модель системы/подсистемы или прототип продемонстрирована в условиях, близких к реальным	<i>MVP¹</i>
УГТ-7	Прототип системы продемонстрирован в реальных условиях эксплуатации	<i>ADV TECH</i>
УГТ-9	Работоспособность системы подтверждена в ходе успешной эксплуатации (достижения цели)	<i>PRO</i>

¹ MVP не соответствует УГТ-3, как это предполагает изначальный замысел и назначение MVP, а соответствует УГТ-6, ввиду того, что для технологий и продуктов в составе платформы, возможность демонстрации открывается после создания прототипа.

Выбранная архитектура Цифровой платформы позволяет:

- создавать автоматизированные защищенные распределенные системы контроля и управления БАС на федеральном, региональных и ведомственных уровнях;
- ускоренно создавать и вводить в действие типовые центры контроля и управления БАС и интегрировать их в единую автоматизированную систему;
- интегрировать в единую систему контроля и управления разнородные БАС различных разработчиков.

В рамках Федерального проекта «Развитие инфраструктуры, обеспечение безопасности и формирование специализированной системы сертификации беспилотных авиационных систем» платформа позволяет:

- создать унифицированную инфраструктуру обеспечения полетов БАС и своевременно оснастить ей субъекты РФ в соответствии с планом до 2030 г.;
- обеспечить контроль воздушной обстановки над защищаемыми объектами, включая критическую инфраструктуру;
- достичь требуемой киберустойчивости БАС и их защиту от неправомерного применения;
- контролировать выполнение полетных заданий, выявлять и предотвращать аномалии в поведении БАС;
- обеспечить соответствие БАС законодательству РФ и требованиям по безопасности.

В завершение раздела, кроме приведенных концептуальных, общих, организационных, технологических и иных аспектов реализации Цифровой платформы, отметим некоторые разработки, выполняемые в целях безопасного управления БАС. В частности, речь идет, например, об интеллектуальной технологии *DroneCerebellum*.

Данный аппаратно-программный инструментарий представляет аналог токена или флэш-карты, подключаемой к БАС через USB-порт (рис. 3.11). Устройство устанавливается на каждый БАС управляемой группировки и позволяет обеспечить процедуры идентификации и аутентификации.

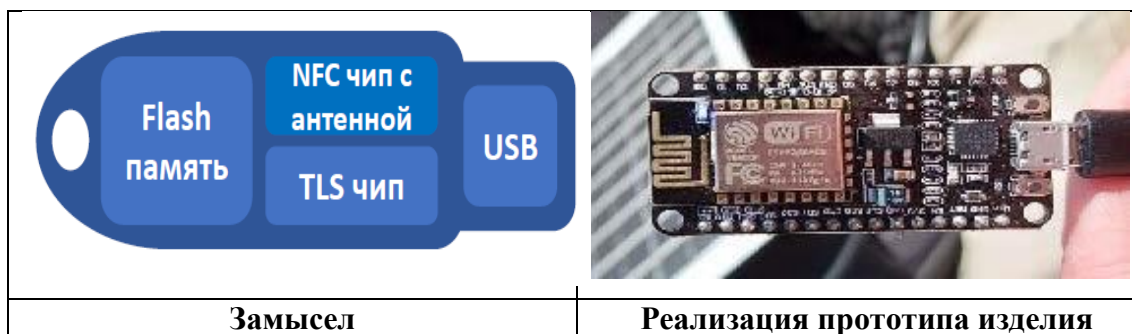


Рис. 3.11. Аппаратно-программная реализация технологии *DroneCerebellum* [258]

В результате технология *DroneCerebellum* в основе Цифровой платформы позволяет контролировать управление беспилотниками из Центра мониторинга как бы за счет инъекции своеобразного «мозжечка» в их систему управления. Применение указанной технологии позволяет эффективно защитить каналы взаимодействия беспилотников с пунктами контроля и управления от перехвата управления.

Использование этой и других интеллектуальных аппаратно-программных разработок под руководством специализированного Центра мониторинга приводит к такому управлению роем (группировкой) БАС, когда достигается единая цель конкретного полетного задания.

О некоторых других интеллектуальных аппаратно-программных разработках будет сказано ниже.

3.6. Выводы по главе 3

1. Глава открывает вторую часть монографии, связанную с вопросами обеспечения кибербезопасности управления беспилотным транспортом от киберпреступлений новых видов. Речь идет о киберугрозах, которые способны привести к самым негативным последствиям: масштабным катастрофам, нарушениям нормального функционирования критических информационных инфраструктур (КИИ) и т. д. В главе отражена авторская концепция создания системы противодействия подобным последствиям, которая ориентирована на использование технологий ИИ.

2. Концепция базируется на создании системы моделей и технологий безопасного управления БТС. Рассмотрены подходы к формированию ее составляющих:

- моделирование киберугроз системам ИИ в управлении беспилотным транспортом;
- моделирование киберустойчивости и управляемости флотом БАС;
- классификация моделей безопасного управления БТС;
- комплексная математическая модель интеллектуальной защиты информации флота БАС.

3. Практическая реализация концепции позволила сформулировать базовые требования, определить ресурсные и правовые решения при создании единой Цифровой платформы безопасного, интеллектуального управления БАС, включающей обоснование ее архитектуры; состав ядра и встроенных средств защиты информации; пути оценки технологической зрелости проекта; организация информационно-технического взаимодействия; программно-аппаратные решения.

Глава 4. Решения прикладных задач управления беспилотным транспортом

Ограничения объема монографии потребовали ограничений в выборе материалов главы. Исходя из этого, представим только следующие направления:

- кибербезопасность БАС в системах дистанционного мониторинга лесных территорий;
- экспертно-криминалистическая деятельность;
- геоинформационные системы в интеллектуально-аналитическом обеспечении раскрытия и расследования преступлений;
- автоматизация распознавания и маршрутизации БТС, принятие решений по безопасности.

4.1. Кибербезопасность беспилотных авиационных систем мониторинга лесных территорий

К решению ряда значимых научно-прикладных задач по данной тематике авторы монографии имели непосредственное отношение. Это и исследование, выполненное в рамках государственного задания Министерства науки и высшего образования РФ (тема № FSFN-2024-0073), и научные работы, результаты которых опубликованы, например, в источниках [255; 258; 260; 363; 400–401], апробации на ведущих форумах страны.

Как известно, Россия обладает уникальным биоресурсом – две трети ее территории покрыто лесами. Общая площадь земель лесного фонда, по данным Рослесхоза России, составляет 1,15 млрд га.

Огромную угрозу данному богатству представляют лесные пожары. Ежегодно их регистрируется до 35 тыс. с общей площадью до 3,5 млн га. Указанная угроза делает исключительно важной задачей предотвращение лесных пожаров. Для этого необходимо развитие эффективных мер предупреждения, раннего обнаружения и реагирования, которые, в свою очередь, определяют актуальность применения средств автоматизации, новых технологий мониторинга и детектирования с применением средств видеонаблюдения, машинного зрения, БАС и ИИ.

В настоящее время в Российской Федерации наблюдение за пожарами ведется с использованием наземных, авиационных и космических средств. На территориях с развитой инфраструктурой мониторинг проводится, в основном, наземными методами по специально установленным и утвержденным маршрутам, а также с пожарно-наблюдательных вышек, господствующих высот и мачт. Применяются и различные разновидности БАС.

Система видеомониторинга организована в 64 субъектах. Информация с камер наблюдения по сетям поступает в центр обработки данных, где располагаются главные сервера. Они обрабатывают видеозображение, автоматически распознавая дыма. Для получения изображения местности используются камеры с 32-кратным оптическим увеличением, позволяющим различать дым на расстоянии до 20 км.

Представление об используемых технологиях дает система управления и дистанционного мониторинга «Лесохранитель» компании «Формоза-софт». Она осуществляет дистанционный мониторинг территории и обнаружение лесных пожаров на ранней стадии в дневное и ночное время, определяет координаты дыма с погрешностью до 100 м.

На труднодоступных территориях работы по обнаружению и тушению лесных пожаров выполняют региональные авиабазы. В настоящее время авиационная охрана лесов России помимо ФБУ «Авиалесоохрана» представлена 27 авиабазами с активными силами и средствами, которые выполняют работы по борьбе с лесными пожарами на площади более 1 млрд га.

Оценка ситуации указывает, что нерешенным остается вопрос автоматизации в труднодоступных местах передачи видеопотока высокого разрешения из-за отсутствия стабильных каналов связи. Это приводит к необходимости использования авиации, в том числе БАС роторного типа или с жестким крылом. В таких условиях важной становится разработка *систем автоматизации управления полетами БАС* для выполнения регулярных облетов территорий в соответствии с полетным заданием. Оно должно передаваться на борт летательного аппарата с помощью защищенных протоколов беспроводной передачи данных с сервера сетевой службы.

Одним из важных аспектов, который остается недостаточно раскрытым при разработке БАС мониторинга лесных массивов, является кибербезопасность. В частности, в ГОСТ Р 70802-2023 «Беспилотные авиационные системы для обеспечения пожаротушения, аварийно-спасательных и других работ, выполняемых в целях предупреждения чрезвычайных ситуаций и ликвидации их последствий. Общие требования» не содержатся прямые требования обеспечения кибербезопасности или указания на официальные документы, устанавливающие такие требования [260].

Зачастую лесные массивы связаны с размещением в них объектов оборонного и оборонно-промышленного комплекса, критической инфраструктуры городов, энергетики, химической промышленности и других (далее, критически важные объекты – КВО). Несмотря на усиленные противопожарные меры, принимаемые для таких объектов, требуются дополнительные меры контроля очагов возгорания и распространения пожаров, для чего применяют БАС.

Кибербезопасность БАС, таким образом, напрямую связана с угрозами объектам КИИ. Критичными при этом выступают *угрозы с перехватом или потерей управления БАС*, реализация которых потенциально ведет к опасным атакам на объекты КВО.

Защита БАС, используемых вблизи объектов КВО, является комплексной задачей и требует:

- защиты данных: обеспечение конфиденциальности, целостности и доступности информации, передаваемой между компонентами БАС и внешними системами управления;
- управления доступом: предоставление доступа к управлению БАС только авторизованным пользователям и предотвращение возможности перехвата управления злоумышленниками;
- мониторинга и обнаружения угроз: внедрение механизмов мониторинга активности БАС и обнаружение аномалий, связанных с возможными киберугрозами;
- защиты каналов связи: использование протоколов передачи данных и средств шифрования для предотвращения перехвата или подмены команд управления;
- обновления ПО и патчей безопасности: регулярная установка обновлений ПО и устранение уязвимостей для минимизации рисков при эксплуатации;
- соответствия нормативным требованиям: соблюдение всех нормативных актов и стандартов, регулирующих использование БАС в зоне КИИ или КВО;
- резервирования отказоустойчивости: разработка резервных механизмов управления и систем защиты, обеспечивающих бесперебойную работу при сбоях или атаках;
- анализа рисков и моделирования сценариев: проведение регулярных оценок возможных атак для своевременной адаптации мер защиты.

Как указано выше, для эффективного решения задачи защиты БАС от киберугроз разрабатывается и поддерживается в актуальном состоянии модель угроз и нарушителей, учитывающая все факторы угроз на жизненном цикле БАС и соответствующая система защиты. Первым приоритетом выступают угрозы, связанные с разработкой и изготовлением, а также особенностями применения БАС. По методологии, рассмотренной в [255], основу модели угроз составляют базовая и типовые модели, в которых учитываются угрозы, связанные с разработкой и изготовлением элементов БАС. Угрозы, связанные с особенностями применения БАС и соответствующие конкретной реализации БАС, отражаются в частной модели угроз.

В связи с обозначенными положениями авторы монографии приняли участие в разработке аппаратно-программной распределенной информационной системы (АПРИС) мониторинга лесных территорий. Экспериментальный образец системы соответствовал составу, кото-

рый рекомендован ГОСТ Р 70802-2023, и включает следующие составные части:

- БАС самолетного типа, дальность полета до 300 км, полезная нагрузка до 7 кг, управление обеспечивается с помощью мобильной установки по радиоканалу;
- стационарные комплексы наблюдения;
- быстро разворачиваемые вышки (опоры);
- специализированная мобильная лаборатория на базе автомобиля типа Соболь;
- мультиспектральный комплекс видеонаблюдения для стационарных и мобильных комплексов наблюдения;
- аппаратно-программный комплекс мониторинга лесных массивов, включающий распределённую систему сбора, обработки и хранения данных, сеть связи, объединяющую стационарные и мобильные комплексы наблюдения с мобильным пунктом управления;
- система связи и передачи данных на больших территориях на основе энергоэффективной электронной компонентной базы;
- ПО превентивного обнаружения пожаров и других техногенных катастроф с применением машинного зрения и технологий ИИ.

На рис. 4.1 показана схема организации работы и взаимодействия элементов АПРИС.

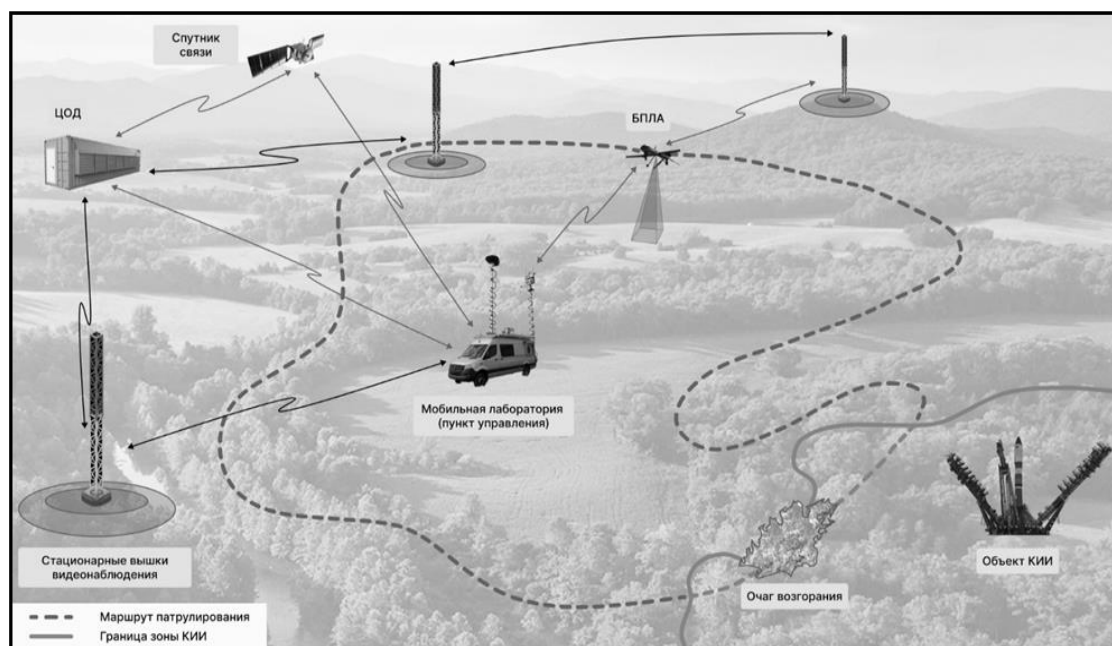


Рис. 4.1. Взаимодействие элементов АПРИС [260]

Особое при этом уделено *киберзащите системы управления*, позволяющей применять БАС в непосредственной близости объектов КВО. Объектами защиты являются:

- система управления БАС;
- система связи и передачи данных;

- мультиспектральный комплекс видеонаблюдения для стационарных и мобильных комплексов наблюдения;

- аппаратно-программный комплекс мониторинга лесных массивов, включающий распределённую систему сбора, обработки и хранения данных, сеть связи, объединяющая стационарные и мобильные комплексы наблюдения с мобильным пунктом управления и центром обработки данных (ЦОД);

- ПО превентивного обнаружения пожаров и других техногенных катастроф с применением машинного зрения и ИИ.

АПРИС предполагает следующие сценарии мониторинга лесного массива, не ограничиваясь ими:

- 1 (основной) – со стационарных вышек и доразведка при помощи БАС;

- 2 (ситуационный) – группировкой БАС, управляемой мобильной лабораторией;

- 3 (комбинированный) – со стационарных вышек и при помощи группировки БАС в местах, труднодоступных для установки вышек.

Местность характеризуется переменными значениями по площади с перепадом высот. Площадь разделяется на зоны (например, квадраты по 20–60 км), которые должны быть покрыты средствами мониторинга (стационарные вышки, БАС) в зависимости от доступности местности, возможностей приемо-передающего оборудования и т. д.

Стационарные пункты контроля размещаются на возвышенностях, по углам зон, в прямой видимости друг друга. Вышки должны покрывать площадь мониторинга таким образом, чтобы она вся контролировалась детекторами, сенсорами, датчиками.

Группировка беспилотников самолетного типа на базе электрического двигателя или двигателя внутреннего сгорания может находиться в воздухе до 4 часов. Поэтому должны быть предусмотрены места взлёта беспилотников и места их посадки на дозаправку и техническое обслуживание.

Угрозы кибербезопасности и *совершения киберпреступлений против АПРИС* могут исходить от внешних и внутренних нарушителей, определяемых по стандартным методикам оценки угроз.

В рамках проведенной работы создан прототип аппаратно-программного комплекса отправки и приёма данных с одного компьютера на другой посредством *mesh*-сети на базе цепочки доступных энергоэффективных электронных компонентов, поддерживающих тип сети *MANET*. Передача изображений стала одной из задач, решенных с помощью *mesh*-сетей. Тестирование прототипа позволило обосновать выбор передачи изображений.

В результате тестирования выбраны следующие технологии: языки программирования *Python* и *C++*; среда разработки *Arduino IDE*; передача сообщений по протоколам *Wi-Fi* и *TCP/IP*. В качестве библиотеки для реализации *mesh*-сети выступает набор микро-

контроллеров, выбрана *PainlessMesh*, позволившая объединять микроконтроллеров для самоорганизации сети передачи данных.

Интересным в проводимом исследовании по моделированию условий функционирования прототипа системы было установление размера передаваемого фрагмента для поддержания корректной работы всей *mesh*-сети. Для увеличения скорости передачи данных рассмотрена возможность приема неполного объема изображения с его последующей обработкой нейросетевыми алгоритмами. На рис. 4.2 можно видеть, как выглядят изображения, полученные с некоторой частью отсутствующих фрагментов. Картинки позволяют судить о достаточном качестве системы детекции при разной степени потерь видеофрагментов.

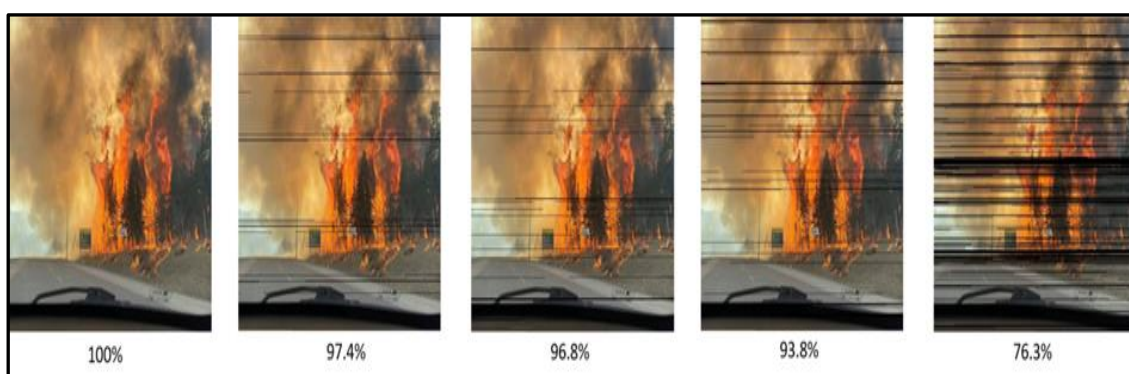


Рис. 4.2. Итоговые изображения с учетом разного уровня потери видеофрагментов [260]

В результате подтверждена возможность высокой эффективности реагирования при обнаружении возгораний. Они выявляются на ранних этапах в труднодоступных местах на получаемых изображениях с применением технологий *MANET* и нейросетевых алгоритмов. Что позволило сделать практические выводы о том, что:

- использование фильтров нормализации, размытия и улучшения четкости границ приводит к увеличению точности обнаружения источника огня нейросетевой моделью *YOLO*;
- применение прототипа *mesh*-сети позволяет передавать изображения размером порядка 3 КБ без значимой потери качества.

4.2. Экспертно-криминалистическая деятельность

Экспертно-криминалистическая деятельность ОВД стала важным направлением применения технологий ИИ. В текущем изложении акцентируем внимание на вопросе ее интеграции с достижениями ИИ и БАС. В этой связи приведем примеры, прежде всего, из материалов научно-аналитического обзора [114], работ В. Ю. Федоровича и результатов других исследователей.

В общем виде функционал и основные тактико-тактические возможности применения БАС раскрыты ранее, опираясь на работы [164]. В них были указаны следующие направления: фото-, видеонаблюдение оперативно-служебного, профилактического назначения; розыскные мероприятия; организация оперативной связи; поддержка оперативно-розыскных и следственных мероприятий; противодействие морскому пиратству; фиксация незаконной разработки недр, хищения биоресурсов, выращивания растений, содержащих наркотические вещества и т. д.

По нашему мнению, определенный интерес для решения задач в экспертно-криминалистической деятельности имеют следующие примеры, разделяемые по двум основным группам.

Первая объединяет технологии фото- и видеонаблюдения, другие потенциальные возможностей компьютерного зрения. В качестве примера отметим работу БАС при мониторинге дорожного движения в реальном масштабе времени (рис. 4.3). Очевидно, что указанный пример может быть обобщен применительно к другим оперативно-служебным задачам ОВД. Это оперативное наблюдение в ходе ОРМ; транспортная безопасность и мониторинг потоков в доказательственных целях; розыск лиц; фиксация незаконной разработки недр, хищения биоресурсов, выращивания растений, содержащих наркотические средства [114].

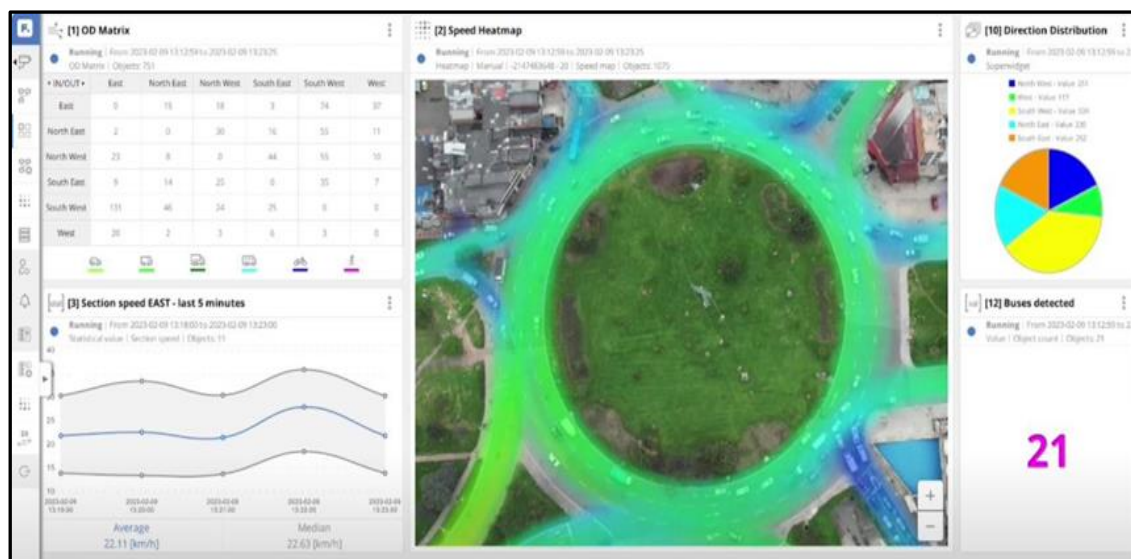


Рис. 4.3. Пример использования видеоаналитики БАС при мониторинге дорожного движения [114]

Обратимся к возможностям *растровой аналитики* и *геоинформационных систем* (ГИС). Группами, формирующими информационные потоки для растровой аналитики, выступают спутниковые изображения, данные аэрофотосъемки и снимки с БАС.

О включении разных типов изображений в ГИС-проекты в целях совершенствования аналитического обеспечения раскрытия и рас-

следования преступлений говорится в работах [90; 92]. Авторы работы [196] приводят результаты исследований по картографированию ареалов наркотических растений с использованием технологий ГИС и дистанционного зондирования. На рис. 4.4 приведены пространственные оценки спутниковых изображений, выполненных интеллектуальными алгоритмами.

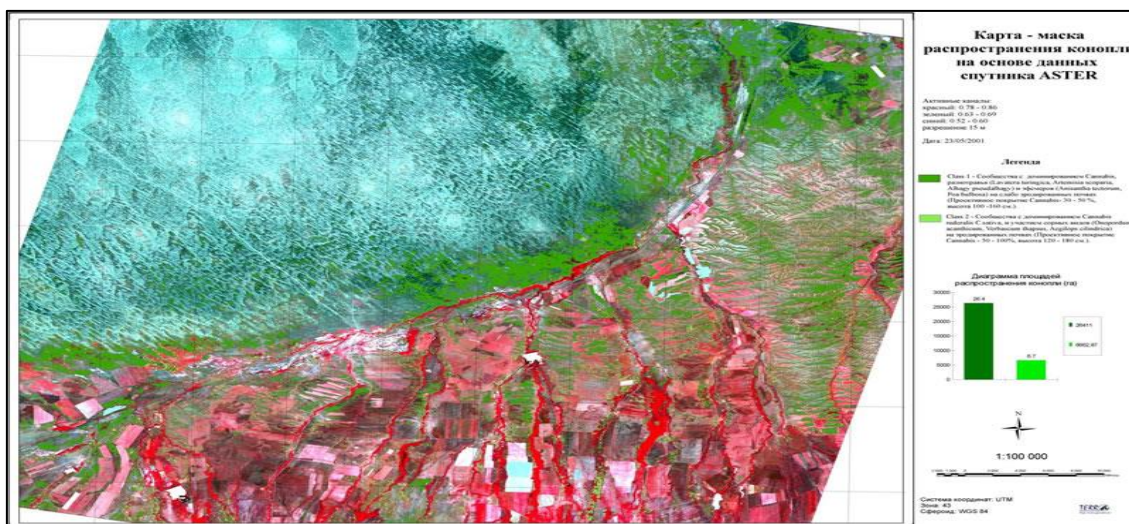


Рис. 4.4. Карта ареала *Cannabis* в Шуйской долине [196]

Другой пример обработки космических снимков приведен в работе коллектива авторов Волгоградской академии МВД России [114]. В частности, на рис. 4.5 показана оценка незаконных хищений лесных биоресурсов.

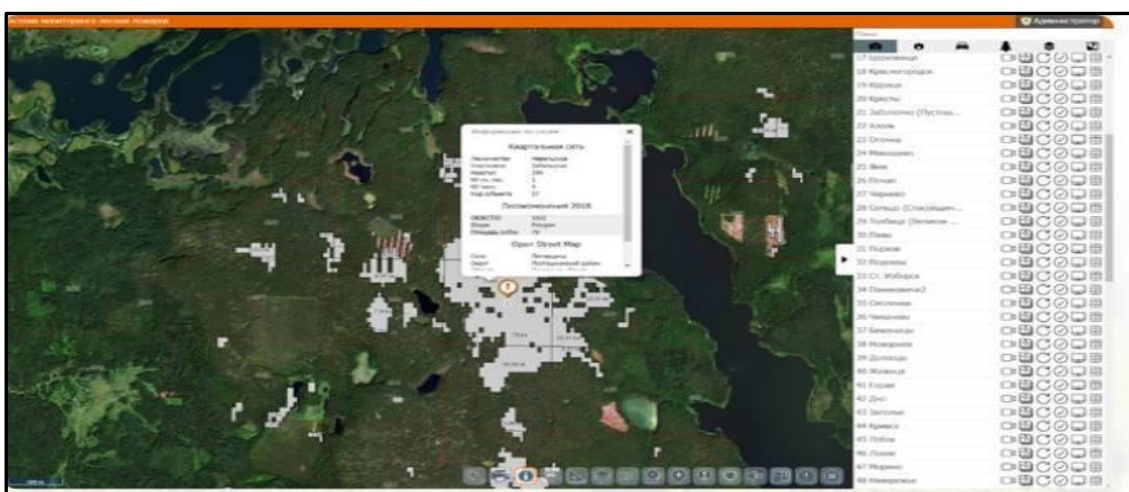


Рис. 4.5. Отображение появившихся лесных вырубок [114]

Отметим, что в области современной криминалистики ведется активная проработка оценки применимости и других новых технологических подходов. Так, в работе [371] рассматривается вопрос ис-

пользования летательных аппаратов беспилотного типа, способных усовершенствовать типовые процедуры.

Обратимся к изображениям, получаемым с БАС для достижения оперативно-служебных целей. Так, специализированные приложения *Drone2Map for ArcGIS* или *ArcGIS Pro* с дополнительным модулем *Image Analyst* обеспечивают большой перечень двумерных и трехмерных данных [268]. Среди них ортомозаики, цифровые модели рельефа и местности и др. Полученные таким образом цифровые данные могут использоваться в задачах распознавания объектов, классификации изображений, трехмерном моделировании, создании дополненной и виртуальной реальности и многих других.

Результаты съемки и последующей обработки могут быть применены в виде веб, мобильных приложений, в которых пользователь может через системы поиска найти нужную территорию, совместив данные с квадрокоптера с другими тематическими данными.

Так, на рис. 4.6 показана растровая ситуация экологического нарушения, позволяющая анализировать различные сценарии разлива нефти, представленные на базе подробной цифровой модели рельефа.

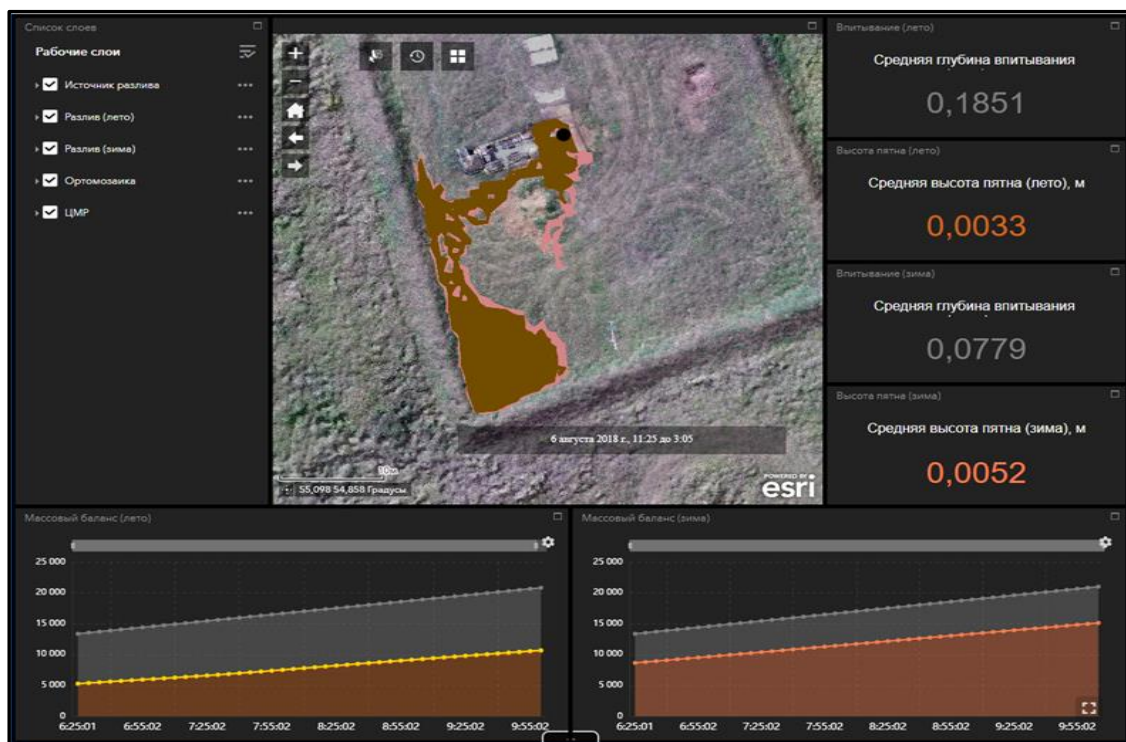


Рис. 4.6. Описание разлива нефти при использовании цифровой модели рельефа [268]

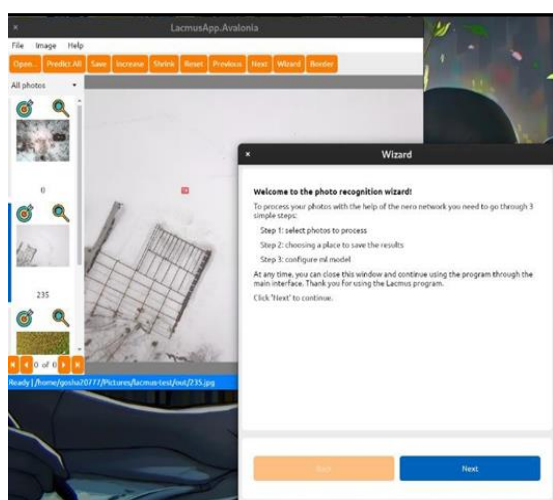
Указанное приложение может быть реализовано в формате мобильного гаджета. На рис. 4.7 отображено изображение, например, которое может быть предоставлено руководителю нефтебазы для просмотра трехмерной модели объекта в режиме офлайн.



Рис. 4.7. Трехмерные объекты
и окружающая местность на мобильном устройстве [268]

Приведем пример обеспечения розыскных задач с применением ИИ. Такие технологии применены отделом криминалистики Следственного управления СК РФ по Волгоградской области для обработки фотографий местности, полученных в ходе мероприятий по поиску пропавших без вести лиц.

В этих целях использовано разработанное ПО *Lastus* с моделями машинного обучения. Программа предназначена для анализа изображений с БАС, позволяя распознавать объекты, не характерные для исследуемой местности, каковыми могут быть фрагменты тела и предметы одежды [28]. Работа программы основана на нейронных сетях и алгоритмах компьютерного зрения, позволяя увеличить эффективность поисковых операций, сократить время на их проведение и, в конечном итоге, повысить вероятность успешного спасения попавших в беду (рис. 4.8).



а)



б)

Рис. 4.8. Пример отображения тела человека (выделено красным)
на снимках (а) и видео (б), полученных с камеры БАС [28]

Вторая группа практических приложений связана с оказанием интеллектуальной и технологической помощи при *проведении следственных мероприятий*. В этом плане одним из главных векторов совершенствования криминалистической науки, активно поддерживаемых ЭКЦ МВД России, является развитие биометрических учетов и новых видов судебных экспертиз. В частности, они касаются развития интеллектуальных технологий, реализующих совместные возможности применения БАС, а также оптического и лазерного 3D-сканирования в качестве новых инструментальных средств [191].

К числу классических следственных мероприятий в экспертно-криминалистической деятельности относится осмотр мест происшествий. При этом для решения типовых и уникальных задач перспективным практическим потенциалом обладает применение технологии оптического и лазерного 3D-сканирования. Его основу составляет использование ранее недоступных возможностей предотвращения утраты следов и объектов, фиксация и изъятие которых традиционными методами затруднены или допускают сбор негодного для исследований материала. Отмеченный же метод располагает технологическими возможностями детально закрепить обстановку места происшествия в виде цветной трехмерной цифровой модели.

Исследование данной модели дает возможность произвести все необходимые измерения, использовать процедуры преобразования исходного изображения с помощью разнообразных приложений, например, изменение цветовой гаммы и ракурсов, позволяющих обеспечить требуемую наглядность, разборчивость, визуализацию зафиксированных особенностей. Исходная модель и ее преобразования фиксируются в цифровом архиве и становятся доступными при обработке следственных и розыскных версий. Продолжением рассматриваемой технологии является 3D-печать, на основе которой могут изготавливаться трехмерные копии объектов с высокоточной передачей идентификационных признаков.

В связи с отмеченными возможностями расширяется использование портативных и стационарных 3D-сканеров, ориентированных для получения трехмерных моделей следов и объектов трасологической, дактилоскопической, пожарно-технической и автотехнической экспертизами.

Для обеспечения деятельности сотрудников экспертно-криминалистических подразделений разработан алгоритм применения обозначенного оборудования при фиксации объемных объектов. Имеющаяся практика его применения убедительно показывает, что с помощью 3D-технологий успешно решаются задачи точного описания обстановки места происшествия.

Примерами являются обследования взаимного расположения транспортных средств на месте дорожно-транспортного происше-

ствия, отдельных сложных следов и объектов, а также оценка типа и мощности взрывных устройств.

Данная технология перспективна при фиксации обстановки места происшествия на основе применения БАС, оснащенных цифровой аппаратурой и видеотехникой, поддерживаемой средствами интеллектуальной обработки и преобразования данных. Это обеспечивает повышенную точность замеров, значительно сокращая время осмотров, а также предоставляя последующий интеллектуальный сервис анализа, оценки и прогнозирования.

Особенно важны данные возможности при осмотрах больших площадей и фиксации многообразной следовой информации. Также это очень актуально при проведении осмотров в труднодоступных и опасных местах. Данная технология применяется как внутри помещений, так и на открытой местности (например, в сгоревших зданиях и сооружениях, а также на прилегающих к ним территориях, лесных массивах, акваториях).

Предложенные модели и методы обучения обладают высоким потенциалом в области архитектурного проектирования. Реализованные в них идеи могут использоваться при автоматизации процессов изготовления планов и схем мест происшествий посредством словесного описания и применения технологии распознавания объектов по видеоизображению.

Цифровое документирование – это область, которая быстро развивается. Технологические достижения вычислительной техники обуславливают появление новых инструментов, с помощью которых можно фиксировать и анализировать окружающие объекты и пространство. Ряд программ и моделей уже применяются при решении конкретных задач, таких как классификация изображений, обнаружение объектов и добавление их в схемы. Например, при использовании биллинга при определении местоположения лица, находящегося под оперативным наблюдением, а также использования при этом специального программного инструмента интеллектуальной обработки данных биллинга.

Интересен опыт проведения анализа состояния наркопреступности в Москве [354, с. 149–150]. Парсинг анонимного сегмента сети дал возможность автоматизированного сбора и систематизация данных о территориальном распространении наркотических закладок. Благодаря этому, получено представление об интенсивности деятельности закладчиков в городе по тепловой карте плотности распределения расфасованного наркотика.

На основе моделирования построены оптимальные маршруты патрульных полицейских нарядов в целях пресечения преступной деятельности в сфере незаконного оборота наркотических веществ в конкретном районе Москвы. Для этого на карту моделируемой территории перенесены необходимые геометки, выделены наиболее рискованные

участки, построены оптимальные маршруты нарядов полиции (один из них отмечен цифрами 1–12 и зеленой линией). Оптимизированный маршрут позволил сократить время патрулирования выделенной территории (рис. 4.9).



Рис. 4.9. Оптимизированный маршрут патрулирования на обслуживаемой территории [354]

Представляется, что данный подход может быть технологически развит добавлением следящего наблюдения с БАС. Это комплексное развитие после соответствующей нормативно-правовой, тактической, технологической доработки способно обеспечить правоохранительные органы разнообразной информацией по широкому спектру общеуголовных и киберпреступлений.

4.3. Геоинформационные системы в аналитическом обеспечении раскрытия и расследования преступлений

Интеграционное объединение геоинформационных систем (ГИС) и их гармоничное включение в информационные системы МВД России уже отмечено выше [90; 92]. Развитие указанной ситуации довольно многогранно и охватывает, по крайней мере, два фактора, отражающих рассматриваемый контекст.

Первый охватывает организационные аспекты совместимости. Кратко обозначим их суть.

Так, сбор розыскных и доказательственных данных определяется эффективным решением следующих вопросов.

1. Совершенствование системы сервисов, имеющих перспективы для правоохранительной и охранной сферы, профилактики катастроф, управления параметрами транспортных средств. Расширение указанного функционала на мобильные устройства, в том числе –

БАС, использующие данные ГИС и входящие в соответствующие технологические процедуры.

2. Информационно-логическое, технологическое, сервисное и иное объединение информационно-телекоммуникационной инфраструктуры ОВД с ГИС, нормативно-правовое и документационное регламентирование циркулирующих информационных потоков и, самое главное, результатов их комплексной интеграции.

3. Включение пространственно-временных данных в систему распознавания, регистрации (в том числе, автоматической), логической обработки, предоставления разнообразных сервисных услуг действующей информационно-телекоммуникационной инфраструктуры ОВД, в первую очередь, ИСОД МВД России.

4. Разработка и внедрение новых сервисов комплексного решения задач раскрытия и расследования преступлений (обеспечение перспективных видов информационно-аналитической обработки данных о лицах, причастных к совершенным правонарушениям, в том числе – киберпреступлениям, объектам противоправной деятельности; выявление связей между материальными и информационными следами, их закрепление на процессуальном уровне).

Решения отмеченных вопросов в целом позволят создать новую технологию работы полиции за счет доступа в реальном масштабе времени к информационным ресурсам МВД России в период несения повседневной службы, а также при возникновении внештатных и аварийных ситуаций, ликвидации террористических угроз и т. д. При этом предполагается:

- интеллектуально поддерживаемый централизованный доступ к базам данных всех уровней, корпоративная почта и т. д.;
- доступ к открытым и закрытым каналам связи, видеоконференциям;
- доступ к системам видеонаблюдения при обеспечении общественного порядка, охране объектов и т. п.;
- сбор необходимой телеметрической, растровой и иной информации со всех видов следящих систем.

Системы спутниковой связи и навигации, позволяющие определить точное местоположения автотранспортных средств, оперативно собрать необходимые пространственно-временные данные, вычислить нужные параметры геолокации, дают возможность собрать сведения о времени, месте и обстоятельствах совершения правонарушений и преступлений, которые далее нужны при формировании доказательственной базы.

Для иллюстрации указанных возможностей обратимся к российскому проекту «ЭРА-ГЛОНАСС». Он обеспечивает автоматическое реагирование и определение необходимости оперативного выезда спецслужб на места автоаварий; охрану транспортных средств с определением их местоположения с точностью до 1 м. Эта система также

способна противодействовать проникновению злоумышленников в салон, попыткам ее взлома, обеспечивая посылку специального предупреждения водителю или диспетчеру, автоматическое подключение служб, фиксирующих местонахождение автомобиля, возможность блокировки его движения, игнорирование и блокирование излучений глушителей радиосигнала.

Аналогичные противоугонные функции реализуются и другими спутниковыми охранными системами (например, «Эшелон» и «Аркан»), которые также способны помочь в раскрытии, расследовании таких преступлений, получении ориентирующей, оперативно-розыскной или доказательной информации.

Спутниковые противоугонные системы помогают в организации тактических мероприятий («машины-ловушки», аппаратура для скрытого наблюдения за подвижными объектами и т. д.), раскрытии преступлений, не только связанных с угоном автотранспорта.

Наряду с противоугонными системами, развиваются и другие, перспективные направления применения систем космической связи и навигации. Навигационная информация предоставляет новые возможности по установлению времени, места и лиц, причастных к совершению преступлений. Например, в процессе раскрытия и расследования преступлений, в том числе – террористической направленности (оборот оружия, взрывчатых и других запрещенных веществ). Также активно применяется *online*-мониторинг при организации исполнения наказаний, не связанных с лишением свободы, при проведении различных ОРМ.

Пространственно-временная информация становится важной для разрешений многих неопределенных ситуаций, особенно при отсутствии материально зафиксированных следов. Эта информация о находившихся в момент совершения преступления лицах и объектах в данном месте может быть использована и как ориентирующая, и как обладающая перспективностью для различных процессуальных форм применения.

Продолжающееся развитие системы космической связи для сегмента, используемого в МВД России, идет по пути создания крупномасштабных корпоративных сетей с магистральными каналами связи большой протяженности. Спутниковым системам связи отводится важная роль в качестве дополнения к наземным сетям связи специального назначения, которые продолжают развиваться на основе волоконно-оптических линий связи. Среди предлагаемых отметим технологию VSAT (сеть малых спутниковых земных станций) как объединяющую возможности передачи данных цифровой телефонии, телевидения, видео-конференц-связи, доступа к ресурсам интернета.

В процессе интеграции с правоохранительной информационной инфраструктурой ключевым элементом в работы инструментов ИИ является база знаний, на которой обучаются модели. Внедрение ИИ

связано с формированием полных, достоверных наборов данных. Очень важен вопрос как их верификации, так и работы моделей [401].

Следует отметить, что источниками данных в ряде случаев служат устаревшие информационные системы ОВД. Поэтому именно высококвалифицированные специалисты должны заниматься вопросами создания баз знаний, определения полноты и достоверности, последующей актуализации, а также интеграции информационных систем, стыковки информации, получаемой из разных баз данных. Обучение моделей должно исходить из тезиса, что не надо слепо доверять интеллектуальным результатам моделирования, а профессионально их осмысливать на основе следующих рекомендаций:

- обязательный *человеческий контроль*. *LLM* должны быть инструментом поддержки, а не заменой следователей, оперативников, экспертов-криминалистов и иных специалистов;

- регулярное *тестирование и аудит* моделей на точность и этичность;

- обеспечение *открытости результатов*. Публичное обсуждение внедрения ИИ укрепит доверие граждан;

- использование *специализированных наборов данных для обучения моделей*. Оно должно проводиться на данных, релевантных локальному контексту (язык, законодательство) и верифицированных высококвалифицированными специалистами. Для верификации также может быть применен метод внешней проверки или *external validation*. Этот метод предполагает обращение к независимой модели или системе оценки качества и надежности по отношению к основной модели.

Интеграция ИИ в сферу общественной безопасности требует эффективного правового регулирования. Среди необходимых шагов здесь – принятие законов, формирование передовых стандартов и протоколов тестирования и сертификации ИИ-продуктов перед внедрением в деятельность правоохранительной системы, разработка правил ответственности производителей и пользователей интеллектуальных систем. Подчеркнем, что усиление правовой базы создаст необходимые условия для безопасного внедрения и эксплуатации инновационных технологий, минимизируя риски злоупотреблений и ошибок.

Таким образом, развитие цифрового полицейского инструментария должно основываться на интеграции передовых технологий и обеспечении надежной инфраструктуры для эффективной реализации новых функций. Однако важно помнить, что новые технологии требуют комплексного подхода к решению вопросов безопасности, права и свободы личности, обеспечивающих доверие общества к современным методам ведения борьбы с преступностью в целом и киберпреступностью – в частности.

Второй аспект связан с логическими, алгоритмическими, аппаратно-технологическими вопросами совместимости и объединения,

расширяющими возможности интеллектуального информационно-аналитического обеспечения правоохранительной деятельности.

Выше уже говорилось о том, что сегодня активно применяются многослойные и векторные информационные карты (с возможностью подключения новых слоев, их заменой и т. д.), медиаархивы видеоданных и зафиксированных событий, реализовано подключение баз данных систем, обеспечивающих оперативно-служебную деятельность ОВД. Интерфейс таких систем является активным, с расширением, например, по отображению техники, оснащенной датчиками ГЛОНАСС: городские и областные автобусы, машины скорой помощи, служебные машины МВД России.

Напомним и еще обо одной опции – геопривязанных панорамных изображениях, получаемых с помощью специальных интеллектуальных приложений, склеивающих отдельные кадры в единую картину. Основные преимущества этого решения состоят в следующем:

- обзорные снимки получаются по локальным площадям до 2-х кв. км с детализацией, недостижимой при использовании космических снимков, а также невозможной при наземной съемке;
- реалистичные 3D модели в трехмерных сценах получаются всего за несколько часов. Отметим, что специализированные пакеты на подобное построение требуют до 2-3-х недель;
- интеллектуальная обработка базируется на использовании сверхвысокого пространственного разрешения при моделировании сложных явлений (разлив нефти, затопление территории, оценка объемов, площадь распространения наркотикосодержащих растений, ущерб от хищений биоресурсов, осмотр места происшествия и т. д.). Это существенно повышает достоверность различных численных расчетов.

Возможности рассматриваемой технологии частично иллюстрируются на рис. 4.10 [224].



Рис. 4.10. Этапы обработки и анализа массивов изображений дистанционного зондирования [224]

К возможностям обозначенных космических и беспилотных технологий, которые активно включаются в информационно-аналитическое обеспечение правоохранительной деятельности, представляется уместным добавить еще и возможности аэростатических мобильных платформ [82].

Рассмотренные технологии представляют собой не только инструменты обнаружения потенциальных угроз, но и средства предотвращения преступлений, защиты общественных мест, отдельных граждан и повышения уровня безопасности в целом.

Важность этих технологий заключается в их способности быстро и эффективно обнаруживать угрозы, предотвращать криминальные события, реагировать на них. Использование передовых технологий в области безопасности играет ключевую роль в защите жизни и имущества граждан, обеспечивая более безопасное и устойчивое развитие общества.

4.4. Автоматическое распознавание и маршрутизация беспилотных транспортных средств

Материал раздела относится к рассмотрению задач *автоматического распознавания*, к которой авторы подробно обращались в работе [84]. Процесс автоматического распознавания объединяет процедуры идентификации, аутентификации, авторизации.

Аутентификация БТС представляет собой процесс гарантированного подтверждения подлинности. Для предоставления основным субъектам (БТС, операторы БТС, владельцы БТС) доступа к ресурсам и/или операциям в системе процесс аутентификации является обязательным шагом.

Основные этапы процесса предоставления доступа.

1. *Идентификация*, определяющая наличие у субъекта системы определенного права доступа к ресурсам. Например, каждый беспилотник должен обладать уникальным идентификатором (регистрационным номером).

2. *Проверка достоверности*, когда оцениваемый субъект подтверждает достоверность и свое соответствие идентифицированному субъекту, заявленным данным владельца или оператора. При этом обычно используется комбинация методов:

- криптографические протоколы – использование цифровых подписей и *TLS*-сертификатов для проверки подлинности отправленных сообщений от беспилотника;
- физические средства защиты – специальные метки или датчики, встроенные непосредственно в конструкцию БТС, препятствующие несанкционированному использованию;

– контроль канала связи – проверка целостности каналов передачи данных между оператором и беспилотником посредством системы специального шифрования.

3. *Авторизация*, формирующая разрешение доступа к определенным ресурсам или операциям после успешной аутентификации. Параметры и возможности авторизации зависят от уровня полномочий субъекта системы, отвечающего за данный функционал.

Идентификация обеспечивает процесс распознавания и однозначного определения конкретного БТС среди множества подобных. Этот процесс необходим для контроля и управления как отдельными БТС, так и для организации движения множества БТС, отслеживания их движения в пространстве, обеспечения системной безопасности.

Идентификация БТС производится по их уникальным отличительным признакам и/или по уникальным идентификаторам – символьным последовательностям, присваиваемым БТС при производстве/регистрации. Кратко поясним наиболее распространенные методы и подходы в организации идентификации БТС:

– *RFID-метки* (Radio Frequency Identification) – радиочастотная идентификация, когда каждая единица оборудования оснащается специальным чипом с уникальным номером. Чип передает сигнал на считывающее устройство для распознавания и регистрации БТС. Ее плюсы: простота, низкая стоимость, высокая надежность;

– *GPS-трекеры* – для отслеживания *GPS*-навигаторами точного пространственного положения БТС в режиме реального времени. Сигнал передается на сервер, где информация сохраняется и доступна уполномоченным органам. Система обеспечивает высокую точность позиционирования, но эффективность зависит от качества сигнала спутников и наличия препятствий;

– *баркодирование*, когда на корпус БТС наносится уникальный штрих-код. Он сканируется специальными камерами для определения принадлежности. У способа низкая стоимость реализации, но уязвимость перед механическими повреждениями и фальсификацией;

– *биометрические маркеры* владельцев или эксплуатирующего персонала обеспечивают проверку уникальных физических характеристик оператора (например, отпечатков пальцев, сетчатки глаза). Этот метод эффективен в ситуациях, когда важно установить личность конкретного лица, управляющего транспортным средством. Тем не менее, биометрию сложно применять массово, ввиду сложности организации постоянного тестирования и хранения больших объемов персональных данных с поддержанием ответственности за них;

– *радиочастотные маячки*, которые установлены на БТС и работают на определенной частоте, непрерывно излучая сигнал с уникальной информацией. Приемные станции фиксируют сигналы и обеспечивают отслеживание передвижений. Технология устойчива к помехам и обладает хорошей дальностью действия;

– *оптическое распознавание образов* на основе использования камер высокого разрешения, которые анализируют БТС дистанционно и автоматически по визуальным признакам (форме корпуса, логотипам производителя и т. д.). Технология особенно полезна там, где отсутствуют препятствия для съемки и есть хорошее освещение. Недостатком является зависимость от условий окружающей среды и низкая надежность при плохих погодных условиях.

Выбор способа идентификации беспилотных транспортных средств зависит от конкретных требований и обстоятельств эксплуатации. Наличие области применения и ограничений часто обосновывает использование комбинации нескольких способов для повышения общей эффективности системы управления и контроля.

В России вопросы идентификации и аутентификации закреплены в постановлении Правительства РФ от 30 ноября 2024 г. № 1701 «Об утверждении требований к оснащению пилотируемых воздушных судов и беспилотных авиационных систем оборудованием связи, навигации, наблюдения, автоматического предотвращения столкновений, к оснащению беспилотных авиационных систем оборудованием удаленной идентификации и оборудованием линий управления беспилотными авиационными системами и контроля беспилотных авиационных систем, средствами криптографической защиты информации, сертифицированными в соответствии с требованиями федерального органа исполнительной власти в области обеспечения безопасности, и Правил оснащения пилотируемых воздушных судов и беспилотных авиационных систем оборудованием, предусмотренным пунктом 1 статьи 78.3 Воздушного кодекса Российской Федерации» [19].

Внедрение технологий ИИ в рассматриваемую сферу определяет ситуацию, что интеллектуальные методы становятся ключевыми в целях обеспечения безопасности, управления движением и интеграции автономных систем в транспортную инфраструктуру. Это обстоятельство определяет определенную трансформацию в задачах идентификации БТС, которые сейчас решаются на основании:

- обнаружения беспилотника в зоне наблюдения;
- распознавания типа транспортного средства;
- трекинга пространственной траектории движения в реальном времени;
- аутентификации – проверки легальности БТС.

Основное применение при этом в настоящее время нашли следующие технологии ИИ:

– *компьютерное зрение* с использованием нейросетей (*CNN*, *Transformer*) для анализа визуальных признаков с камер. Примеры проектов: *YOLO*, *Faster R-CNN*;

– *датчики и сенсоры*, к которым относят лидары, радары и ультразвуковые датчики для создания 3D-карты местности, обеспечивают сбор данных об окружении БТС, его состоянии. Для обработки полу-

ченных сведений применяют алгоритмы машинного обучения (например, *PointNet* для лидарных данных);

- *V2X (Vehicle-to-Everything)* обеспечивает беспроводную коммуникацию между БТС и инфраструктурой (например, через стандарты *DSRC* или *5G*), а ИИ анализирует передаваемые метаданные (*ID*, скорость, маршрут);

- *акустический анализ* для распознавания звуковых сигнатур двигателей или пропеллеров (актуально для БПЛА в условиях СВО).

Другое направление использования ИИ ориентировано на распознавание и классификацию объектов. Здесь применение нашли различные методы машинного обучения:

- *глубокое обучение* моделей применяется в случае больших наборов данных (например, для дронов – *UAVDT*), а трансформеры (например, ViT) улучшают точность моделирования;

- *ансамбли моделей* на базе комбинаций разных алгоритмов повышают надежность функционирования управляемого объекта;

- метод *Few-shot learning* обеспечивает обучение на ограниченном количестве примеров. Метод подходит, когда машину необходимо обучить идентифицировать БТС в условиях ограниченных ресурсов, данных (например, для новых моделей БТС), времени или вычислительных мощностей.

Вместе с тем остается еще много нерешенных задач как научного, так и практического характера. Это – доверие и безопасность; уязвимости перед атаками (например, атаки на камеры); обеспечение конфиденциальности; риски утечек данных при трекинге; применимость инструментов в сложных условиях; работа в плохую погоду или при помехах радиосвязи.

Требуют совершенствования также вопросы стандартизации и унификации, отсутствуют единые протоколы идентификации для разных производителей. Это обусловлено развитием технологий (например, квантовых сенсоров или нейроморфных чипов), когда точность будет расти, а массовое внедрение беспилотников ускорится.

Возникнут проблемы в идентификации, связанной с интеграцией БТС в системы организации движения пилотируемого транспорта. Прежде всего, это системы умных городов – сервисы мониторинга беспилотных курьеров и такси в городах, логистики на транспорте и организации мультимодальных перевозок, а также военной сферы – опознавание своих и вражеских дронов.

ИИ меняет подходы в автоматизации планирования маршрутов беспилотного транспорта, маршрутизации БТС в движении. Это позволяет отдельным БТС и их флотам выбирать наиболее эффективные пути с учетом множества факторов, динамически адаптироваться, осуществлять групповую маршрутизацию и т. д.

Для решения перечисленных задач используются различные ме-

тоды, алгоритмы и технические средства. Например, алгоритмы Дейкстры, Флойда-Уоршелла, A^* (*A-star*), Муравьиный.

Алгоритмы и методы ИИ для маршрутизации основаны на машинном обучении и глубоком обучении: нейросетевые модели, обучение с подкреплением (*RL*), графовые нейросети. Особая группа – эволюционные и роевые методы и алгоритмы: генетические алгоритмы (*GA*), методы оптимизации (*PSO – Particle Swarm Optimization*).

В итоге непосредственно для БТС технологии ИИ обеспечивают реализацию специфических функций в управлении. К их числу относятся, например, локальная навигация и огибание препятствий; глобальная маршрутизация и поиск оптимальных маршрутов; избегание зон запретов полетов; оптимизация расхода энергии батарей, топлива за счет маршрутов и/или времени рейса при сниженной ветровой нагрузке.

Полученные достижения сосуществуют и с рядом вызовов, которым предстоит еще найти пути для эффективного разрешения. Например, это преодоление вычислительной сложности для больших городов; снижение вероятности нежелательных воздействий от неопределенностей среды (непредсказуемые события); этические вопросы (допустим, приоритеты в аварийных ситуациях). Перспективность в этих задачах видится в применении квантовых алгоритмов для ускорения расчетов, ИИ и технологий блокчейна для децентрализованного решения задач маршрутизации, создания полностью автономных транспортных средств, что снизит влияние человеческого фактора, исключит многие ошибки, ведущие к транспортным происшествиям.

После отмеченных положений несколько слов отведем основному вопросу монографии: организации противодействия преступлениям, связанных с развитием технологий ИИ и больших данных для предсказания мест, времени и участников преступлений.

Выше уже отмечались реализации моделей, позволяющих анализировать средствами ИИ исторические данные и, в конечном итоге, выявлять «горячие точки» преступности. В контексте сказанного социальные сети и чаты требуют применения ИИ при мониторинге подозрительной активности на предмет планирования преступлений, распространения ложной информации, целенаправленного дезинформирования и клеветы.

Еще одним рассмотренным срезом является технология автоматического распознавания разыскиваемых лиц и автомобилей в потоковой информации с камер наружного наблюдения. Собранные данные могут становиться основой для работы интеллектуальных моделей, определяющих корреляционные связи между появлением БТС, людей в районах совершения преступлений с их подготовкой, организацией и реализацией противоправных действий.

Использование преступными элементами технологий ИИ для расчета путей отхода ведет к встречному противодействию: интеллект-

туальному предсказанию маршрутов преступников на основании имитационного моделирования возможных сценариев движения, отработки блокирования ключевых точек (мосты, развязки, иные особенности препятствий).

Мониторинг поведения БТС позволяет детектировать аномалии в движении БТС. Так могут быть выявлены подозрительные маршруты (например, машина кружит без цели – возможная разведка) или предотвратить запрещенную активность БТС, например, ночные полеты в запрещенных зонах.

На структурные подразделения, по сути, выполняющие функции киберполиции возлагаются задачи выявления и «взламывания» криминальных ИИ-систем; внедрения в *darknet*-форумы по продаже преступникам ИИ-инструментов; использования враждебных атак на ИИ, например, подбрасывание фейковых данных, чтобы нарушить работу алгоритмов контрабандистов.

Автоматизированная слежка с применением БПЛА и умных камер с ИИ позволяют распознать подозрительное поведение, получать информацию по подготовке, совершению преступлений, сокрытию их следов.

Отдельным направлением может выступать блокировка алгоритмов обнаружения подозрительной маршрутизации. Системы ее обнаружения используют подход, в котором применяется поведенческий анализ, выявление признаков «разведывательного» поведения, обнаружение попыток обхода виртуальных границ. Алгоритмы выявляют отклонения в движении БТС – движение по странной траектории без очевидной причины или неестественное изменение траектории вследствие аварии, обнаруживают «странные» остановки или петли на маршруте.

В данных алгоритмах проводится динамическая верификация маршрутов, проверяется соответствие заявленного и фактического маршрутов, контролируется целостность навигационных данных, ведется детекция *GPS*-спуфинга. Для получения данных о БТС осуществляются сложные интеграции и сбор данных с камер, радаров, лидаров; перекрестная проверка *GPS*-координат с визуальным позиционированием; анализируется телеметрия (расход энергии, скорость, ускорение).

Следует отметить, что регуляторные инструменты не всегда так эффективны, как технические. Поэтому в деятельности полиции для успешного противодействия следует создать и поддерживать технологическое преимущество над возможностями и инновациями, применяемыми в преступной среде.

Таким образом, нами рассмотрены основные понятия, связанные с задачами автоматического распознавания и маршрутизации БТС. Далее рассмотрим процесс принятия решений, определяемых результатами автоматического распознавания и обоснованных требованиями безопасности.

Принятие решений по безопасности ориентировано на классический подход опознавания или удаленной идентификации по принципу «свой-чужой»:

1) для положительно идентифицированных БВС – поддержка системы управления в безопасном состоянии при выполнении штатных заданий;

2) для отрицательно идентифицированных БВС – определение мер принудительного воздействия: безопасное сопровождение; уничтожения; смена маршрутного задания; захват; пресечение реализации киберугроз и совершения киберпреступлений.

Обозначенные меры принудительного воздействия на БВС, как видно, имеют широкий спектр возможностей. Одно из радикальных направлений связано с физическим уничтожением БВС или полным прекращением его вредоносного потенциала.

В этом плане не будем анализировать развернутые сведения, они рассмотрены в открытых источниках. Ограничимся только напоминанием о недавних успешных испытаниях российских лазерных систем в противодействии беспилотникам [104] и о методах РЭБ. По последнему направлению предлагаем краткую информацию о продуктах двух ведущих организаций, творчески сотрудничающих с авторами в вопросах безопасного управления беспилотным транспортом.

Они ведут теоретико-практические изыскания и создают приложения, придерживаясь принципа «ИИ против ИИ». Интерес к разработкам этих компаний состоит в тех потенциальных возможностях, которые могут быть непосредственно реализованы в практической деятельности ОВД по противодействию общеуголовной и киберпреступности.

Первая компания – специализированное конструкторское бюро (СКБ) Т-АВИАС, создающая информационно защищенные БПЛА и системы по противодействию БПЛА (рис. 4.11).

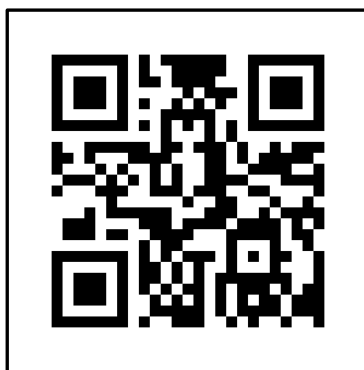


Рис. 4.11. QR-код
СКБ Т-АВИАС

Разработки СКБ Т-АВИАС направлены на обеспечение защиты объектов критической инфраструктуры, безопасность населения. Стратегия развития компании базируется на следующих принципах.

Безопасность и стабильность в современном мире, где БАС могут быть использованы не только военными, но и террористическими или криминальными группировками, должна поддерживаться внедрением интегрированных решений защиты. Тем самым формируется надежная технологическая и кибербезопасность государства, общества и граждан.

В ряду наиболее распространенных изделий компании считаются системы обнаружения и нейтрализации БПЛА. Они содержат: подаватели дронов и антидроновые ружья, комплексы противодействия FPV-дронам, всенаправленные детекторы БПЛА, модули обнаружения, модули генерации радиопомех.

Некоторые примеры изделий, выполненных в СКБ Т-АВИАС, приведены на рис. 4.12.



Рис. 4.12. Основные модули системы СКБ Т-АВИАС

Вторая организация – это компания *3mx*, QR-код которой приведен на рис. 4.13.



Рис. 4.13. QR-код
компании *3mx*

Компания *3mx* представлена на рынке радиоэлектроники и связи более двадцати лет. Основное направление работы – борьба с БПЛА.

Готовые и модернизированные системы успешно показали себя не только в зоне СВО, но, кроме того, появились пилотные проекты для правоохранительных органов. Важным и перспективным направлением в деятельности компании является обеспечение комплексной безопасности массовых мероприятий. Это, например, ПМЭФ-2024, «Алые паруса-2024», Международный военно-морской салон «ФЛОТ-2024», саммит Евразийского экономического союза.

Основные изделия компании *3mx* приведены на рис. 4.14.

		
Портативный подавитель БПЛА «Айрат 100» v.3	Автоматический комплекс противодействия FPV-дронам «Сания»	Портативный всенаправленный детектор БПЛА «Булат» v.4

Рис. 4.14. Основные изделия компании *3mx*

4.5. Выводы по главе 4

1. Важной задачей предотвращения экологических и иных катастроф и стихийных бедствий, а также решения многих задач правоохранительной деятельности является необходимость создания эффективной системы раннего обнаружения, предупреждения и реагирования, которая определяет актуальность применения новых технологий мониторинга и детектирования с использованием интеллектуальных средств видеонаблюдения, машинного зрения и БАС.

2. Сложно решаемым является вопрос автоматизации мониторинга и детектирования экологической и криминогенной ситуации в труднодоступных местах (лесные массивы, горная местность) из-за отсутствия стабильных каналов связи для передачи видеопотока высокого разрешения. В таких условиях важной становится разработка систем автоматизации управления полетами БАС для выполнения регулярных облетов территорий в соответствии с полетным заданием, которое должно передаваться на борт летательного аппарата посредством защищенных протоколов беспроводной передачи данных.

3. Защита БАС, используемых вблизи критически важных объектов, требует защиты данных, надежного управления доступом, мониторинга и обнаружения угроз и аномалий, защиты каналов связи, оперативного обновления программного обеспечения и патчей безопасности, соответствия нормативным требованиям, резервирования отказоустойчивости, анализа рисков и моделирования сценариев кибератак. Для эффективного решения задачи защиты БАС от киберугроз разрабатывается аппаратно-программная распределенная информационная система мониторинга.

4. Объектами защиты являются система управления БАС, система связи и передачи данных, мультиспектральный комплекс видеонаблюдения, аппаратно-программный комплекс мониторинга территорий, программное обеспечение превентивного обнаружения техногенных катастроф и аномалий криминогенной обстановки с применением машинного зрения и ИИ.

5. Экспертно-криминалистическая деятельность ОВД, как и многие другие направления правоохранительной работы, стали средой для применения технологий ИИ. Среди таких направлений – фото-, видеонаблюдение оперативно-служебного, профилактического назначения; организация оперативной связи; поддержка проведения оперативно-розыскных и следственных мероприятий; противодействие морскому пиратству; фиксация незаконной разработки недр, хищения биоресурсов, выращивания растений, содержащих наркотические средства и т. д.

6. Одним из главных векторов совершенствования криминалистической науки является развитие биометрических учетов и новых видов судебных экспертиз. В частности, они касаются развития интеллектуальных технологий, реализующих совместные возможности применения БАС, а также оптического и лазерного 3D-сканирования в качестве новых инструментальных средств. Отмеченный метод располагает технологическими возможностями детально закрепить обстановку места происшествия в виде цветной трехмерной цифровой модели.

7. Исследование цифровой модели дает возможность произвести все необходимые измерения, использовать процедуры преобразования исходного изображения с помощью разнообразных приложений, например, изменение цветовой гаммы и ракурсов, позволяющих обеспечить требуемую наглядность, разборчивость, визуализацию зафиксированных особенностей. Исходная модель и ее преобразования фиксируются в цифровом архиве и становятся доступными для отработки следственных и розыскных версий, инициируемых в ходе процессуального разбирательства с собранными первичными данными.

8. Интеграция геоинформационных систем с автоматизированными учетами МВД России призвана создать новую технологию работы полиции за счет доступа в реальном масштабе времени ко всем ресурсам МВД России в сочетании с космическими технологиями. При-

менение этой технологии актуально в период несения повседневной службы, а также при возникновении внештатных и аварийных ситуаций, ликвидации террористических угроз и т. д.

При этом система спутниковой связи и навигации позволяет точно определить местоположение автотранспортных средств, собрать пространственно-временные данные об объектах в той или иной аномальной ситуации, вычислить различные параметры геолокации.

9. Эксплуатация БАС с учетом применения технологий ИИ позволяет реализовать такие приложения, как:

- обеспечение кибербезопасности систем дистанционного мониторинга территорий;
- создание новых возможностей аппаратно-аналитической поддержки современной и перспективной экспертно-криминалистической деятельности;
- интеграция с геоинформационными системами для совершенствования информационно-аналитического обеспечения раскрытия и расследования киберпреступлений;
- решения по обеспечению безопасности в оперативных задачах автоматического распознавания объектов наблюдения и управления маршрутизацией БАС.

Глава 5. Выбор технических и нормативных решений для создания цифровой платформы управления беспилотными системами

Цифровая платформа предназначена для создания распределенных защищенных автоматизированных систем контроля и управления БАС. Ее цель – обоснование рациональных требований, формирование облика и определение достижимого уровня технологий, их характеристик для построения сети центров контроля и управления движением БАС. Макетный образец цифровой платформы БАС необходим для первоначальной проверки корректности принятых технических решений, а также принципов ее построения и разработки.

Развитие нормативно-правовой, нормативно-технической базы, методических документов в области беспилотной авиации, контроля и управления движением БВС должно осуществляться в рамках «дорожной карты» по совершенствованию законодательства и устранения административных барьеров, а именно Плана реализации Концепции интеграции БВС в единое воздушное пространство (ВП) [22]. Концепция предусматривает три этапа интеграции:

Первый (организационный, до 2023 г.) – внедрялись сервисы электронной регистрации и учета БВС, удаленной идентификации БВС, находящихся в полете.

Второй (технологический, до 2027 г.) – автоматизированное планирование использования ВП беспилотными и пилотируемыми воздушными судами, технологии обеспечения безопасного выполнения полетов БВС, инфраструктуры связи, навигации и наблюдения.

Третий (цифровой, до 2030 г.) – внедрение средств динамического геозонирования ВП, обеспечение цифрового интерфейса взаимодействия эксплуатантов и внешних пилотов БВС с ОрВД, разрешения конфликтных ситуаций на тактическом уровне (в процессе полета) на базе цифровых платформ.

В главе даны характеристики рациональных технических решений для макетного образца защищенной цифровой платформы БАС, базирующиеся на соответствующей нормативно-технической базе.

5.1. Международные и национальные стандарты Российской Федерации в области беспилотных авиационных систем

К началу 2025 г. в РФ утверждены и введены в действие восемь национальных стандартов:

1) ГОСТ Р 57258-2016. Системы беспилотные авиационные. Термины и определения [43].

В стандарте введены термины и определения беспилотных воздушных судов и авиационных систем, а также дистанционно пилотируемых воздушных судов и беспилотных систем;

2) ГОСТ Р 59517-2021. Беспилотные авиационные системы. Классификация и категоризация. Стандарт устанавливает [39]:

- классификацию и категории БАС для определения требований по обеспечению безопасности полета, необходимого объема работ по сертификации «Разработчика», «Образца», «Изготовителя» БАС;

- правила использования ВП;

3) ГОСТ Р 59751-2021. Беспилотные авиационные системы с беспилотными воздушными судами самолетного типа. Требования к летной годности [38].

Документ устанавливает требования к летной годности и распространяется на БАС, в состав которых входят БВС самолетного типа, имеющие максимальную взлетную массу от 30 до 5 700 кг. Требования применяют при формировании сертификационного базиса, обеспечивающего безопасную эксплуатацию БАС, относящихся к сертифицируемой категории по ГОСТ Р 59517;

4) ГОСТ Р 59520-2021. Беспилотные авиационные системы. Функциональные свойства станции внешнего пилота [41].

Он устанавливает требования к функциональным свойствам станций внешнего пилота в составе БАС;

5) ГОСТ Р 56122-2014 Воздушный транспорт. Беспилотные авиационные системы. Общие требования [42].

В нем регламентированы требования к БАС и их элементам при разработке, производстве, сертификации, эксплуатации, согласовании единообразного подхода к процедурам, касающимся гражданских БАС;

6) ГОСТ Р 59519-2021. Беспилотные авиационные системы. Компоненты беспилотных авиационных систем. Спецификация и общие технические требования [40].

Стандарт устанавливает состав (спецификацию) БАС и общие технические требования к их компонентам;

7) ГОСТ Р 70802-2023. Беспилотные авиационные системы для обеспечения пожаротушения, аварийно-спасательных и других работ, выполняемых в целях предупреждения чрезвычайных ситуаций и ликвидации их последствий. Общие требования [37].

Представлены общие требования к БАС, применяемым при тушении пожаров, обеспечении аварийно-спасательных и других работ в экстремальных условиях;

8) ГОСТ Р 54344-2011. Техника пожарная. Мобильные робототехнические комплексы для проведения аварийно-спасательных работ и пожаротушения. Классификация. Общие технические требования. Методы испытаний [44].

Ссылочный документ в ГОСТ Р 70802-2023 по классификации и общим техническим требованиям применительно к БАС.

Мировые тенденции по контролю и управлению движением БВС отражены в следующих документах:

1) *Doc. 10019 ICAO. Руководство по дистанционно пилотируемым авиационным системам (ДПАС)* [30] одобрено ИКАО в 2015 г. и направлено на обеспечение безопасной интеграции ДПАС в ВП.

Основные цели документа включают разработку международной нормативной базы, основанной на стандартах и рекомендуемой практике, которые обеспечат безопасные полеты ДПАС на уровне, сопоставимом с воздушными судами с пилотом на борту.

В документе обсуждается развитие нормативных требований для беспилотных летательных аппаратов, начиная с Парижской конвенции 1919 г. и до Чикагской конвенции 1944 г., с последующими обновлениями. Особое внимание обращается на контроль за беспилотными аппаратами для предотвращения угроз гражданским воздушным судам.

Руководство подчеркивает важность разработки согласованных технических требований и стандартов для БАС. Отмечается, что ИКАО играет координирующую роль, сотрудничая с международными организациями в разработке таких требований.

В результате документ является важным шагом в регулировании использования БАС и их интеграции в международное ВП, что требует согласованных действий многих заинтересованных сторон;

2) *Приложение 10 к Конвенции о международной гражданской авиации «Авиационная электросвязь», а также Том VI «Системы и правила, относящиеся к линии C2 дистанционно пилотируемых авиационных систем».*

Том VI Приложения 10 ИКАО [29] является ключевым документом, устанавливающим международные требования к системам и процедурам управления и контроля (C2) для безопасной интеграции ДПАС в глобальную систему гражданской авиации;

3) *Doc. 10039 ICAO. Руководство по концепции общесистемного управления информацией (SWIM)* [34].

Данная разработка ИКАО представляет собой фундаментальный документ, закладывающий основы для реализации SWIM (*System Wide Information Management*) как ключевого элемента глобальной системы организации воздушного движения (ОрВД). Документ освещает цели, принципы, преимущества, компоненты и этапы внедрения SWIM.

Концепция SWIM направлена на повышение эффективности обмена информацией в сфере ОрВД путем своевременного предоставления нужной информации соответствующим участникам через стандартизированные сервисы и инфраструктуру. Это позволит повысить ситуационную осведомленность, качество принятия решений, гибкость и экономичность взаимодействия, а также поддержать будущие усовершенствования ОрВД.

В основе *SWIM* лежит сервис-ориентированная архитектура, предполагающая разделение предоставления и потребления информации, слабую связанность систем и использование открытых стандартов. Принципами *SWIM* являются:

- использование интероперабельных информационных прикладных сервисов;
- разделение функций поставщика и потребителя информации;
- открытые стандарты;
- защищенный обмен информацией;

4) *Doc. 9869 ICAO. Руководство по связи и наблюдению, основанное на характеристиках* [36].

По сути своей является он ключевым документом, определяющим принципы и процедуры внедрения систем связи и наблюдения в авиации. Этот документ предоставляет всеобъемлющее руководство для регулирующих органов, поставщиков аэронавигационного обслуживания, авиакомпаний и других заинтересованных сторон.

Данное регламентирование возникло как ответ на растущую потребность в более эффективном использовании ВП и увеличении пропускной способности системы ОрВД. Традиционные системы связи и наблюдения, основанные на жестких правилах и разделениях, становятся все менее пригодными для удовлетворения потребностей современной авиации.

Документ предлагает более гибкий и адаптивный подход, при котором требования к характеристикам систем определяются на основе фактических потребностей и условий ВП. Это открывает возможности для более эффективного использования ресурсов, снижения затрат и повышения гибкости системы ОрВД.

Кроме того, подробно описывается процесс определения требуемых характеристик связи и наблюдения для различных типов операций и воздушных пространств. В этих целях представлены оба подхода для выбора необходимых характеристик:

- требования к производительности системы связи (такие как время транзакции, целостность и доступность) определяются на основании рекомендаций *RCP (Required Communication Performance)*;
- формирование требований к производительности системы наблюдения (точность, целостность, доступность и время обновления) выделяются по подходу *RSP (Required Surveillance Performance)*;

5) *Doc. 9882 ICAO. Руководство по требованиям к системе организации воздушного движения* [32].

В документе дается краткий обзор его взаимосвязи с другими ключевыми документами ИКАО по ОрВД, такими как «Глобальная эксплуатационная концепция ОрВД», «Глобальные характеристики» и «Основные принципы перехода к основанной на характеристиках системе»;

б) *Doc. 9694 ICAO. Руководство по применению линии передачи данных (ЛПД) при обслуживании воздушного движения* [35].

Данный документ разработан в целях:

- объяснения концепции системы управления воздушным движением на основе ЛПД и требований по связи для цифрового обмена сообщениями при обслуживании воздушного движения;

- определения того, каким образом управление, основанное на использовании ЛПД, улучшит существующее обслуживание воздушного движения;

- обеспечения руководящего материала для авиационных полномочных органов, пользователей ВП и представителей системы обслуживания:

- а) по описанию концепции и системы;

- б) описанию эксплуатационных процедур;

- в) рассмотрению возможностей автоматизации;

- г) реализации стратегии перехода, которые дают руководящие принципы, включая описание конкретных видов обслуживания;

7) *Doc. 9896 ICAO. Руководство по сети авиационной электросвязи (ATN), использующей стандарты и протоколы пакета протоколов интернет (IPS)* [31].

Данное руководство разработано ИКАО в целях определения минимальных требований к организации сети ATN на основе использования протокола IP. Руководство подготовлено для обеспечения функциональной совместимости различных реализаций ATN/IPS между государствами и международными организациями на основе единых принципов и подходов.

В тексте руководства даются общие рекомендации по выбору физических линий передачи данных, планированию адресного пространства IP, обеспечению мобильности пользователей, информационной безопасности, качеству обслуживания. Кроме того, приводятся примеры конфигурации сети, сценарии развертывания, варианты переходных решений. Справочный раздел содержит ссылки на релевантные стандарты ИКАО, IETF, EUROCAE и другие документы;

На сегодняшний день разработано еще около двух-трех десятков важных документов международного уровня, в которых раскрываются многие другие детали стандартов, правил, нормативов, необходимых к учету при разработке, тестировании и эксплуатации БВС.

5.2. Основные технические средства и системы контроля и управления движением беспилотных воздушных судов

Существующие правила визуальных полетов (ПВП/VFR) и правила полетов по приборам (ППП/IFR) разработаны для пилотируемой авиации и пока что недостаточно адаптированы применительно к высокоавтоматизированным авиационным системам. Сегодня мировое

авиационное сообщество склоняется к новым правилам цифровых полетов (ПЦП/DFR), основанным на цифровых информационных сервисах. В такой ситуации поставщиком информационных услуг для БАС является цифровая платформа информационного обслуживания полетов (ЦП ИОП).

В результате получается, что предоставляемая информация, в зависимости от уровня обслуживания, зрелости технологий и регулирования, может носить справочный характер, рекомендательный или, наоборот, обязательный характер к исполнению цифровых указаний.

На разных уровнях зрелости системы обслуживания полетов человек может находиться внутри или вне контура управления. Соответствующим образом перераспределяется ответственность и полномочия в принятии решений между автоматизированной системой, пилотом, регулятором, производителем и разработчиком технических средств.

ЦП ИОП является комплексом взаимосвязанных цифровых информационных сервисов, который предоставляет информацию на основе аэронавигационных, геопространственных, метеорологических и других данных и использует инфраструктуру связи, навигации, наблюдения, управления радиочастотным спектром для измерения параметров движения БАС.

Часть функций ЦП ИОП связана с обеспечением безопасности, и информационное обслуживание регулируется соответствующей нормативной базой. Другая часть информации предоставляется по соглашению поставщика информации и ее потребителя для повышения эффективности операций БАС.

В зависимости от уровня рисков функции ЦП ИОП, средства обеспечения данными должны быть стандартизированы и сертифицированными, включая процедуры оценки безопасности и присвоения компонентам системы соответствующих уровней гарантии.

Взаимодействие ЦП ИОП с поставщиками и потребителями данных осуществляется на основе протоколов информационного взаимодействия (*API*), которые также должны быть предметом стандартизации. Система обеспечения безопасности в такой высокоавтоматизированной системе базируется на постоянном мониторинге и плановом обеспечении всех компонентов на нормативно требуемом уровне безопасности.

Международная организация гражданской авиации (ИКАО) в Циркуляре 278 представила руководящие принципы по разработке национальных планов внедрения систем связи, навигации, наблюдения и ОрВД (*CNS/ATM*) [33]. Этот документ служит основой для гармонизированного и скоординированного перехода к более современным авиационным системам во всем мире.

Концепция *CNS/ATM* является частью инициативы ИКАО по модернизации и интеграции глобальной авиатранспортной системы. *CNS* относится к элементам связи, навигации и наблюдения, в то время как *ATM* охватывает организацию воздушного движения. Цель со-

стоит в том, чтобы заменить устаревшие технологии и процедуры новыми цифровыми решениями для повышения безопасности, эффективности и пропускной способности ВП.

Ключевые элементы *CNS/ATM* включают:

- спутниковую связь и навигацию;
- усовершенствованное наблюдение, такое как АЗН-В (*ADS-B* – автоматическое зависимое наблюдение-вещание);
- улучшенные метеорологические системы;
- управление информацией во всей системе;
- совместное принятие решений участников;
- гибкое использование ВП;
- оптимизацию траектории полета.

Переход к *CNS/ATM* – это сложный процесс, требующий тщательного планирования и координации на национальном уровне. Каждое государство несет ответственность за модернизацию своей авиационной инфраструктуры в соответствии со стандартами и рекомендациями ИКАО.

Национальный план *CNS/ATM* служит дорожной картой для этого перехода. Он определяет конкретные потребности, приоритеты и действия страны, обеспечивая при этом согласование с региональными и глобальными стратегиями. Эффективный национальный план имеет решающее значение для успешной реализации и получения преимуществ от новых технологий и процедур.

При этом Циркуляр 278 ИКАО предоставляет подробные рекомендации по разработке национального плана *CNS/ATM*. Этот процесс включает несколько ключевых шагов:

- создание национального органа, отвечающего за разработку и реализацию плана *CNS/ATM*. Этот орган должен включать все заинтересованные стороны – авиационные власти, поставщики аэронавигационного обслуживания, авиакомпании, аэропорты и структуры безопасности. При этом необходимо обеспечить четкое и адекватное распределение ролей, обязанностей и ресурсов;

- анализ имеющейся системы и определение ее недостатков. Всесторонний анализ существующей инфраструктуры *CNS/ATM* и операций необходим для выявления узких мест и областей, требующих улучшения. Этот анализ должен охватывать технические, эксплуатационные, организационные, нормативные и финансовые аспекты. Следует также рассмотреть совместимость с системами в соседних странах, определить операционные требования и ожидаемые выгоды, а также обратить внимание на возможные варианты распространения нарушений кибербезопасности.

На основе анализа недостатков и с учетом прогнозируемого роста трафика и новых типов БВС должны быть определены будущие потребности. Они включают:

- требования к производительности системы, уровню обслуживания в области связи, навигации, наблюдения, управления, информационного обеспечения и т. д. Необходимо определить и ожидаемые выгоды от внедрения *CNS/ATM*, такие как повышение безопасности, экономию затрат, увеличение пропускной способности и экологические преимущества;

- разработку стратегии внедрения *CNS/ATM*, исходя из доступных ресурсов и возможностей. Последние включают выбор подходящих технологий и стандартов, которые будут использоваться в компонентах системы.

Стратегия должна определять приоритеты, этапы внедрения и реалистичные сроки. Переход к *CNS/ATM* обычно происходит поэтапно в течение ряда лет, поэтому план должен предусматривать управление параллельными операциями в переходный период;

- планирование человеческих ресурсов и обучение кадров. Внедрение новых систем и процедур требует квалифицированного персонала. Это касается как технического персонала (например, инженеров и техников), так и операционного (например, диспетчеров воздушного движения и пилотов);

- финансовое планирование, анализ затрат и выгод. Модернизация систем *CNS/ATM* требует значительных инвестиций. Поэтому должен быть проведен детальный анализ затрат, связанных с каждым элементом стратегии внедрения, включающей как первоначальные капитальные затраты, так и эксплуатационные расходы.

Затраты необходимо сопоставить с ожидаемыми выгодами, чтобы оценить окупаемость инвестиций. План должен определять механизмы финансирования, такие как сборы с пользователей воздушного пространства, государственные инвестиции или со стороны государственно-частных партнерств;

- сотрудничество и координация заинтересованных сторон. Успешное внедрение *CNS/ATM* требует тесного сотрудничества и координации между всеми заинтересованными сторонами на национальном и международном уровнях;

- управление рисками, включающее их оценку и стратегию смягчения для каждого элемента. Оно включает технические риски, такие как отказы системы, а также организационные риски, связанные, например, с сопротивлением изменениям. План управления должен включать меры на случай непредвиденных обстоятельств для обеспечения непрерывности обслуживания;

- мониторинг, оценка и корректировка. Внедрение *CNS/ATM* требует постоянного мониторинга и оценки для отслеживания процесса, выявления проблем и оценки достижения целей. Национальный план должен устанавливать ключевые показатели эффективности и отчетность. По результатам план следует периодически и систематически корректировать.

Национальный план внедрения систем *CNS/ATM* является важнейшим инструментом для государств при переходе к более современной и интегрированной авиатранспортной системе. Следуя руководящим принципам, изложенным в Циркуляре 278 ИКАО, страны могут разработать всеобъемлющие планы, которые учитывают их специфические потребности и обстоятельства, обеспечивая при этом согласование с глобальными и региональными целями.

Эффективное планирование и реализация систем *CNS/ATM* имеют решающее значение для удовлетворения растущего спроса на авиаперевозки безопасным, эффективным и экологически устойчивым образом. Это требует тесного сотрудничества и приверженности всех заинтересованных сторон, а также постоянных инвестиций в технологии, людей и процессы.

Учитывая масштабы и сложность перехода к *CNS/ATM*, национальное планирование является непрерывным процессом, требующим регулярного пересмотра и адаптации. Обмен опытом и извлеченными уроками между государствами также имеет важное значение для продвижения вперед.

Как уже говорилось, вопросы интеграции БАС в единое воздушное пространство рассмотрены в Концепции [22], разработанной в целях достижения такого состояния авиатранспортной системы Российской Федерации, авиационной инфраструктуры и подготовки авиационного персонала, при котором выполнение полетов всех воздушных судов будет обеспечено на приемлемом уровне безопасности как в традиционном, так и в киберпространственном понимании данного термина.

Под интеграцией БВС в единое воздушное пространство в Концепции понимается процесс совершенствования законодательства, разработки и внедрения технологий обслуживания воздушного движения (управление полетами), успешное завершение которого обеспечивает безопасное выполнение полетов пилотируемых и БВС в ВП России.

Базовыми принципами интеграции БАС в единое ВП являются:

- не снижение существующего уровня безопасности полетов, не увеличение имеющегося и не создание нового риска для жизни и здоровья, а также риска причинения вреда наземной инфраструктуре и имуществу граждан;
- выполнение правила в области подготовки, выполнения и обеспечения полетов БВС – чем выше риск, тем выше требования;
- наличие у беспилотной и пилотируемой авиации равного доступа к ВП Российской Федерации с учетом реализации требований в области безопасности полетов;
- соответствие беспилотных и пилотируемых воздушных судов установленным техническим требованиям в области безопасности полетов;

- соответствие внешних пилотов установленным требованиям в области подготовки авиационного персонала;
- обеспечение киберзащищенности авиационной транспортной системы и всех компонентов ее инфраструктуры;
- формирование и введение в действие нормативно-технической и нормативно-правовой базы в области беспилотной авиации, учитывающей стандарты и рекомендуемую практику ИКАО;
- приоритетное использование электронной компонентной базы, программно-аппаратных комплексов и ПО отечественной разработки и производства в целях защищенности авиационной транспортной системы.

Основными задачами при интеграции БВС в единое ВП РФ являются:

- оценка и прогнозирование рисков эксплуатации БВС на основе инструктивных материалов, изложенных в Документе 9859 «Руководство по управлению безопасностью полетов» ИКАО. Там прописаны требования минимизации негативных последствий, возникающих при совместных полетах беспилотных и пилотируемых воздушных судов, разработки мероприятий по снижению рисков до приемлемого уровня, установления численных показателей безопасности полетов в контролируемом и неконтролируемом едином ВП РФ с учетом современной международной практики [31];
- установление критериев категорирования БВС и БАС;
- дифференциация требований к авиационному персоналу и подготовке его специалистов, летной годности БВС, к разработчикам и изготовителям БВС, БАС и их компонентов в соответствии с установленными критериями и классификацией воздушного движения;
- подготовка и допуск внешних пилотов БВС и пилотов пилотируемых ВС к выполнению полетов в едином ВП по соответствующим программам подготовки;
- разработка, внедрение и развитие технологий, необходимых для интеграции БВС в единое ВП;
- организация информационного обеспечения полетов БВС, в том числе – по принципу «единого окна»;
- совершенствование правил полетов, технологий обслуживания воздушного движения, структуры и классификации ВП при выполнении совместных полетов БВС и пилотируемых средств в едином ВП РФ.

Рост числа БВС создает новые вызовы для обеспечения безопасности воздушного движения. В этом контексте разработка и внедрение современных технических средств контроля и управления движением БВС становятся приоритетной задачей как для зарубежных стран, так и для России.

В комплекс таких средств входят технологии мониторинга движения воздушного транспорта, которые становятся все более распространенными, охватывая все его виды и обеспечивая высокий уровень

ситуационной осведомленности экипажей транспорта. Это снижает риски столкновений, а также своевременно позволяет информировать службы спасения о чрезвычайных ситуациях.

Отмеченные технологии основаны на получении информации о собственном местоположении от глобальных навигационных спутниковых систем (ГНСС) или иных источников данных. Далее формируется сообщение, содержащее идентификатор транспорта, информацию о местоположении и иную информацию.

Сообщение может быть получено службами мониторинга или другими участниками воздушного движения по открытому или специальному каналам связи. За счет увеличения ситуационной осведомленности экипажей воздушных и морских судов повышается безопасность движения, снижается вероятность столкновения, что будет еще более эффективно при увеличении числа судов в будущем [201].

Отметим, что некоторые системы мониторинга используют собственные системы передачи информации, а, например, ЭРА-ГЛОНАСС передает данные по сетям мобильных операторов.

В настоящее время согласно генеральному плану ИКАО на 2013–2028 гг. и программе Министерства транспорта РФ все суда пассажирской и транспортной авиации должны оснащаться оборудованием АЗН-В, реализующего два стандарта 1090ES и *VDL mode 4* [213].

Оборудование 1090ES обеспечивает ситуационную осведомленность для служб наблюдения, используя технологии вторичного обзорного локатора. Эти функции, основанные на использовании бортового оборудования, не требуют какой-либо поддержки с Земли.

Нужно отметить, что указанное оборудование, использующееся сегодня российскими авиаперевозчиками и судоходными компаниями, производится за границей, поэтому нуждается в авионике отечественного производства, которая бы позволила использовать независимые технологии АЗН-В.

Учитывая направленность настоящей монографии, отметим актуальную проблему кибербезопасности технологии АЗН-В [143–144]. Для решения этой проблемы определяется истинность положения отправителя сообщения.

Она выполняется с помощью системы мультилатерации, фиксирующей местоположение источника сигнала АЗН-В путем измерения разности дальностей от источника до нескольких наземных пунктов приема сигналов. Если определенное таким образом местоположение не совпадает с положением беспилотника, которое передано в сообщении, значит, оно от фантома [410].

Приведем некоторые тактико-технические характеристики.

Станция АЗН-В предназначена для приема радиосигналов на частоте 1090 МГц от бортовых приемоответчиков и передатчиков воздушных судов, радиомаяков транспортных средств, наземных приемоответчиков. Внешний вид станции представлен на рис. 5.1.

Бортовой передатчик «Москит» стандарта 1090ES представлен на рис. 5.2. Он предназначен для передачи текущего положения, скорости, высоты, идентификатора БВС по линии передачи данных системы АЗН-В (1090 ES).

Характеристики передатчика подтверждены на практике на различных типах беспилотников. После подачи питания бортовой передатчик определяет своё местоположение встроенным приемником ГНСС по сигналам спутников ГЛОНАСС (или ГЛОНАСС и GPS) и осуществляет передачу сообщений.



Рис. 5.1. Станция АЗН-В

Бортовой передатчик «Москит» формирует и передает сообщения, содержащие следующую информацию:

- идентификатор (24-битный адрес);
- местоположение БВС, высоту, скорость, курс;
- опознавательный индекс и категорию БВС,
- статус аварийной обстановки, эксплуатационный статус.

Идентификатор представляет число, которое может быть закодировано без использования адресов, выделенных ИКАО для РФ. В качестве опознавательного индекса может выступать регистрационный номер, полученный при регистрации БВС.



Рис. 5.2. Бортовой передатчик «Москит», установленный на БВС

Указанный бортовой передатчик выпускается в автономном и встраиваемом вариантах. Автономный бортовой передатчик «Москит» оснащен собственными источниками навигационной информации и электропитания.

Во встраиваемом варианте он обладает теми же характеристиками, что и предыдущий, но поставляется в виде удобном для монтажа внутри летательного аппарата. Данное исполнение предназначено для разработчиков и производителей беспилотных систем для внедрения в собственную конструкцию «с завода». Обмен информацией с полетным контроллером осуществляется по открытому протоколу *MAVLink* версии 2. Вес устройства составляет 8 г (рис. 5.3).

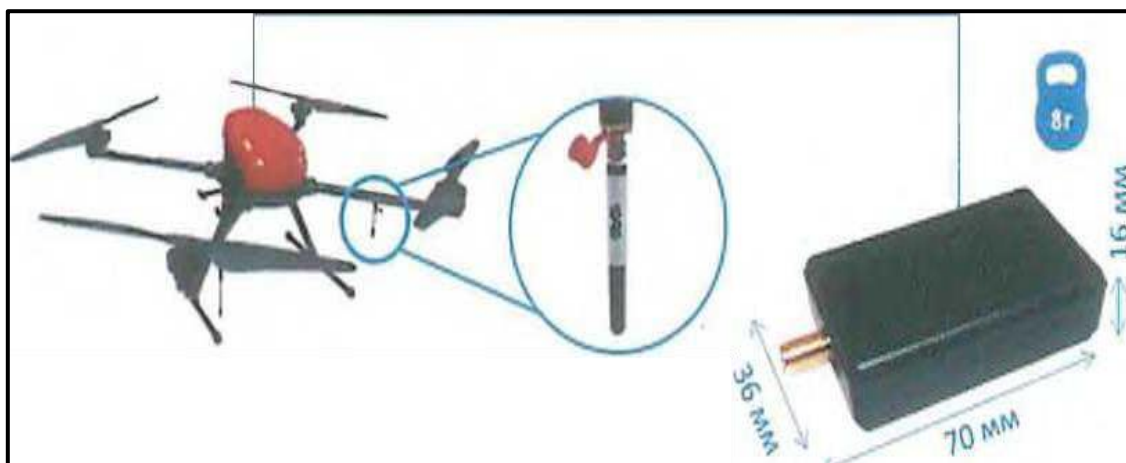


Рис. 5.3. Бортовой передатчик «Москит» на беспилотнике «Геоскан 401»

Для обеспечения наибольшей надежности идентификации беспилотника в условиях сложного городского рельефа, что особенно

важно для решения оперативно-служебных задач служб ОВД, на базе автономного варианта разработан бортовой передатчик «Москит+», который имеет дополнительный встроенный модуль для работы в сетях мобильного оператора.

После подачи питания и определения своего местоположения устройство регистрируется в сети мобильного оператора и осуществляет передачу сообщений одновременно по каналам *GPRS* и 1090 МГц. Устройство обеспечивает резервирование канала передачи данных, а также полное отсутствие «слепых» зон и углов затенения в зоне покрытия оператора сотовой связи (т. е. 100 % покрытие в черте города и прилегающих территориях). Однако повышение надежности связано с дополнительными расходами на услуги сотового оператора.

Технические характеристики бортового передатчика «Москит» приведены в табл. 5.1.

Таблица 5.1

Технические характеристики бортового передатчика «Москит»

Характеристика	Вариант	
	Автономный	Встраиваемый
Частота излучения, МГц	1 090	
Мощность излучения, Вт	0,5 или 2	
Дальность действия, км	до 7 или до 15	
Навигация (ГНСС)	ГЛОНАСС/GPS	От БВС
Время автономной работы, мин	Не менее 60	Ограничено временем работы аккумулятора БВС
Размеры, мм	70x51x22	30x40x6
Вес, г	56	5

Бортовой передатчик «Беркут» решает аналогичные задачи, но в отличие от передатчика «Москит» исключительно встраиваемый и обладающий большей выходной мощностью. Преимуществом устройства является наличие не только передатчика, но и приемника, работающего на той же частоте 1 090 МГц и позволяющего БВС по-

лучать информацию о воздушной обстановке вокруг себя. Вес устройства – 250 г. Внешний вид передатчика представлен на рис. 5.4.

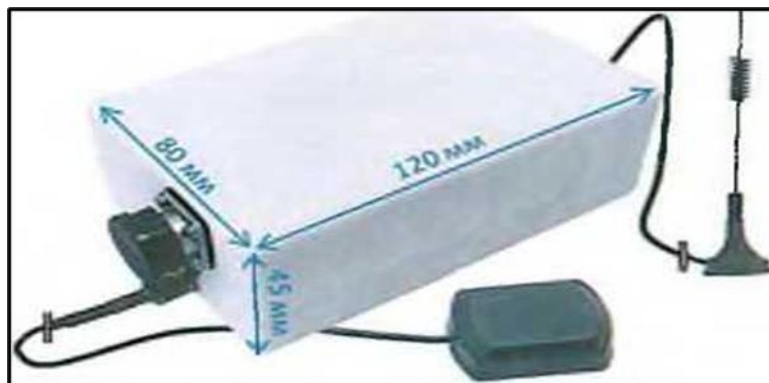


Рис. 5.4. Бортовой передатчик «Беркут»

Данные ГНСС предоставляются встроенным приёмником. По умолчанию он использует сигналы систем ГЛОНАСС и *GPS*, при настройке бортового передатчика предусмотрена возможность выбора только системы ГЛОНАСС. Антенна ГНСС должна размещаться на верхней части БВС для обеспечения беспрепятственного прохождения радиосигнала поодаль от излучающих антенн и затеняющих конструкций. Антенна 1 090 МГц выполнена в виде штыря и размещается вертикально в нижней части БВС. Бортовой передатчик «Беркут» способен передавать сообщения на расстояние до 50 км.

Система мониторинга использования ВП (система МИВП) предназначена для повышения безопасности ВП над населенными пунктами посредством непрерывного наблюдения (с возможностью фиксации, хранения и передачи информации) за нарушениями/отклонениями от действующих требований по использованию ВП и планов полётов.

Основными функциями системы МИВП являются:

- осуществление непрерывного автоматизированного мониторинга ВП над заданной территорией;
- выявление случаев нарушения воздушными судами действующих требований по безопасному использованию ВП и официальных планов полетов;
- обработка собранных данных и представление результатов оператору.

В состав системы МИВП входит:

- программно-аппаратный комплекс мониторинга ЦИВР. 461262.011;
- многопозиционная система наблюдения (МПСН) ЦИВР. 462319.008, предназначенная для обнаружения, сопровождения и идентификации воздушных объектов, оснащенных транспондерами вторичной радиолокации и/или аппаратурой АЗН-В в режиме 1090 ES.

МПСН принимает от воздушных объектов ответы на собственные запросы и запросы соседних радиолокаторов, а также сообщения АЗН-В;

- радиолокационный комплекс обнаружения малозаметных целей ЦИВР.461311.031-03, предназначенный для решения задач круглосуточного автоматического обнаружения, измерения координат, сопровождения, оценки параметров малозаметных целей, в том числе – малоскоростных и малоразмерных, и выдачи сообщения по ним потребителям.

АМПСН «Тетра» предназначена для обнаружения, наблюдения и идентификации воздушных судов во время их полёта в районе аэродромов, взлёте и посадке, рулении и стоянке, а также транспортных средств и наземных объектов, оснащённых ответчиками и находящихся в аэродромной зоне.

Преимущества АМПСН:

- возможность построения с использованием принципов как единого, так и распределенного времени;
- обнаружение воздушных судов и транспортных средств на поверхности аэродрома в границах контролируемой зоны;
- обнаружение воздушных судов в границах аэродромной зоны на высотах до 100 м и в зоне воздушных подходов на удалении до 10 км от порогов взлетно-посадочной полосы;
- точность определения положения объектов наблюдения до нескольких метров с интервалом обновления данных 1 раз в секунду;
- реализацию функций мониторинга захода воздушного судна на посадку, выдерживания высоты при посадке;
- высокую отказоустойчивость в условиях работы сторонних систем, в том числе – ГНСС;
- автоматический контроль технического состояния элементов системы;
- регистрацию и хранение радиолокационной информации в течении 30 суток;
- обеспечение безопасности аэродромного движения в условиях роста пропускной способности;
- низкие затраты на организацию расстановки наземных станций и последующую эксплуатацию.

В состав АМПСН «Тетра» входят:

- приемные станции ЦИВР.464339.018-01 (до 36 комплектов);
- приемные станции ЦИВР.464339.018-02 с прикладным ПО (до 50 комплектов);
- приемные станции ЦИВР.464339.018-03 с прикладным ПО (до 50 комплектов);
- передающие станции ЦИВР.464233.009-01 с прикладным ПО (от 2 до 10 комплектов);
- наземные приемоответчики ЦИВР.462612.002-01 (от 1 до 4 комплектов);

- программно-технический комплекс обработки сигналов и информации ЦИВР.466535.002-02 с ОС «*Astra Linux Special Edition*» и прикладным ПО;

- выносной терминал управления ЦИВР.468323.003-01 с ОС «*Astra Linux Special Edition*» и прикладным ПО;

- распределительные щитки ЦИВР.656516.001-01 (от 4 до 150 комплектов).

Общее количество приемных и передающих станций составляет от 6 до 146 комплектов, при этом типы и количество станций определяются проектом установки АМПСН «Тетра».

МПСН «Тетра-И» предназначена для:

- обнаружения, сопровождения и идентификации воздушных судов, оборудованных приёмоответчиками в режиме (АЗН-В) и широкозонной многопозиционной системы наблюдения (МПСН-Ш);

- передачи запросов приемоответчикам воздушных судов;

- передачи информации в систему автоматизированного управления воздушным движением.

5.3. Развитие технологий современной связи и беспилотный транспорт

За последние 40 лет сменилось четыре поколения мобильных технологий связи, каждая из которых весьма серьезно повлияла на весь телекоммуникационный рынок. В результате этих изменений на смену друг другу появлялись новые услуги, виды оборудования и бизнес-модели. Развитие мобильной связи к настоящему времени обернулось настоящей технологической революцией, которая позволила передавать данные с крайне низкой задержкой сигнала (до 2 мс в последних версиях стандартов *LTE*), огромной скоростью (до 3–6 Гбит/с), а также поддерживать продвинутые сервисы беспроводных коммуникаций.

Пятое поколение связи обещает дальнейший рост ее параметров: задержку сигнала до 1 мс, эффективность использования радиочастотного диапазона на 30–50 % выше, чем в самых современных версиях стандарта четвертого поколения, использование еще более широких радиочастотных каналов и возможность оказания новых услуг, требующих поддержки огромного количества мобильных устройств на ограниченной территории.

По оценкам, к концу 2025 г. технологией *4G (LTE)* в России будут пользоваться 80 % мобильных абонентов, тогда как на *2G (GSM)* и *3G (UMTS)* в совокупности будет приходиться не более 11 %, соответственно. Сегодня во всем мире укрепляется тенденция на полный вывод из эксплуатации сетей связи второго и третьего поколения. С одной стороны, операторы не хотят нести расходы по поддержке устаревших технологий, с другой – крайне заинтересованы в перспек-

тивном перераспределении освобождающегося радиочастотного спектра, оптимизации получаемых при этом ресурсов.

По прогнозам, несмотря на предстоящий запуск и развитие сетей 5G (*IMT-2020*), большую часть ближайшего десятилетия «рабочей лошадкой» в России будут сети 4G. Исключением будут только отраслевые сервисы в сегменте *B2B*, где пятое поколение гораздо быстрее станет более важным звеном.

Создание отечественного телекоммуникационного оборудования является одним из ключевых направлений по развитию специализированного нацпроекта «Экономика данных и цифровая трансформация государства».

Цели нацпроекта по созданию отечественного телекоммуникационного оборудования до 2030 г. следующие:

- разработать и запустить производство оборудования базовых станций стандартов *GSM/LTE/5G*;
- доработать ПО для ядра мобильной сети стандартов *LTE/5G* для сетей общего пользования;
- запустить тестирование оборудования на сетях операторов связи в реальных условиях;
- создать задел для обеспечения технологического суверенитета России в критичных высокотехнологичных отраслях.

По прогнозам аналитиков, к 2030 г. производство радиомодулей и блоков для базовых станций в России вырастет почти в 3 раза с общей стоимостью до 1,4 трлн рублей. Это связано как с активным развёртыванием сетей 5G, так и с импортозамещением телекоммуникационного оборудования [366]. Одновременно наблюдается усиление интереса промышленных компаний к интеграции систем сотовой связи и систем управления БВС.

Однако, несмотря на очевидные успехи, этого пока недостаточно для повсеместного замещения решений иностранных производителей на сетях связи по всей территории РФ. Многие системы и компоненты сотовой связи, в том числе обеспечивающие реализацию технологии идентификации БВС, остаются зарубежными. Однако, при сохранении существующей тенденции, задача импортозамещения ключевых компонентов сотовой связи в обозримом будущем вполне выполнима.

Кратко проанализируем основные системы спутниковой связи, играющие все более значительную роль в задачах телекоммуникации, а также в области беспилотного транспорта. Особенно это актуально для обеспечения жизнедеятельности в труднодоступных российских регионах.

По состоянию на 2025 г. в нашей стране развивается несколько отечественных спутниковых систем связи (табл. 5.2):

- низкоорбитальная спутниковая система связи «Гонец»;
- спутниковая система связи «Экспресс», использующая спутники на высоких эллиптических орбитах;

– спутниковая система связи «Ямал», использующая спутники на геостационарных орбитах;

– спутниковая система связи «Сфера» (находится в разработке).

Рассмотрим для примера отечественную систему спутниковой связи «Гонец» для гражданского использования. Она доставляет текстовые сообщения из любой точки России, обеспечивает связь на территориях Беларуси, Казахстана, Грузии, Азербайджана, Монголии и частично Украины. Максимальная скорость передачи данных зависит от того, какой канал используется, сколько спутников в зоне видимости терминала, а также от исполнения самого терминала.

Система «Гонец» на сегодняшний день обеспечивает передачу коротких сообщений и телеметрии, позиционирование и мониторинг подвижных объектов. Спутниковая группировка состоит из 12 космических аппаратов на низких околоземных орбитах. Наземный сегмент включает центр управления, станции сопряжения и пользовательские терминалы. Используется в государственном секторе, МЧС, нефтегазовой отрасли, экологическом мониторинге, в рыбопромысловом флоте, для отслеживания местоположения и маршрута специальной техники и грузового транспорта, а также для обеспечения персональной связи в тех регионах, где не развёрнуты сети GSM. Покрытие территории спутниковой группировкой системы «Гонец» представлено на рис. 5.5.

Таблица 5.2

Основные характеристики систем спутниковой связи

Название, орбита	Количество спутников	Скорость передачи	Зона покрытия
«Гонец», низкоорбитальная	3	20 Кбит/с	Вся территория РФ
«Экспресс», высокий эллипс	13	До 80 Мбит/с	Вся территория РФ
«Ямал», геостационарная	4	От 20 до 100 Мбит/с (зависит от спутника)	Мировой масштаб, кроме части северной Африки, Австралии и США
«Сфера», низкоорбитальная	До 640	1 млрд транзакций в сутки	Мировой масштаб

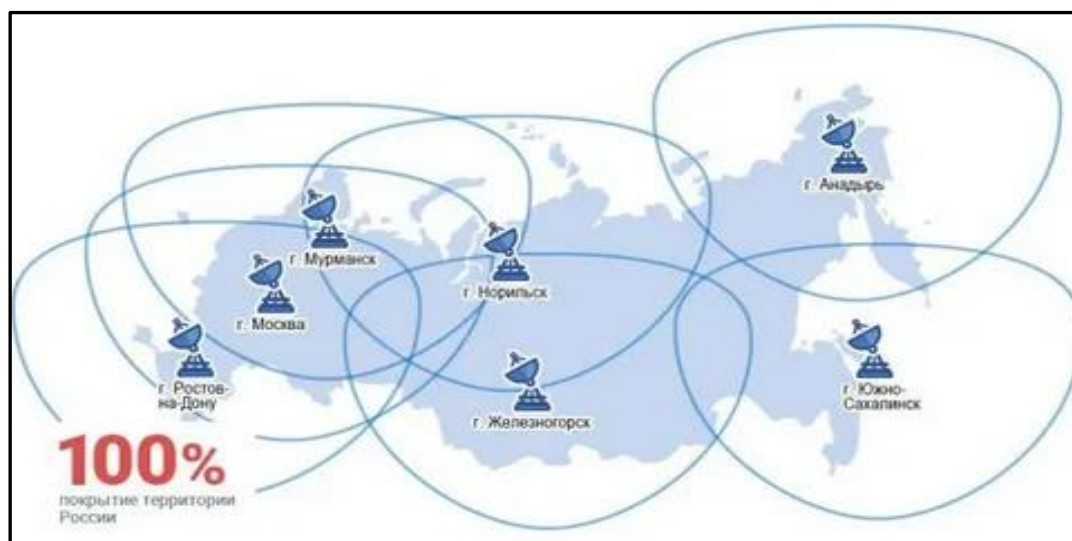


Рис. 5.5. Карта покрытия спутниковой группировкой «Гонец»

Спутниковая связь системы «Гонец» может использоваться для передачи циркулярных сообщений группам пользователей, когда необходимо довести информацию до групп абонентов, рассредоточенных на местности – на суше, на воде и в особенности в удаленных и труднодоступных районах, которые имеются в значительном количестве на территории России. Циркулярное сообщение может формироваться как с абонентского терминала «Гонец», так и через Web-приложения «Гонец», подключенные к сети Интернет.

Сообщение передается на региональную станцию «Гонец», отсюда – на один из спутников группировки системы «Гонец», который передает его адресатам группы. Диаметр зоны обслуживания одного космического аппарата «Гонец» достигает до 5 000 км, что позволяет передать циркулярное сообщение абонентам, находящимся на значительном удалении друг от друга.

Уже можно назвать примеры практического применения системы связи «Гонец» для управления БВС непосредственно со спутника. Так, компания «Геоскан» провела наземные тесты на основе проектно-образовательного портала «Архипелаг-2024» в Сахалинской области [128]. В ходе этого эксперимента успешно переданы данные о местоположении, телеметрические данные БВС в центр обработки спутниковой системы «Гонец», а также отправлена команда через спутник о принудительном возвращении БВС на место запуска.

В другом эксперименте в июле 2024 г. выполнялись наземные тесты и полёты на аэродроме «Пушистый». В их ходе производилась установка связи, передача данных телеметрии с борта БВС «Геоскан 201», оснащённого экспериментальным бортовым модемом и специальной облегчённой версией антенны (рис. 5.6), на космический аппарат «Гонец-М» и отправка команд с наземной станции управления «Геоскан» на БВС через спутник [303].



Рис. 5.6. БВС «Геоскан 201»

Спутниковый модем системы «Гонец» представляет собой радиомодем, обеспечивающий передачу данных по спутниковому каналу связи. Технические характеристики указаны в табл. 5.3.

Помимо компактных модемов в систему «Гонец» входят спутниковые терминалы различного исполнения, обеспечивающие более высокую скорость передачи данных, но имеющие большие массогабаритные характеристики.

Таблица 5.3

Технические характеристики модемов системы «Гонец»

Рабочий диапазон	312–315 МГц – передача, 387–390 МГц – приём
Мощность передатчика	5 Вт – при питании 5 В, 3 Вт – при питании 3,6 В
Чувствительность приёмника	117 дБ/мВт
Скорость передачи данных	ПК – 2.4, 4.8, 9.6 ОК – 9.6, 19.2, 38.4, 76.8 кБит/с
Антенна	Внешняя
Навигационный приёмник	Нет
Интерфейс	UART
Напряжение питания	3,3–5 В
Диапазон рабочих температур	-40...+60 °С
Габариты	56x22x4 мм

Мобильный комплект позволяет осуществлять персональные коммуникации в любой точке. Терминал имеет локальную сеть *Wi-Fi* для подключения мобильных устройств.

Абонентский автономный терминал в едином конструктиве совмещает блок приёма-передачи с антенной. Это позволяет использовать терминал в ограниченном пространстве и не требует кабеля.

Внешний вид вариантов космических аппаратов типа «Гонец» представлен на рис. 5.7.

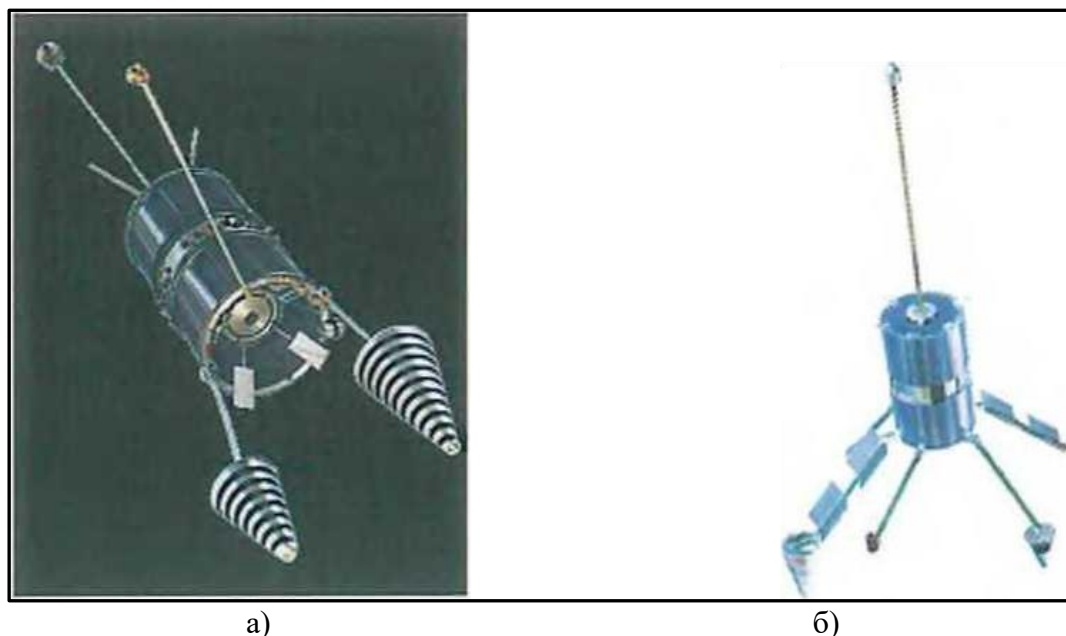


Рис. 5.7. Космические аппараты: а) «Гонец-Д1»; б) «Гонец-М»

Несколько слов о перспективной спутниковой системе «Сфера», которая разрабатывается на отечественных технологиях и компонентах для обеспечения высокоскоростной Интернет и мобильной связи, а также оперативной передачи данных. Она направлена на охват всех населенных пунктов России, включая самые удаленные. Планируется развернуть группировку из сотен спутников на низких околоземных орбитах, наземный сегмент которой будет включать центры управления, шлюзы и пользовательские терминалы.

Кроме того, учитывая исключительную значимость Единой системы государственного радиолокационного опознавания (ЕС ГРЛО) РФ для выявления и своевременного отсеечения «чужих» беспилотников, прокомментируем основные моменты ее применения.

Информация системы опознавания используется средствами Федеральной службы разведки и контроля воздушного пространства (ФСР КВП), в АСУ командных пунктов всех звеньев управления видами Вооруженных сил РФ, огневых комплексах. Оснащение беспилотных объектов средствами опознавания позволяет обеспечить эффективное боевое и оперативно-тактическое применение наземных и воздушных группировок, взаимодействие отдельных подразделений, безопасность транспортировки.

Для защиты от компрометации действующего в ЕС ГРЛО ключа в ответчиках можно использовать «выделенные» ключи. Однако это

не исключает проблемы оснащения аппаратурой запросчиков ЕС ГРЛО, ежедневным вводом этих ключей в аппаратуру запросчиков и ответчиков и наличие грифа секретности на всей аппаратуре.

Соответствующие изделия функционируют только в имитостойком режиме, поэтому получение запросчиком дополнительной информации от данных ответчиков невозможно.

Принимая во внимание существующую вероятность захвата и потери БВС, нецелесообразно использование ответчиков ЕС ГРЛО «Пароль» («Страж») для опознавания (идентификации) объектов без специальной модернизации и надежной правовой поддержки. В числе таких объектов: принадлежащие Вооруженным силам РФ либо особо важным для безопасности государства структурам; гражданские или относящиеся к различным коммерческим организациям.

В то же время, нужно отметить, что высокая коммерциализация рынка дронов, государственная поддержка инновационных проектов и высокая степень цифровизации способствуют появлению не всегда оправданных решений, которые позволяют тем или иным способом встраивать БВС в существующую инфраструктуру управления воздушным движением. И к этому на данном этапе развития беспилотного транспорта и усиления его кибербезопасности нужно отнестись с особым вниманием и настороженностью.

5.4. Системы искусственного интеллекта как фактор управления безопасностью беспилотных воздушных судов

На тему внедрения ИИ в авиацию имеются многие положительные суждения экспертов ИКАО, которые видят исключительное преимущество в виде человеко-машинной синергии для улучшения общей производительности, эффективности и безопасности воздушного транспорта. Да и многие владельцы крупного бизнеса отмечают существенные риски в случае игнорирования технологий ИИ.

Совершенствование инструментов ИИ для ОрВД позволяет устранить рутину, сократить время для принятия жизненно важных решений, повысить эффективность и безопасность, что, в свою очередь, повышает качество услуг аэронавигационного обслуживания. Наиболее перспективными направлениями внедрения ИИ в авиатранспортную систему являются система ОрВД, аэропортовые службы, авионика, но наиболее интересным является создание цифровой защищенной платформы управления воздушным движением.

Внедрение технологий ИИ в авиатранспортную систему поможет в решении задач [308]:

- снижения пропускной способности системы ОрВД;

- преодоления высокого уровня сложности авиатранспортной системы;
- реагирования на изменения погодных условий полетов;
- обеспечения цифровой трансформации отрасли, и ряда других системных задач.

Рассмотрим более детально пути применения ИИ в решении указанных задач.

Такие меры, как динамическая секторизация ВП, развитие новых технологий связи, мониторинга и контроля полетов относятся к решению задач, по которым ИИ находит свое активное применение и является весьма перспективным. Их эффективное выполнение должно обеспечить возможность увеличить пропускную способность ОрВД путем более качественной обработки и анализа информации (аэронавигационные, метеорологические данные, информация систем наблюдения о движении, скорости и местоположении воздушных судов в полете и прочее).

Более того, ИИ сможет предложить и ряд инновационных решений. Они основаны на неявных связях в системе воздушного движения. Учет данных обстоятельств позволит улучшить масштабируемость, эффективность и отказоустойчивость системы в связи с увеличением количества беспилотных аппаратов в небе.

На самом деле, постоянно увеличивающаяся интенсивность воздушного движения, появляющиеся новые пользователи воздушного пространства (сверхзвуковые коммерческие самолёты, дистанционно-пилотируемые летательные аппараты, БАС) в сочетании с развивающимися технологиями связи, схемами полетов и увеличивающейся скорости приводят к беспрецедентной сложности воздушного движения, создания проблем безопасного управления в ВП. Это, в свою очередь, требует дальнейшей автоматизации с применением ИИ.

Быстро развивающаяся отрасль БАС создает серьезную проблему для системы ОрВД, поскольку большое количество разнообразных беспилотных аппаратов уже работают на разных эшелонах, растет интерес к эксплуатации воздушных судов в стратосфере. Данные обстоятельства еще больше усложняют обслуживание воздушного движения и требуют масштабировать систему ОрВД на новые эшелоны.

Отметим и еще одну важную сторону. ИИ может быть применен в автономном полете воздушного судна для распознавания воздушной обстановки и определения потенциальных конфликтных ситуаций.

Кроме того, как подчеркивается в Европейском генеральном плане ОрВД и исследовании архитектуры воздушного пространства *SES (Single European Sky – Единое европейское небо)*, ожидается фундаментальный сдвиг в виде повышения уровня автоматизации как при стратегическом, предтактическом и тактическом планировании в авиационных полетах, так и для управления беспилотным движением (*UTM, Unmanned Traffic Management*).

Ожидается, что это будет все больше приводить к переходу от операций в воздушном пространстве к операциям на основе траекторий. В этой связи ИИ станет незаменимым помощником для всех участников системы ОрВД, начиная с аэронавигационных провайдеров, заканчивая эксплуатантами.

К тому же ИИ будет стимулировать развитие новых услуг ОрВД и повысит безопасность за счет предоставления новых средств обнаружения и разрешения опасных инцидентов, консультирования по вопросам графика полетов. Речь идет, например, о голосовых/текстовых ботах с технологией распознавания речи и/или текста, сопряженных со средствами наблюдения и связи, планами полетов, разрешениями, метеоинформацией и другими летными характеристиками, а также об отмеченных выше проблемах киберустойчивости.

Цифровая трансформация является основой развития российской системы ОрВД. От ее широкомасштабного внедрения ожидается решение вопросов безопасно и эффективно справляться с ростом и разнообразием воздушного движения.

Центральное место в отмечаемой цифровой трансформации занимает повышение уровня автоматизации, кибербезопасного обмена данными и подключения к интернету. Кроме того, ИИ позволит вывести на новый уровень качества инфраструктуру и услуги по обслуживанию движения во всех зонах ВП, начиная с операций на очень низкой и заканчивая операциями на предельно большой высоте.

Вместе с тем технологии ИИ позволят системе стать более модульной и гибкой, а также повысить устойчивость к сбоям, увеличению интенсивности воздушного движения. Указанный подход ориентирован на расширение круга пользователей ВП, включая различные типы беспилотных аппаратов, которые продолжают активно развиваться и имеют тенденцию появления абсолютно новых конструкций, особенностей полетной практики и необходимости развития соответствующих технологий управления и обеспечения безопасности.

ИИ представляет собой прорывную технологию, которая может радикально повлиять на производственно-сбытовую цепочку авиатранспортной системы или трансформировать ее. По сути своей рассматриваемый прорывный импульс потенциально воздействует на все заинтересованные стороны, включая производителей оригинального оборудования и их бизнес-модели.

Влияние преобразующего ИИ будет ощущаться во всей отрасли производства, применения беспилотников и за ее пределами. В том числе, развитие этих направлений затрагивает и отмеченные ведомственные интересы – при решении оперативных и тактических задач различных подразделений ОВД, осуществляющих борьбу с организованной преступностью, с незаконным выращиванием и распространением наркотикосодержащих растений, преступлениями в киберпро-

странстве, электронным мошенничеством и другими социально опасными деяниями.

Отмечаемая в монографии область БАС пока не располагает обширными ретроспективными данными. Соответственно, разработки ИИ в основном сосредоточены на «обнаружении и уклонении», точной навигации и распознавании изображений.

В частности, уже функционирует ряд прикладных программ. Например, Маастрихтский центр управления ВП продемонстрировал решение задач прогнозирования и планирования при управлении потоками воздушного движения и пропускной способностью при входе в мониторируемое ВП на основе четырехмерной модели ИИ, включая координаты воздушного судна, эшелон и время.

Алгоритм ИИ также поддерживает функцию «что, если», позволяя имитировать влияние правил или ограничений по использованию воздушного пространства на прогнозируемую траекторию. С использованием этого приложения нагрузка на операторов снизилась, а эксплуатационные показатели улучшились.

В заключение главы перечислим *критические технологии, обеспечивающие создание цифровой платформы БАС*.

В соответствии с положениями Стратегии развития беспилотной авиации Российской Федерации на период до 2030 года и на перспективу до 2035 года к технологиям интеграции БВС судов в единое ВП РФ и к технологиям, обеспечивающим создание цифровой платформы БАС, относятся критические технологические решения в области:

- удаленной идентификации БВС;
- программно-аппаратных средств, обеспечивающих организацию воздушного движения и использование ВП;
- организации воздушного движения в рамках городской аэромобильности;
- мониторинга инфраструктуры передачи информации; системы наблюдения и компактных бортовых ответчиков с учетом положений, закрепленных ИКАО;
- цифровых радиолиний связи, контроля и управления в полосах частот, утвержденных Международным союзом электросвязи;
- средств навигации на основе ГНСС, системы дифференциальной коррекции и мониторинга;
- единой базы данных авиационной метеорологической информации, единой базы данных аэронавигационной информации;
- систем оперативного предоставления аэронавигационной, полетной и метеорологической информации внешним пилотам БВС и другим участникам воздушного движения;

- системы предупреждения столкновений БВС с пилотируемыми воздушными судами, обеспечивающие безопасное выполнение совместных полетов;
- создания пилотных зон тестирования, верификации и валидации технологий, включая комплексы имитационного моделирования.

5.5. Выводы по главе 5

Анализ нормативной базы, существующих и разрабатываемых технологий и технических средств контроля и управления движением БВС показал следующее.

1. Традиционные правила полетов недостаточны для высокоавтоматизированных БАС. Международные авиационные стандарты переводятся к новым цифровым правилам полетов (ПЦП/DFR), опирающимся на цифровые информационные сервисы. Ключевую роль при этом играет цифровая платформа информационного обслуживания полетов (ЦП ИОП), обеспечивающая безопасное функционирование беспилотных систем.

2. В России разработан проект концепции интеграции БВС в единое воздушное пространство. Российские специалисты ведут активные исследования и разработки, направленные на улучшение технологий мониторинга и идентификации БВС. Например, созданы национальные системы автоматической идентификации (АЗН-В), которые начинают активно внедряться.

3. Несмотря на достигнутые успехи, остается ряд нерешенных задач, таких как полная реализация стандартных подходов и расширение охвата территорий технологиями мониторинга и идентификации беспилотников. Дальнейшее развитие систем и технологий позволит России занять лидирующие позиции в области управления беспилотным воздушным движением и обеспечить безопасное и эффективное использование воздушного пространства.

4. Системы ИИ имеют высокий потенциал применения в авиатранспортной отрасли. Особенно эффективным видится его применение для БАС, где автономность технических средств растет и необходимо иметь возможность принятия решений без участия человека.

5. Анализ зарубежных и российских платформ отмечает имеющиеся различия в структуре, функционале и подходе к обеспечению кибербезопасности беспилотного транспорта. Российские платформы тяготеют к адаптивности к отечественным стандартам и нормативным актам, однако часто уступают иностранным аналогам по уровню развитости инфраструктуры и интеграции с внешними сервисами. В то же время необходим компромисс между преимуществами обеих платформ, сохраняя соответствие высоким стандартам кибербезопасности, надежности и эффективности.

6. Перспективные системы контроля и управления движением БВС характеризуются повышением автономности, использованием интеллектуальных технологий и распределённой архитектурой, а также возможностью дистанционного контроля и корректировки полёта. Такие системы позволят управлять полётом БВС без постоянного участия оператора, а также взаимодействовать с другими участниками воздушного движения, что расширяет сферы их применения, включая решение оперативных и тактических задач различных подразделений ОВД, осуществляющих борьбу с организованной преступностью, с незаконным выращиванием и распространением наркотикосодержащих растений, киберпреступностью, электронным мошенничеством.

7. Основными критическими технологиями, обеспечивающими интеграцию БВС в воздушное пространство РФ, являются сетевая модель управления воздушным движением, его сервис-ориентированная инфраструктура, унификация риск ориентированной модели обмена информацией между участниками движения, опережающие технологии обеспечения кибербезопасности, связи, наблюдения и навигации, применение цифровых двойников.

Заключение

Структура изложения монографии определила необходимость формулирования выводов после каждой главы с отражением ключевых аспектов рассмотренного материала. Чтобы не повторять их в заключении, отразим в нем только основные результаты выполненных исследований с указанием перспектив развития системных направлений, подходов, мнений, рассмотренных в работе.

Монография представлена в двух частях.

Первая часть сосредоточила основные сведения об использовании технологий ИИ, которые применяются правоохранительными органами при организации мероприятий по противодействию и профилактике киберпреступности и, в частности, кибермошенничеству, как наиболее вызывающему социальную напряженность в последнее время. Структурно первая часть содержит две главы.

В *первой главе* систематизированы базовые положения, определяющие понятийную сферу технологий ИИ: срез исторического появления, формирования и развития, влияние на становление кибербезопасности. Рассмотрены факторы развития киберпреступности, в том числе – кибермошенничества. Обсуждены проблемы и новые возможности использования ИИ как в криминальной среде, так и в деятельности ОВД по противодействию этому новому антисоциальному явлению.

Материал *второй главы* конкретизирует применимость ИИ для информационно-аналитического обеспечения решения оперативно-служебных задач при противодействии киберпреступности. Изложены современные и перспективные научно-прикладные направления применения технологий ИИ в практической деятельности ОВД по борьбе с кибермошенничеством и другими проявлениями киберпреступности.

Вторая часть работы освещает задачи организации безопасного управления беспилотным транспортом, находящего все большее применение в борьбе с киберпреступностью, но, в то же время, и активно становящегося предметом реализации киберугроз.

В частности, *третья глава* содержит систематизированные сведения об организации интеллектуального противодействия киберпреступности на основе использования БАС. Направления этой работы охватывают создание основ классификации, разработки и апробации моделей безопасного управления беспилотным транспортом.

При разработке моделей рассмотрены киберугрозы системам ИИ при управлении беспилотным транспортом; киберустойчивость и управляемость флотом беспилотных транспортных средств; комплексная математическая модель системы интеллектуальной защиты информации БАС; основы построения Цифровой платформы безопасного управления БАС.

На основе приведенных концептуальных положений сформирован материал завершающей *четвертой главы*. Она является определенной иллюстрацией авторских наработок в решениях прикладных задач управления беспилотным транспортом, организации интеллектуального противодействия киберпреступности, в том числе и новым киберугрозам непосредственно БАС.

Читателю представлены основные сведения по таким приложениям, как кибербезопасность БАС дистанционного мониторинга территорий; новые подходы к экспертно-криминалистической деятельности, в том числе обеспечения доказательственной базы киберпреступлений; интеграция с геоинформационными системами для совершенствования информационно-аналитического обеспечения раскрытия, расследования, профилактики киберпреступлений; автоматическое распознавание объектов и маршрутизация БАС, принятие решений по обеспечению их безопасности.

В *пятой главе* монографии рассмотрены документы ИКАО по разработке и внедрению в систему беспилотного воздушного движения перспективных технологий связи, навигации, наблюдения/организации воздушного движения, приведен обзор соответствующих руководств и документов. Рассмотрен план мероприятий Концепции интеграции БВС в единое ВП РФ. Проведен анализ существующих и разрабатываемых технологий и технических средств контроля и управления движением БВС. Рассмотрены перспективные направления и мировые тенденции внедрения ИИ в авиатранспортную систему, к которым относятся: система организации воздушного движения; аэропортовые службы; авионика, цифровая защищенная платформа управления. Приведены конкретные примеры применения ИИ в авиатранспортных системах.

Показано, что перспективными направлениями исследований в области беспилотного транспорта являются:

- обоснование и выбор интеграционной шины отечественной разработки;
- разработка на базе технологий ИИ алгоритмов, программ, структур данных и протоколов взаимодействия, а также выбор технических решений по получению данных о состоянии БВС в центры контроля и управления движением БВС;
- опережающее развитие модели угроз и нарушителей, требований по обеспечению кибербезопасности применения беспилотников;
- разработка экспериментального образца, типового защищенного перспективного авиационного комплекса для построения центров АСКУД БВС;
- разработка технического задания на ОКР по созданию опытного образца цифровой платформы БАС.

Список использованных источников

Нормативно-правовая база

1. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) Доступ из справ.-правовой системы «Гарант».

2. А/79/460. Конвенция Организации Объединенных Наций против киберпреступности. Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. 24-22383. 56 с. // URL: mail.ifap.ru/pr/2024/n241230a.pdf (дата обращения: 22.03.2025).

3. Окинавская хартия глобального информационного общества: принята на о. Окинава 22 июля 2020 г. Доступ из справ.-правовой системы «КонсультантПлюс».

4. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26.07.2017 № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

5. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»: федер. закон от 02.07.2021 № 331-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

6. О внесении изменений в Уголовный кодекс Российской Федерации: федер. закон от 23.04.2018 № 111-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

7. О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»: федер. закон от 24.04.2020 № 123-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

8. О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 01.04.2025 № 41-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

9. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».

10. Об основах системы профилактики правонарушений в Российской Федерации: федер. закон от 23.06.2016 № 182-ФЗ: ред. от 08.08.2024 № 232-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

11. Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации: федер. закон от 31.07.2020 № 258-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».

12. Национальная стратегия развития искусственного интеллекта на период до 2030 года: Указ Президента Рос. Федерации от 15.02.2024 № 124. Доступ из справ.-правовой системы «КонсультантПлюс».

13. О развитии искусственного интеллекта в Российской Федерации: Указ Президента Рос. Федерации от 10.10.2019 № 490. Доступ из справ.-правовой системы «КонсультантПлюс».

14. О стратегии национальной безопасности Российской Федерации: Указ Президента Рос. Федерации от 02.07.2021 № 400. Доступ из справ.-правовой системы «КонсультантПлюс».

15. О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Рос. Федерации от 09.05.2017 № 203. Доступ из справ.-правовой системы «КонсультантПлюс».

16. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Рос. Федерации от 05.12.2016 № 646. Доступ из справ.-правовой системы «КонсультантПлюс».

17. Об утверждении Концепции внешней политики Российской Федерации: Указ Президента Рос. Федерации от 30.11.2016 № 640. Доступ из справ.-правовой системы «КонсультантПлюс».

18. Аналитический отчет за 2024 г. по реализации Государственной программы Российской Федерации «Обеспечение общественного порядка и противодействие преступности»: Постановление Правительства Рос. Федерации от 15.04.2014 № 345. Доступ из справ.-правовой системы «КонсультантПлюс».

19. Об утверждении требований к оснащению пилотируемых воздушных судов и беспилотных авиационных систем оборудованием связи, навигации, наблюдения, автоматического предотвращения столкновений, к оснащению беспилотных авиационных систем оборудованием удаленной идентификации и оборудованием линий управления беспилотными авиационными системами и контроля беспилотных авиационных систем, средствами криптографической защиты информации, сертифицированными в соответствии с требованиями федерального органа исполнительной власти в области обеспечения безопасности, и Правил оснащения пилотируемых воздушных судов и беспилотных авиационных систем оборудованием, предусмотрен-

ным пунктом 1 статьи 78.3 Воздушного кодекса Российской Федерации: Постановление Правительства Рос. Федерации от 30.11.2024 № 1701. Доступ из справ.-правовой системы «КонсультантПлюс».

20. Приоритетные направления проектов технологического суверенитета и проектов структурной адаптации экономики Российской Федерации: Постановление Правительства Рос. Федерации от 15.04.2023 № 603. Доступ из справ.-правовой системы «КонсультантПлюс».

21. Стратегия развития беспилотной авиации Российской Федерации на период до 2030 года и на перспективу до 2035 года: Постановление Правительства Рос. Федерации от 21.06.2023 № 1630-р. Доступ из справ.-правовой системы «КонсультантПлюс».

22. Об утверждении Концепции и плана реализации Концепции интеграции беспилотных воздушных судов в единое воздушное пространство Российской Федерации в части развития технологий: утв. Распоряжением Правительства Рос. Федерации от 05.10.2021 № 2806-р. Доступ из справ.-правовой системы «КонсультантПлюс».

23. Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 года: Распоряжение Правительства Рос. Федерации от 19.08.2020 № 2129-р. Доступ из справ.-правовой системы «КонсультантПлюс».

24. Паспорт федерального проекта «Искусственный интеллект» национальной программы «Цифровая экономика Российской Федерации»: приложение № 3 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 27.08.2020 № 17. Доступ из справ.-правовой системы «КонсультантПлюс».

25. Основные направления дальнейшего развития единой системы информационно-аналитического обеспечения деятельности МВД России на период с 2020 по 2024 годы: утв. исполняющим обязанности Министра внутренних дел Рос. Федерации от 21.01.2020. Доступ из специализир. территориально распределенной автоматизированной системы «Юрист».

26. Об утверждении Наставления по организации экспертно-криминалистической деятельности в системе МВД России: приказ МВД России от 11.01.2009 № 7: ред. от 09.03.2023. Доступ из специализированной территориально распределенной автоматизированной системы «Юрист».

27. Сведения об опыте создания и применения специального программного обеспечения с технологиями искусственного интеллекта в Московской академии Следственного комитета Российской Федерации имени А. Я. Сухарева: письмо от 10.04.2024, исх. № 28-1653-24.

28. Сведения об опыте применения в Следственном управлении СК РФ по Волгоградской области специального программного обеспечения, в котором используются нейронные сети и технологии искусственного интеллекта: письмо от 19.03.2024, исх. № 2/3-23-24.

29. Приложение 10 к Конвенции о международной гражданской авиации «Авиационная электросвязь». Том VI «Системы и правила, относящиеся к линии C2 дистанционно пилотируемых авиационных систем. ICAO, 2006. 636 с.

30. ICAO Doc. 10019. Руководство по дистанционно пилотируемым авиационным системам (ДПАС). ICAO, 2015. 190 с.

31. Doc. 9896-AN/469 ICAO. Руководство по сети авиационной электросвязи (ATN), использующей стандарты и протоколы пакета протоколов Интернет (IPS). ИКАО, 2010. 112 с.

32. Doc. 9882 ICAO. Руководство по требованиям к системе организации воздушного движения. ICAO, 2009. 81 p.

33. Cir. 278 ИКАО. National Plan for CNS/ATM Systems Guidance Material. ICAO CIRCULAR 278. 2000. 170 p.

34. Doc. 10039 ICAO. Manual on System Wide Information Management (SWIM) Concept. Canso strategic technology workgroup (STWG) – Technology assessments, 2020. 21 p.

35. Doc 9694-AN/955 ICAO. Manual of air traffic services data link application. International civil aviation organization, 1999. 212 p.

36. Doc. 9869 ICAO. Performance-based Communication and Surveillance (PBCS) Manual. CAP 28 Rev 02, 2021. 14 с.

37. ГОСТ Р 70802-2023. Беспилотные авиационные системы для обеспечения пожаротушения, аварийно-спасательных и других работ, выполняемых в целях предупреждения чрезвычайных ситуаций и ликвидации их последствий. Общие требования. М.: Стандартинформ, 2023. 8 с. Доступ из справ.-правовой системы «КонсультантПлюс».

38. ГОСТ Р 59751-2021. Беспилотные авиационные системы с беспилотными воздушными судами самолетного типа. Требования к летной годности. М.: Стандартинформ, 2021. 126 с. Доступ из справ.-правовой системы «КонсультантПлюс».

39. ГОСТ Р 59517-2021. Беспилотные авиационные системы. Классификация и категоризация. М.: Стандартинформ, 2021. 10 с. Доступ из справ.-правовой системы «КонсультантПлюс».

40. ГОСТ Р 59519-2021. Беспилотные авиационные системы. Компоненты беспилотных авиационных систем. Спецификация и общие технические требования. М.: Стандартинформ, 2021. 10 с. Доступ из справ.-правовой системы «КонсультантПлюс».

41. ГОСТ Р 59520-2021. Беспилотные авиационные системы. Функциональные свойства станции внешнего пилота. М.: Стандартинформ, 2021. 15 с. Доступ из справ.-правовой системы «КонсультантПлюс».

42. ГОСТ Р 56122-2014. Воздушный транспорт. Беспилотные авиационные системы. Общие требования. М.: Стандартинформ, 2015. 11 с. Доступ из справ.-правовой системы «КонсультантПлюс».

43. ГОСТ Р 57258-2016. Системы беспилотные авиационные. Термины и определения. М.: Стандартинформ, 2016. 21 с. Доступ из справ.-правовой системы «КонсультантПлюс».

44. ГОСТ Р 54344-2011. Техника пожарная. Мобильные робототехнические комплексы для проведения аварийно-спасательных работ и пожаротушения. Классификация. Общие технические требования. Методы испытаний. М.: Стандартинформ, 2012. 31 с. Доступ из справ.-правовой системы «КонсультантПлюс».

45. ГОСТ Р ИСО/МЭК 27000-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология (утвержден и введен в действие Приказом Росстандарта от 19.05.2021 № 392-ст).

46. Проект национального стандарта ГОСТ Р 56939. Защита информации. Разработка безопасного программного обеспечения. Общие требования // URL: <https://fstec.ru/tk-362/standarty/proekty/proekt-natsionalnogo-standarta-gost-r-56939> (дата обращения: 23.05.2025).

47. Сводный отчет по России о результатах деятельности органов внутренних дел Российской Федерации по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, а также результатах деятельности структурных подразделений органов внутренних дел Российской Федерации, специализирующихся на противодействии преступлениям данного вида, за январь–декабрь 2021 года.

48. Сводный отчет по России о результатах деятельности органов внутренних дел Российской Федерации по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, а также результатах деятельности структурных подразделений органов внутренних дел Российской Федерации, специализирующихся на противодействии преступлениям данного вида, за январь–декабрь 2022 года.

49. Сводный отчет по России о результатах деятельности органов внутренних дел Российской Федерации по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, а также результатах деятельности структурных подразделений органов внутренних дел Российской Федерации, специализирующихся на противодействии преступлениям данного вида (сформирован с учетом требования приказа Генерального прокурора Российской Федерации от 03.07.2023 № 429), за январь–декабрь 2023 года.

50. Сводный отчет по России о результатах деятельности органов внутренних дел Российской Федерации по противодействию пре-

ступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, а также результатах деятельности структурных подразделений органов внутренних дел Российской Федерации, специализирующихся на противодействии преступлениям данного вида (сформирован с учетом требования приказа Генерального прокурора Российской Федерации от 03.07.2023 № 429), за январь–декабрь 2024 года.

Иные источники

51. Абрамова Я. «Гонка вооружений»: искусственный интеллект и кибербезопасность // Журнал «Директор информационной службы»: [сайт]. URL: <https://www.osp.ru/cio/2017/10/13053560> (дата обращения: 20.01.2025).

52. Автоматы и разумное поведение / Н. М. Амосов [и др.]. Киев: Наукова думка, 1973. 375 с.

53. Акишин Д. Н., Банников А. М., Газизов В. А. Перспективы развития программно-аппаратных средств при производстве портретных экспертиз // Энциклопедия судебной экспертизы. 2018. № 4 (19). С. 21–33.

54. Алгоритм мониторинга динамической зоны распространения лесных пожаров группой беспилотных летательных аппаратов / Ф. Б. Тебугева [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. 2023. Т. 50, № 1. С. 140–151.

55. Алексеева Е. Ф., Стефанюк В. Л. Экспертные системы – состояние и перспективы // Известия АН СССР: Техническая кибернетика. 1984. № 5. С. 153–167.

56. Алпадайн Э. Машинное обучение: новый искусственный интеллект / пер. с англ. Д. З. Вибе. М.: Точка, 2017. 191 с.

57. Амосов Н. М. Алгоритмы разума. Киев: Наукова думка, 1979. 223 с.

58. Аносов А. В. Современные нейросети в контексте угроз информационной безопасности // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 22–30.

59. Арбиб М. Метафорический мозг / пер. с англ. М.: Мир, 1976. 286 с.

60. Аргуновский Д. И., Толпыгин А. С. Стратегии импортозамещения средств защиты информации в условиях ресурсных ограничений для предприятий оборонно-промышленного комплекса: практические аспекты реализации, выбор оптимальных решений // Материалы II науч.-практ. конф. «Актуальные проблемы защиты информации: современность и перспективы» (Москва, 9–10 апреля 2024 г.) М.: МГТУ имени Н. Э. Баумана, 2025. С. 53–60.

61. Асатрян А. Применение ИИ и машинного обучения в кибер-

безопасности // Астрал. Безопасность, 01.06.2023: [сайт]. URL: <https://is.astral.ru/news/blog/primenenie-ii-i-mashinnogo-obucheniya-v-kiberbezopasnosti/> (дата обращения: 20.01.2025).

62. Астахова Е. А. Совершенствование автоматизированных информационных систем, используемых в расследовании преступлений // Правовая политика и правовая жизнь. 2024. № 3. С. 73–81.

63. Атабеков А. Р. Применение искусственного интеллекта в рамках реализации административной функции правоохранительных органов: опыт, перспективы, регламентация // Теория и практика общественного развития. 2023. № 4. С. 122–127.

64. Аткинсон Р., Бауэр Г., Кротерс Э. Введение в математическую теорию обучения / пер. с англ. М.: Мир, 1969. 487 с.

65. Ахметвалиев А. М. О возможности визуального распознавания речи в оптических каналах утечки информации // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 37–43.

66. Бабушкин А. А. Теоретико-правовая модель системы оперативно-розыскного контроля органов внутренних дел за лицами, склонными к совершению преступлений в условиях развития информационного общества // Философия права. 2024. № 3 (110). С. 95–101.

67. Балалаева Ю. С. «AI bias»: «Предвзятость искусственного интеллекта» или результат деятельности разработчиков? // Юристы-Правоведь. 2023. № 3(106). С. 7–14.

68. Батищев Д. И. Генетические алгоритмы решения экстремальных задач: учеб. пособие. Воронеж: ВГТУ, 1995. 69 с.

69. Батоев В. Б. «Большие данные (big data)» и предиктивная аналитика в оперативно-розыскной деятельности: проблемы использования и пути решения // Вестник Волгоградской академии МВД России. 2020. № 1 (52). С. 11–17.

70. Батоев В. Б. Использование предиктивной аналитики в правоохранительной деятельности // Общество и право. 2022. № 4 (82). С. 99–107.

71. Батоев В. Б. Применение искусственного интеллекта в деятельности правоохранительных органов // Вестник Академии Следственного комитета Российской Федерации. 2020. № 4 (26). С. 83–87.

72. Батоев В. Б., Семенчук В. В. Предиктивная аналитика в оперативно-розыскной деятельности: международный и отечественный опыт проведения оперативно-розыскного мониторинга информационно-телекоммуникационных сетей и систем // Вестник Краснодарского университета МВД России. 2020. № 1 (47). С. 53–60.

73. Батулин Ю. М. Проблемы компьютерного права. М.: Юридическая литература, 1991. 272 с.

74. Батулин Ю. М., Жодзишский А. М. Компьютерная преступ-

ность и компьютерная безопасность. М.: Юридическая литература, 1991. 160 с.

75. Бахтеев Д. В. Искусственный интеллект: этико-правовые основы: моногр. М.: Проспект, 2021. 176 с.

76. Бахтеев Д. В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений: дис... д-ра юрид. наук. Екатеринбург, 2022. 385 с.

77. Бёрджесс Э. Искусственный интеллект – для вашего бизнеса? Руководство по оценке и применению / пер. с англ. М.: Альпина Паблишер, 2020. 232 с.

78. Бердникова О. П., Андроник Н. А. Особенности расследования хищений, совершенных с использованием ИТ-технологий: учеб.-практ. пособие. Екатеринбург: Уральский юридический институт МВД России, 2022. 72 с.

79. Бердникова О. П., Дерюгин Р. А. Особенности расследования мошенничества в сфере компьютерной информации: учеб. пособие. Екатеринбург: Уральский юридический институт МВД России, 2022. 84 с.

80. Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений. М., 2021. 816 с.

81. Бессонов А. А. Криминалистическая характеристика преступлений в цифровую эпоху // Сб. материалов Междунар. науч.-практ. конф.. В 2 ч. (Москва, 20 мая 2022 г.). Ч. 1. М., 2022. С. 54–62.

82. Бецков А. В. Высотные аэростатические мобильные платформы как перспективное научно-техническое направление // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 94–97.

83. Бецков А. В. Баранов В. В. Информационные технологии управления: курс лекций. М.: Академия управления МВД России, 2023. 91 с.

84. Биометрическая защита объектов: моногр. / В. А. Минаев, К. М. Бондарь, С. В. Дворянкин, А. М. Алюшин, В. Ю. Федорович; под ред. В. А. Минаева, К. М. Бондаря; Дальневосточный юридический институт МВД России имени И. Ф. Шилова. Хабаровск: РИО ДВЮИ МВД России имени И. Ф. Шилова, 2024. 284 с.

85. Блюменау Д. И. Информация и информационный сервис. М.: Наука, 1989. 192 с.

86. Бокова И., Галов Д., Котиков Н. Итоги кибербезопасности за 2024 год: атаки с помощью ИИ и манипуляция эмоциями // Hi-Tech Mail, 17.01.2025: [сайт]. URL: <https://hi-tech.mail.ru/review/121083-itogi-kiberbezopasnosti-za-2024-god/> (дата обращения: 20.01.2025).

87. Болотова Л. С. Системы искусственного интеллекта. Модели и технологии, основанные на знаниях. М.: Финансы и статистика, 2012. 664 с.

88. Бонгард М. М. Проблема узнавания. М.: Наука, 1967. 320 с.

89. Бондарь К. М., Броненкова Ю. В. Актуальные направления противодействия киберпреступности // Сб. науч. тр. Всерос. семинара «Применение современных информационных и телекоммуникационных технологий в раскрытии и расследовании киберпреступлений» (Хабаровск, 25 июня 2025 г.). Хабаровск: РИО ДВЮИ МВД России имени И. Ф. Шилова, 2025. С. 29–36.

90. Бондарь К. М., Дунин В. С. Геоинформационные системы как элемент информационно-аналитического обеспечения раскрытия и расследования преступлений // Сб. науч. тр. Всерос. семинара «Применение современных информационных и телекоммуникационных технологий в раскрытии и расследовании киберпреступлений» (Хабаровск, 24 июня 2021 г.). Хабаровск: РИО ДВЮИ МВД России, 2021. С. 74–83.

91. Бондарь К. М., Дунин В. С. Поисковая техника, средства контроля и досмотра: учеб.-практ. пособие (изд. 2-е, доп., перераб.). Хабаровск: РИО ДВЮИ МВД России, 2022. 156 с.

92. Бондарь К. М., Дунин В. С. Пути интеграции геоинформационных систем для аналитического обеспечения раскрытия и расследования преступлений // Новые информационные технологии в научных исследованиях; Материалы XXV Юбилейной Всерос. науч.-техн. конф. студентов, молодых ученых и специалистов. Рязань, 2020. С. 248–249.

93. Бондарь К. М., Дунин В. С., Чемарев Д. В. Сетевая модель распространения информации при возникновении массовых беспорядков // Вестник МВД России. 2019. № 5 (162). С. 24–32.

94. Бондарь К. М., Киселев В. И. Автоматизированные банки данных и их использование в органах внутренних дел: учеб. пособие. Хабаровск: ДВЮИ МВД России, 2000. 92 с.

95. Бондарь К. М., Минаев В. А., Коломина А. С. Технологии поиска дискредитирующей информации в социальных медиа // Информация и безопасность. 2024. Т. 27. Вып. 4. С. 591–598.

96. Бостром Н. Искусственный интеллект. Этапы. Угрозы. Стратегии / пер. с англ. С. Филина. М.: Манн, Иванов и Фербер, 2016. 404 с.

97. Бринк Х., Ричардс Д., Феверолф М. Машинное обучение / пер. с англ. И. Рузмайкиной. СПб.: Питер, 2017. 330 с.

98. Бронфельд Г. Б. Основы искусственного интеллекта. Н. Новгород: Нижегородский государственный технический университет имени Р. Е. Алексеева, 2014. 253 с.

99. Бронфельд Г. Б. Прямое наложение знаний и его возможности. Анализ, методология, новая модель знаний, алгоритмы, возмож-

ности «невозможности». Saarbrücken, Deutschland: LAP LAMBERT Academic Publishing, 2014. 236 с.

100. Бруссард М. Искусственный интеллект: пределы возможного / пер. с англ. Е. Арье. М.: Альпина нон-фикшн, 2020. 361 с.

101. Будко Д. В. Искусственные генеративные технологии в механизме преступной деятельности // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 118–125.

102. Бурков А. Машинное обучение без лишних слов / пер. с англ. А. Киселева. СПб.: Питер, 2020. 188 с.

103. Буч Г., Рамбо Д., Джекобсон А. Язык UML. Руководство пользователя / пер. с англ. М.: ДМК, 2000. 432 с.

104. В России прошли масштабные испытания лазерных систем против беспилотников // URL: https://www.rbc.ru/technology_and_media/13/06/2025/684c0ccf9a794728e33abf85?ysclid=mc6wwdi238224650112 (дата обращения: 18.06. 2025).

105. Варфоломеев А. А., Пеленицын М. Б. Методы криптографии и их применение в банковских технологиях. М., 1995. 116 с.

106. Введенская О. Ю. Расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий: учеб.-практ. пособие. Краснодар: Краснодарский университет МВД России, 2022. 52 с.

107. Вейценбаум Дж. Возможности вычислительных машин и человеческий разум. От суждений к вычислениям / пер. с англ. М.: Радио и связь, 1982. 368 с.

108. Великий китайский файрвол: как Китай контролирует внутренний Интернет // URL: <https://skillbox.ru/media/code/velikiy-kitayskiy-fayrvol-kak-kitay-kontroliruet-vnutrenniy-internet/>. (дата обращения: 11.10.2024).

109. Венда В. Ф. Системы гибридного интеллекта: эволюция, психология, информатика. 2-е изд. М.: URSS: ЛЕНАНД, 2020. 446 с.

110. Ветрова Е. ИИ в кибербезопасности: вызовы, возможности, угрозы // URL: <https://virtre.ru/articles/artificial-intelligence/ii-v-kiber-bezopasnosti-vyzovy-vozmozhnosti-ugrozy> (дата обращения: 22.01.2025).

111. Видеоспектральные методы и средства мониторинга контролируемых параметров лесных пожаров и аварий, связанных с разливом нефтепродуктов / А. С. Сизиков [и др.] // Приборы и методы измерений. 2023. Т. 14, № 1. С. 62–70.

112. Винер Н. Кибернетика и общество. Творец и робот / пер. с англ. М.: Тайдекс Ко, 2003. 246 с.

113. Владимиров В. Ю., Данилов И. А., Ильин Н. Н. Искусственный интеллект в борьбе с серийными преступлениями. Научная

разработка в практику // Труды Академии управления МВД России. 2024. № 4 (72). С. 139–150.

114. Возможности использования искусственного интеллекта в экспертно-криминалистической деятельности: науч.-аналит. обзор (37/8-6263) / А. Н. Бардаченко [и др.]; Волгоградская академия МВД России. Волгоград, 2025. 138 с.

115. Волков А. А. Современные алгоритмы распознавания лиц // Сб. науч. тр. Всерос. семинара «Применение современных информационных и телекоммуникационных технологий в раскрытии и расследовании киберпреступлений» (Хабаровск, 25 июня 2025 г.). Хабаровск: РИО ДВЮИ МВД России имени И. Ф. Шилова, 2025. С. 61–68.

116. Волков А. В. Искусственный интеллект: от компьютеров к киборгам. М.: Вече, 2020. 254 с.

117. Вычерова Н. Р., Будевич Е. А., Беляев А. Э. Разработка системы раннего обнаружения лесных пожаров с использованием беспилотных летательных аппаратов и искусственного интеллекта // Resources and Technology. 2022. Т. 19, No 4. Pp. 85–101.

118. Вычислительные машины и мышление / под ред. Э. Фейгенбаума и Дж. Фельдмана / пер. с англ. под ред. Э. М. Бравермана [и др.]. М.: Мир, 1967. 552 с.

119. Вычислительные системы, сети и телекоммуникации: учеб. / А. П. Панибратов [и др.] / под ред. А. П. Панибратова. М.: Финансы и статистика, 1998. 400 с.

120. Гаазе-Рапопорт М. Г. Автоматы и живые организмы. М.: Физматгиз, 1961. 224 с.

121. Гаазе-Рапопорт М. Г., Поспелов Д. А. От амёбы до робота: модели поведения. М.: Наука, 1987. 288 с.

122. Гаврилова Т. А., Хорошевский В. Ф. Базы знаний интеллектуальных систем. СПб.: Питер, 2001. 384 с.

123. Гайкович В. Ю., Ершов Д. В. Основы безопасности информационных технологий: учеб. пособие. М.: МИФИ, 1995. 82 с.

124. Галатенко В. А. Основы информационной безопасности: курс лекций. М.: Национальный открытый университет ИНТУИТ, 2024. 266 с.

125. Гаспарян Д. Э., Стырин Е. М. Прикладные проблемы внедрения этики искусственного интеллекта в России: отраслевой анализ и судебная система. М.: Издат. дом Высш. школы экономики, 2020. 109 с.

126. Гельманова З. С., Бакаев Т. К. Внедрение искусственного интеллекта в деятельность органов внутренних дел // Юридические науки LEGAL SCIENCES. 2024. С. 45–48.

127. Геополитика и основы безопасности государства / С. А. Модестов [и др.]; под. ред. Ю. М. Батурина. М.: ВА ГШ, РАГС, 1995. 50 с.

128. Геоскан. Итоги Архипелага 2024: новые рынки и инициати-

вы в области беспилотных технологий // URL: <https://www.geoscan.ru/ru/blog/itogi-arkhipelaga-2024> (дата обращения: 03.05.2025).

129. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. Книги 1, 2. М.: Энергоиздат, 1994. 576 с.

130. Герасименко В. А., Малюк А. А. Основы защиты информации. М.: МОПО, МИФИ, 1997. 537 с.

131. Гладун В. П. Партнерство с компьютером (человеко-машинные целеустремленные системы). К.: Port-Royal, 2000. 128 с.

132. Гладун В. П. Эвристический поиск в сложных средах. Киев: Наукова думка, 1977. 166 с.

133. Глобальный атлас регулирования искусственного интеллекта 2024: исследование мирового опыта. 3-е изд., доп. и перераб. / под ред. А. В. Незнамова // Вектор БРИКС. М., 2024. 384 с.

134. Глобальный атлас регулирования искусственного интеллекта / под ред. А. В. Незнамова. Доступ из справ.-правовой системы «КонсультантПлюс».

135. Глобальный атлас регулирования искусственного интеллекта. Издание 2023 / под ред. А. В. Незнамова. Доступ из справ.-правовой системы «КонсультантПлюс».

136. Глушков В. М. Введение в кибернетику. Изд. 2-е. М.: URSS, 2022. 328 с.

137. Глушков В. М. Введение в теорию самосовершенствующихся систем. 2-е изд., стереотип. М.: URSS, 2022. 112 с.

138. Гордеев А. Ю. Перспективы развития и использования искусственного интеллекта и нейросетей для противодействия преступности в России (на основе зарубежного опыта) // Научный портал МВД России. 2021. № 1 (53). С. 123–135.

139. Горелов И. Н. Разговор с компьютером: психолингвистический аспект проблемы. М.: Наука, 1987. 256 с.

140. Грек А. Обратная сторона ИИ: как нейросети работают в руках кибермошенников // URL: <https://www.techinsider.ru/technologies/1567177-obratnaya-storona-ii-kak-neyroseti-rabotayut-v-rukah-kibermo-shennikov/> (дата обращения: 23.01.2025).

141. Гречанюк Ф. А., Здирук К. Б., Толпыгин А. С. Киберконтракт как инструмент регулирования гражданско-правовых отношений в цифровой экономике / Тезисы докладов XVI Всерос. науч. конф. «Нейрокомпьютеры и их применение». М.: Изд-во МГППУ, 2018. С. 376–377.

142. Григорьев А. С виртуальным помощником проще служить // Полиция России. 2024. № 4. С. 18–21.

143. Григорьев И. Д., Орлов В. Г. Анализ уязвимостей АЗН-В на базе 1090 Extended Squitter // Фундаментальные проблемы радиоэлектронного приборостроения, 2016. № 5. Т. 16. С. 171–174.
144. Григорьев И. Д., Орлов В. Г. Исследование вопросов безопасности системы АЗН-В // Телекоммуникации и информационные технологии, 2016. Т. 3. С. 53–55.
145. Гринбаум А. Машина-доносчица: как избавить искусственный интеллект от зла. М.: ТрансЛит, 2017. 75 с.
146. Гурвич И. С. Защита ЭВМ от помех. 2-е изд., перераб. и доп. М.: Энергоатомиздат, 1984. 224 с.
147. Давыдов В. О. Преступность и искусственный интеллект: криминалистическое прогнозирование факторов благоприятствования // Философия права: научно-теоретический журнал. 2024. № 3 С. 109–115.
148. Дашков Т. К., Домышева Т. В., Комоско А. А. К вопросу о применении алгоритмов искусственного интеллекта при установлении лиц, совершивших преступление // Криминалистика: вчера, сегодня, завтра. 2021. № 4 (20). С. 31.
149. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие: в 2 ч. / А. В. Аносов [и др.]. Ч. 1. М.: Академия управления МВД России, 2019. 208 с.
150. Дж. Вандер Плас. Python для сложных задач: наука о данных и машинное обучение / пер. с англ. И. Пальти. СПб.: Питер, 2021. 572 с.
151. Джордан Джон. Роботы / пер. с англ. П. Шера, Ю. Левчука. М.: Точка: Фонд развития промышленности, 2017. 259 с.
152. Доклад Святейшего Патриарха Кирилла на XIII Рождественских Парламентских встречах // URL: <https://pravoslavie.ru/166899.html?ysclid=m6kqtgamja23547138> (дата обращения: 30.01.2025).
153. Доклад Святейшего Патриарха Кирилла на пленарном заседании XXXIII Международных Рождественских образовательных чтений «80-летие Великой Победы: память и духовный опыт поколений» // URL: <https://vn-eparhia.ru/obshchetserkovnye-novosti/19106-doklad-svyatejshego-patriarkha-kirilla-na-plenarnom-zasedanii-xxkhiii-mezhdunarodnykh-rozhdestvenskikh-obrazovatelnykh-chtenij.html> (дата обращения: 30.01.2025).
154. Доэрти П. Уилсон Д. Человек + машина. Новые принципы работы в эпоху искусственного интеллекта / пер. с англ. О. Сивченко, Н. Яцюк. М.: Манн, Иванов и Фербер, 2019. 297 с.
155. Дрейфус Х. Чего не могут вычислительные машины. Критика искусственного разума / пер. с англ. М.: Прогресс, 1978. 333 с.
156. Дрейфус Х. Чего не могут вычислительные машины: критика искусственного разума / пер. с англ. Н. Родман. 2-е изд. М.: Либерком, 2010. 333 с.

157. Дрон «Князь Вандал» уничтожил технику НАТО на сумму свыше 2 миллиардов долларов. Что известно о российском беспилотнике? // URL: <https://lenta.ru/news/2025/06/21/dron-knyaz-vandal-unichtozhil-tehniku-nato-na-summu-svyshe-2-milliardov-dollarov-cto-izvestno-o-rossiyskom-bespilotnike/?ysclid=mc6uft6njd68717114> (дата обращения: 22.06.2025).

158. Дронова О. Б., Смагоринский Б. П. Интеграция данных экспертно-криминалистических и оперативных учетов как способ повышения уровня информационного обеспечения раскрытия и расследования преступлений // Юридическая наука и правоохранительная практика. 2024. № 2 (68). С. 51–58.

159. Дубровский Д. И. Сознание, мозг, искусственный интеллект. М.: Стратегия-Центр, 2007. 272 с.

160. Дунин В. С., Бондарь К. М. Математическое моделирование для обеспечения интеллектуальных задач правоохранительной деятельности // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов». М.: Академия управления МВД России, 2023. С. 108–116.

161. Дэвенпорт Т. Внедрение искусственного интеллекта в бизнес-практику. Преимущества и сложности / пер. с англ. М.: Альпина Паблишер, 2020. 315 с.

162. Естественный и искусственный интеллект: методологические и социальные проблемы: сборник статей / под ред. Д. И. Дубровского и В. А. Лекторского. М.: Канон+, 2011. 351 с.

163. Ефимов Е. И. Решатели интеллектуальных задач. М.: Наука, 1982. 320 с.

164. Жданов Ю. В., Овчинский В. С. Полиция будущего. М., 2018. 166 с.

165. Жельников В. Криптография от папируса до компьютера. М.: АБФ, 1996. 336.

166. Завьялов И. А. Зарубежный опыт использования искусственного интеллекта в раскрытии преступлений // Вестник Московского университета МВД России. 2021. № 3. С. 228–236.

167. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учеб. пособие. Барнаул: АлтГТУ, 2011. 252 с.

168. Заде Л. Понятие лингвистической переменной / пер. с англ. М.: Мир, 1976. 165 с.

169. Защита информации в компьютерных системах и сетях / Ю. В. Романец [и др.]; под. ред. В. Ф. Шаньгина. М.: Радио и связь, 1999. 328 с.

170. Здирук К. Б. Реализация задач сбора, консолидированной обработки и управления разнородными источниками данных процесса подготовки космонавтов при интеграции ФГБУ «НИИ ЦПК имени

Ю. А. Гагарина» в единое информационное пространство ракетно-космической отрасли // Материалы XI Междунар. науч.-практ. конф. Пилотируемые полеты в космос. Звездный городок: Научно-исследовательский испытательный центр подготовки космонавтов имени Ю. А. Гагарина, 2015. С. 119–121.

171. Зегжда Д. П., Ивашко А. М. Как построить защищенную информационную систему / под ред. Д. П. Зегжды и В. В. Платонова. СПб.: Мир и семья-95, 1997. 312 с.

172. Иванов А. И., Лекарь Л. А. Автоматическое формирование портретов телефонных мошенников // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 168–175.

173. ИИ уже поглотил все человеческие знания, предупреждает Илон Маск // URL: <https://new-science.ru/ii-uzhe-poglotil-vse-chelovecheskie-znaniya-preduprezhdaet-ilon-mask/> (дата обращения: 12.01.2025).

174. Информатизация и информационная безопасность правоохранительных органов // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. 448 с.

175. Информатика и информационные технологии в юридической деятельности: учеб. пособие. 2-е изд., перераб. / К. М. Бондарь [и др.] / под ред. В. А. Минаева, А. П. Фисуна, К. М. Бондаря. Хабаровск: ДВЮИ МВД России, 2011. 380 с.

176. Информационно-безопасные системы. Анализ проблемы: учеб. пособие. Изд. 2-е, испр. и доп. М.: МИФИ, 1995. 84 с.

177. Информационные технологии в аналитической разведке: учеб. пособие / сост. Е. С. Поликарпов. Краснодар: Краснодарский университет МВД России, 2016. 238 с.

178. Информационные технологии управления в органах внутренних дел / В. А. Минаев [и др.]; под ред. В. А. Минаева. М.: Академия управления МВД России, 1997. 704.

179. Информация и информационная безопасность: учеб. пособие / К. М. Бондарь [и др.]. Хабаровск: ДВЮИ МВД России, 2002. 528 с.

180. Искалиев Р. Г. Первичный поиск оперативной информации подразделениями ЭБиПК в современных условиях // Труды Академии управления МВД России. 2023. № 4 (68). С. 107–117.

181. Искалиев Р. Г. Противодействие органов внутренних дел преступлениям в сфере экономической деятельности в условиях цифровой трансформации: моногр. М.: Проспект, 2024. 144 с.

182. Искусственный интеллект на службе полиции: сб. ст. Междунар. науч.-практ. конф. М.: Академия управления МВД России, 2021. 118 с.

183. Искусственный интеллект (большие данные) на службе полиции // Сб. ст. междунар. науч.-практ. конф. М.: Академия управления МВД России, 2020.
184. Искусственный интеллект в кибербезопасности // Developers.sber.ru, 10.01.2025: [сайт]. URL: <https://developers.sber.ru/help/gigachat-api/cybersecurity> (дата обращения: 20.01.2025).
185. Искусственный интеллект в кибербезопасности: перспективы, проблемы и преимущества // Esapro, 01.08.2023: [сайт]. URL: <https://esapro.ru/blog/iskusstvennyy-intellekt-v-kiberbezopasnosti-perspektivy-problemy-i-preimushchestva/?ysclid=m6e29ijhtf627396014> (дата обращения: 20.01.2025).
186. Искусственный интеллект: справ. В 3-х кн. Кн. 1: Системы общения и экспертные системы / под ред. Э. В. Попова. М.: Радио и связь, 1990. 461 с.
187. Искусственный интеллект: справ. В 3-х кн. Кн. 2: Модели и методы / под ред. Д. А. Поспелова. М.: Радио и связь, 1990. 304 с.
188. Исследование технологий моделирования на основе искусственного интеллекта с целью фальсификации цифровых доказательств: аналитический обзор с предложениями / С. В. Лемайкина [и др.]. Ростов н/Д.: Ростовский юридический институт МВД России, 2023. 37 с.
189. История года: влияние искусственного интеллекта на кибербезопасность / В. Тушканов [и др.] // URL: <https://securelist.ru/story-of-the-year-2023-ai-impact-on-cybersecurity/108558/> (дата обращения: 20.01.2025).
190. К 2029 году ИИ станет умнее всех людей, вместе взятых, считает Маск // URL: <https://ria.ru/20240313/ii-1932723756.html?in=t>. (дата обращения: 29.12.2024).
191. Казьмин В. Готовы противостоять любым вызовам // Полиция России. 2024. № 3. С. 12–16.
192. Казьмин В., Громова А. Как распознать искусственную речь // Полиция России. 2024. № 4. С. 12–14.
193. Кандрашина Е. Ю., Литвинцева Л. В., Поспелов Д. А. Представление знаний о времени и пространстве в интеллектуальных системах / под ред. Д. А. Поспелова. М.: Наука, 1989. 328 с.
194. Каримов А. М., Смирнов С. В., Марданов Г. Д. Основы кибербезопасности: учеб.-практ. пособие. Казань: КЮИ МВД России. 63 с.
195. Карпушин Е. Методология обработки информации в искусственном интеллекте. М.: LAP Lambert Academic Publishing, 2012. 156 с.
196. Картографирование ареалов наркотических растений с использованием технологий ГИС и дистанционного зондирования / Н. П. Огарь [и др.] // URL: <https://arcreview.esri-cis.ru/2008/05/13/gis-vegetation-mapping/> (дата обращения: 12.05. 2025).
197. Кахро М. И., Калья А. П., Тыугу Э. Х. Инструментальная система программирования ЕС ЭВМ (ПРИЗ). М.: Финансы и статистика, 1981. 158 с.

198. Келли К. Неизбежно. 12 технологических трендов, которые определяют наше будущее / пер. с англ. М.: Манн, Иванов и Фербер, 2017. 352 с.
199. Кемпф В. А. Обеспечение информационной безопасности в органах внутренних дел: учеб. пособие. Барнаул: Барнаульский юридический институт МВД России, 2019. 63 с.
200. Киберустойчивость информационной инфраструктуры: модели исследования: моногр. / М. П. Сычев [и др.] / под общ. ред. С. В. Скрыля. М.: РУСАЙНС, 2021. 256 с.
201. Клёсова Ю. В., Татарчук И. А., Кулаков М. С. Перспективные технологии в авиации на базе ОВЧ ЛПД режима 4 // Телекоммуникации и транспорт, 2015. Т. 9. № 8. С. 63–67.
202. Кольер Р., Монтонен К., Азарми Б. Машинное обучение в Elastic Stack: получите максимальную отдачу от ваших данных благодаря уникальному сочетанию передовых технологий / пер. с англ В. С. Яценкова. М.: ДМК Пресс, 2022. 379 с.
203. Копылов В. А. Информационное право: учеб. пособие. М.: Юрист, 1997. 472 с.
204. Королькова Е. Проблема острая, решение есть // Полиция России. 2025. № 1. С. 11.
205. Костанди М. Нейропластичность / пер. с англ. В. Карпюк, К. Разживин. М.: ФРП: Точка, 2017. 156 с.
206. Кресан Е. Как взломать «матрешку» // Полиция России. 2025. № 1. С. 24–27.
207. Кроуфорд К. Атлас искусственного интеллекта: руководство для будущего / пер. с англ. О. Захватовой. М.: АСТ, 2023. 318 с.
208. Крылов В. В. Информационные компьютерные преступления. Расследование преступлений в сфере информации. М.: Изд-во «Городец», 1998. 264 с.
209. Крылов В. В. Расследование преступлений в сфере информации. М.: Инфра-М, 1997. 285 с.
210. Крылов Д. Blue CRUSH POLICE – Информационные технологии в руках полиции // URL: <https://brightonbeachnews.com/rus/blue-crush-police-> (дата обращения: 20.02.2025).
211. Кузнецов Д. В. Уголовно-процессуальные и организационно-тактические вопросы выявления и расследования преступлений, связанных с использованием криптовалют и других виртуальных активов: учеб. пособие. Казань: Казанский юридический институт МВД России, 2022. 76 с.
212. Кузьмина К. А. Нейросетевые модели мониторинга социальных медиа для выявления деструктивного контента // «Цифропол–2025». М., 2025. С. 34–38.
213. Кулаков М. С. Разработка принципов организации мобильных сетевых структур в авионике: дис. ... канд. техн. наук. М., 2018. 186 с.

- /214. Курейчик В. М. Генетические алгоритмы. Таганрог: ТРТИ, 1998. 242 с.
215. Курин А. А., Гаужаева В. А. Электронно-цифровые следы как объекты криминалистической регистрации // Право и управление. 2023. № 7. С. 141–147.
216. Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. М.: Новый Юрист, 1998. 256 с.
217. Лагуточкин А. В. Сущность, формирование и перспективы использования нейросетевых технологий в оперативно-розыскной деятельности // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2022. Т. 8 (74). № 4. С. 354–365.
218. Лапшин И. О., Волков А. А. Робастное распознавание лиц: сравнительный анализ современных алгоритмов // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 203–213.
219. Лапшина И. Е., Зеленкова Л. К. Международная организация уголовной полиции (Интерпол): вопросы правосубъектности, правового регулирования и деятельности в киберпространстве // Юридическая наука. 2023. № 6. С. 192–198.
220. Лащёнов М. С., Лащёнов П. М. Роль информационных технологий в борьбе с кибермошенничеством // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 214–219.
221. Левин В. И., Поспелов Д. А. Развитие искусственного интеллекта в СССР // Problems of Artificial Intelligence. 2021. № 2 (21) С. 59–64.
222. Леонов А. П., Копейна А. В., Макшанцева А. В. Основы кибербезопасности: курс лекций. Екатеринбург: Уральский юридический институт МВД России, 2022. 176 с.
223. Леонов Б. П. О методах автоматического реферирования (США 1958–1974 гг.) // Научно-техническая информация, сер. 2. 1975. № 6. С. 16–20.
224. Лидтке Д. Растровая аналитика расширяет использование изображений в ГИС // URL: <https://arcreview.esri-cis.ru/2019/12/31/images-in-gis/> (дата обращения: 12.05.2025).
225. Лингвистическое обеспечение в системе автоматического перевода третьего поколения / Ю. Д. Апресян [и др.]. М.: ВИНТИ, 1978. 47 с.
226. Ллойд С. Программируя Вселенную: квантовый компьютер и будущее науки. 4-е изд. / пер. с англ. А. Стативка. М.: Альпина нон-фикшн, 2019. 254 с.
227. Локнов А. И., Синещук Ю. И., Родин В. Н. Средства и системы обработки информации: учеб. пособие. СПб.: СПбУ МВД России, 2023. 124 с.

228. Лорьер Ж.-Л. Системы искусственного интеллекта / пер. с англ. М.: Мир, 1991. 568 с.
229. Макаров К. С. Структурная схема комплекса с беспилотным летательным аппаратом, предназначенным для мониторинга территории и объектов в условиях низкой доступности каналов связи // Auditorium. Электронный научный журнал Курского государственного университета. № 4 (24). 2019.
230. Малкольм Ф., Рериг П., Принг Б. Что делать, когда машины начнут делать все. Как роботы и искусственный интеллект изменят жизнь и работу. М.: Бомбора, 2019. 320 с.
231. Марков А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности. 2022. № 1(47). С. 1–9.
232. Маркофф Дж. Номо roboticus? Люди и машины в поисках взаимопонимания / пер. с англ. В. ИONOва, С. Махарадзе. М.: Альпина нон-фикшн, 2017. 404 с.
233. Маркс К., Энгельс Ф. Соч. 2-е изд. Т. 26. Ч. 1.
234. Маслов С. Ю. Теория дедуктивных систем и ее применение. М.: Радио и связь, 1986. 135 с.
235. Матвеев М. Г., Свиридов А. С., Алейникова Н. А. Модели и методы искусственного интеллекта. Применение в экономике. М.: Финансы и статистика, 2008. 448 с.
236. Математические модели анализа, оценки, прогнозирования и управления в органах внутренних дел: моногр. / В. А. Минаев [и др.]; под ред. В. А. Минаева, К. М. Бондаря. Хабаровск: РИО ДВЮИ МВД России, 2022. 308 с.
237. Мельчук И. А., Равич Р. Д. Автоматический перевод 1949–1963: критико-библиограф. справ. М.: ВИНТИ, 1967. 517 с.
238. Менщиков А. А., Заколдаев Д. А., Воробьева А. А. Введение в кибербезопасность и киберустойчивость: учеб.-метод. пособие. СПб.: Университет ИТМО, 2024. 72 с.
239. Метсола Р. Европарламент одобрил первый в истории комплексный закон об ИИ // URL: <https://ria.ru/20240313/zakon-1932729659.html> (дата обращения: 29.12.2024).
240. Миклашевская А. ИИ разложили по юридическим полочкам // URL: <https://www.kommersant.ru/doc/6394442> (дата обращения: 29.12.2024).
241. Минаев В. А. Обеспечение безопасности социальных медиа на основе методов искусственного интеллекта // Кибернетика и информационная безопасность, 2023. С. 14–15.
242. Минаев В. А. Опыт и перспективы применения математического моделирования в решении задач анализа, оценки и прогнозирования криминогенной обстановки / В. А. Минаев, К. М. Бондарь, В. С. Дунин, П. Б. Скрипко // Криминологический журнал. 2022. № 1. С. 103–110.

243. Минаев В. А., Коломина А. С. Моделирование процессов распространения дискредитирующей информации в социальных сетях // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 234–253.

244. Минаев В. А., Королев И. Д., Мухортов В. В. Марковские модели защиты информационных систем беспилотных робототехнических объектов // Интернет-журнал «Технологии техносферной безопасности». 2016. № 6 (70). URL: [http:// ipb.mos.ru/ttb/2016-6.html](http://ipb.mos.ru/ttb/2016-6.html) (дата обращения: 15.04.2024).

245. Минаев В. А., Мокшанцев А. В. Системное описание оперативной обстановки по линии служб чрезвычайного реагирования // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2024. С. 180–188.

246. Минаев В. А., Мокшанцев А. В., Фаддеев А. О. Новая парадигма геодинамического риск-зондирования российских территорий // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 243–253.

247. Минаев В. А., Поликарпов Е. С. Китайский взгляд на развитие и безопасность киберпространства // Информация и безопасность. 2023. Т. 26. С. 535–542.

248. Минаев В. А., Рабчевский А. Н., Рабчевский Е. А. Моделирование активности ботов в ходе информационных атак // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 254–261.

249. Минаев В. А., Рабчевский Е. А. Идентификация ролей пользователей в социальных медиа // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2024. С. 189–196.

250. Минаев В. А., Реброва А. Д., Симонов А. В. Выявление деструктивного контента в социальных медиа на основе моделей машинного обучения // Информация и безопасность. 2021. Т. 24. Вып. 1. С. 7–20.

251. Минаев В. А., Симонов А. В. Сравнение моделей-трансформеров BERT при выявлении деструктивного контента в социальных медиа // Информация и безопасность. 2022. Т. 25. № 3. С. 341–348.

252. Минаев В. А., Симонов А. В., Поликарпов Е. С. Применение глубоких нейронных сетей для выявления деструктивного кон-

тента в социальных медиа // Информация и безопасность. 2021. Т. 24. Вып. 3. С. 361–372.

253. Минаев В. А., Толпыгин А. С. Беспилотный транспорт и технологии кибербезопасности // Общество. Право. Современность: материалы науч.-представит. мероприятий. Красноярск: Сибирский юридический институт МВД России, 2024. С. 230–235.

254. Минаев В. А., Толпыгин А. С. Кибербезопасность беспилотного транспорта // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2024. С. 197–204.

255. Минаев В. А., Толпыгин А. С. Кибербезопасность и киберустойчивость беспилотных транспортных систем // Информация и безопасность. 2024. Т. 27. № 2. С. 177–184.

256. Минаев В. А., Толпыгин А. С. Кибербезопасность систем управления беспилотным транспортом // Актуальные проблемы науки и практики: сб. науч. тр. по итогам научно-представительских мероприятий. Хабаровск: РИО ДВЮИ МВД России, 2024. С. 142–147.

257. Минаев В. А., Толпыгин А. С. Кибербезопасность управления беспилотным транспортом // Сб. науч. тр. Второй Всерос. науч.-техн. конф. «Кибернетика и информационная безопасность – КИБ-2024». М.: Национальный исследовательский ядерный университет «МИФИ», 2024. С. 180–181.

258. Минаев В. А., Толпыгин А. С. Цифровая платформа для защищенных информационно-управляющих систем беспилотного транспорта // Информация и безопасность. 2024. Т. 27. № 3. С. 309–318.

259. Минаев В. А., Толпыгин А. С. Цифровая платформа информационной защиты беспилотного транспорта // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 262–269.

260. Минаев В. А., Толпыгин А. С., Бондарь К. М. Кибербезопасность беспилотных авиационных систем мониторинга лесных территорий // Информация и безопасность. 2024. Т. 27. № 4. С. 553–568.

261. Минаев В. А., Фаддеев А. О. Геофизические факторы как угрозы кибербезопасности // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 205–211.

262. Минаев В. А., Швырев Б. А., Ромашкин Т. Р. Безопасность Интернета вещей: основные решения // Информация и безопасность. 2023. Т. 26. Вып. 2. С. 163–168.

263. Минаев В. А., Бондарь К. М., Федорович В. Ю. Биометрия защиты объектов: возможности и перспективы // Информация и безопасность. 2025. Т. 28. Вып. 1. С. 47–56.

264. Минаев В. А., Толпыгин А. С. Кибербезопасность систем

управления беспилотным транспортом // Применение современных информационных и телекоммуникационных технологий в раскрытии и расследовании киберпреступлений (Хабаровск, 27 июня 2024 г.). Хабаровск: РИО ДВЮИ МВД России имени И. Ф. Шилова, 2024. С. 142–147.

265. Минделл Д. Восстание машин отменяется! Мифы о роботизации / пер. с англ. В. Краснянской. М.: Альпина нон-фикшн, 2016. 310 с.

266. Минский М. Фреймы для представления знаний / пер. с англ. М.: Энергия, 1979. 150 с.

267. Минский М., Пейперт С. Перцептроны / пер. с англ. М.: Мир, 1971. 266 с.

268. Митакович С. А. Бюджетный квадрокоптер – богатые ГИС возможности // ГИС для управления инфраструктурой. 2020. № 1 (92). URL: <https://arcreview.esri-cis.ru/2020/04/30/uav-products-for-gis/> (дата обращения: 16.04.2025).

269. Митрофанов Д. Г., Злобинова М. В. Совершенствование процесса управления комплексом математических моделей в системах поддержки принятия решений реального времени // Тр. Военно-космической академии имени А. Ф. Можайского. 2014. № 645. С. 44–51.

270. Михайлов А. И., Черный А. И., Гиляревский Р. С. Основы информатики. М.: Наука, 1968. 756 с.

271. Многозначные логики и их применения. Том 1. Логические исчисления, алгебры и функциональные свойства. Изд. стереотип. / Аншаков О. М., Виноградов Д. В., Финн В. К. / под ред. В. К. Финна. М.: URSS, 2020. 502 с.

272. Многозначные логики и их применения. Том 2. Логики в системах искусственного интеллекта. М.: ЛКИ, URSS, 2008. 240 с.

273. Многозначные логики и их применения. Том 2: Логики в системах искусственного интеллекта. Изд. стереотип. / Аншаков О. М., Виноградов Д. В., Финн В. К. / под ред. В. К. Финна. М.: URSS, 2020. 228 с.

274. Моделирование обучения и поведения. М.: Наука, 1975. 236 с.

275. Моисеев Н. Н. Алгоритмы развития. Природа и общество как одно целое: в поисках единого процесса развития. Развитие интеллекта и эволюция живой материи. Искусственный интеллект и проблемы глобального характера. М.: URSS, 2021. 320 с.

276. Мыльников Л. А. Статистические методы интеллектуального анализа данных. СПб.: БХВ-Петербург, 2021. 240 с.

277. Наумов Р. С., Благодарящев И. В. Подходы к стратегическому планированию развития беспилотной авиации и беспилотного авиастроения // Техника воздушного флота. Вып. 2. 2023. С. 3–6.

278. Национальная технологическая инициатива // URL: <https://nti2035.ru/markets/aeronet> (дата обращения: 23.03.2025).

279. Нейман Дж. Вычислительная машина и мозг / пер. с англ. М.: URSS, 2023. 192 с.

280. Нейман Дж. Теория самовоспроизводящихся автоматов. Изд. 2-е / пер. с англ. М.: URSS, 2010. 384 с.

281. Немов Ф. Что противопоставить виртуальному злу // Полиция России. 2025. № 1. С. 12–15.
282. Нильсон Н. Искусственный интеллект. Методы поиска решений / пер. с англ. М.: Мир, 1973. 273 с.
283. Нильсон Н. Принципы искусственного интеллекта / пер. с англ. М.: Радио и связь, 1985. 376 с.
284. Овчинский А. С. Оперативно-розыскная деятельность и цифровая трансформация: от первых АИПС до ГИС «Посейдон» / Сб. науч. тр. «Оперативно-розыскная деятельность и современность» / под ред. В. С. Овчинского. М.: ИНФРА-М, 2022. 177 с.
285. Овчинский А. С., Борзунов К. К. Цифровые технологии в профилактике и раскрытии преступлений: учеб. пособие. М.: МосУ МВД России имени В. Я. Кикотя, 2022. 106 с.
286. Овчинский В. С., Маслов А. А., Бабушкин А. А. О перспективах использования технологий искусственного интеллекта в оперативно-розыскной деятельности органов внутренних дел: науч. доклад. М.: ВНИИ МВД России, 2020. 110 с.
287. Оперативно-розыскная деятельность в цифровом мире: сб. науч. тр. / под ред. В. С. Овчинского. М.: ИНФРА-М, 2021. 630 с.
288. Оперативно-розыскная деятельность и современность: сб. науч. тр. / под ред. В. С. Овчинского. М.: ИНФРА-М, 2022. 177 с.
289. Организационно-правовые основы технической защиты конфиденциальной информации: учеб. пособие / Ю. И. Синешук [и др.] / под общ. ред. Ю. И. Синешука. СПб.: СПбУ МВД России, 2023. 80 с.
290. Осипенко А. Л. Об участии органов внутренних дел в системе обеспечения кибербезопасности Российской Федерации // Общество и право. 2018. № 3 (65). С. 35–42.
291. Осипов Г. С. Лекции по искусственному интеллекту. 2-е изд., испр. и доп. М.: URSS, Либроком, 2013. 267 с.
292. Основные цели, задачи, этапы и технологии интеллектуализации комплексов бортового оборудования перспективных воздушных судов гражданской авиации / А. В. Дутов [и др.] // Техника воздушного флота. 2023. № 1. С. 11–20.
293. Основы государственного управления в сфере информатизации в Российской Федерации. М.: Юрист, 1997. 334 с.
294. Основы кибербезопасности в деятельности сотрудников правоохранительных органов: учеб. пособие / А. Н. Прокопенко и [др.]. Белгород: Белгородский юридический институт МВД России имени И. Д. Путилина, 2023. 153 с.
295. Основы кибербезопасности: учеб. пособие / С. В. Лемайкина и [др.]. Ростов н/Д.: РЮИ МВД России, 2023. 64 с.
296. Основы кибербезопасности: учеб. пособие / С. Ю. Кропачев [и др.]. Н. Новгород: Нижегородская академия МВД России, 2022. 133 с.

297. Основы кибербезопасности: учеб. / А. В. Бецков и [др.]. М.: Академия управления МВД России, 2023. 108 с.
298. Основы кибербезопасности: учеб. / В. А. Минаев [и др.]. Воронеж–Москва: ГУРЛС, 2024. 392 с.
299. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации: учеб.-метод. пособие / Э. Д. Нугаева [и др.]. Уфа: Уфимский ЮИ МВД России, 2023. 96 с.
300. Остроух А. В. Введение в искусственный интеллект: моногр. Красноярск: Научно-инновационный центр, 2020. 250 с.
301. От искусственного интеллекта к искусственной социальности: новые исследовательские проблемы современной социальной аналитики / А. В. Резаев [и др.] / под ред. А. В. Резаева. М.: ВЦИОМ, 2020. 255 с.
302. От моделей поведения к искусственному интеллекту / под ред. В. Г. Редько. Изд. стереотип. М.: URSS: ЛЕНАНД, 2016. 447 с.
303. Отчёт «Тестирование компонентов Системы обеспечения эксплуатации беспилотных авиационных систем (СОЭ БАС) специализированного программного обеспечения, вычислительного оборудования, систем радиолокации, позиционирования и связи БАС в ходе проведения проектно-образовательного интенсива «Архипелаг-2024». ООО «АэроЛинк», 2024. 206 с.
304. Охлупина А. Н., Федорович В. Ю. Возможности проведения исследовательской работы в области почерковедения с помощью интеллектуальной системы автоматизированной поддержки научных исследований // Теория и практика судебной экспертизы: международный опыт, проблемы, перспективы. М.: МосУ МВД России имени В. Я. Кикотя, 2019. С. 265–267.
305. Охлупина А. Н., Федорович В. Ю. Подготовка базы данных для проведения идентификационных почерковедческих исследований с применением ДСМ-метода автоматического порождения гипотез // Теория и практика судебной экспертизы: международный опыт, проблемы, перспективы. М.: МосУ МВД России имени В. Я. Кикотя, 2017. С. 573–576.
306. Оценка устойчивости функционирования критической информационной инфраструктуры / К. М. Бондарь [и др.] // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2018. № 4. С. 129–138.
307. Парк Ч, Чанг Х, Дефранко Д. Многоуровневая киберзащита для умного города // Открытые системы. СУБД. 2022. № 02: URL: <https://www.osp.ru/os/2022/02/13056210> (дата обращения: 30.04.2025).
308. Перспективы применения технологий искусственного интеллекта в авиастроении и авиатранспортных системах: информ.-аналит. обзор. Национальный исследовательский центр «Институт имени Н. Е. Жуковского» / под ред. А. В. Дутова [и др.]. М.: Вып. 2. 2022. 211 с.

309. Першиков В. И., Савинков В. М. Толковый словарь по информатике. 2-е изд., доп. М.: Финансы и статистика, 1995. 554 с.

310. Петров В. А., Пискарев А. С., Шеин А. В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах: учеб. пособие. Изд. 2-е, испр. и доп. М.: МИФИ, 1995. 84 с.

311. Петровский А. А. Новые зарубежные разработки в области искусственного интеллекта для оснащения правоохранительных органов: аналитический обзор. М.: ФКУ НПО «СТиС» МВД России, 2021. 24 с.

312. Петухов Г. Б., Якунин В. И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. М.: АСТ, 2006. 504 с.

313. Пешкова И. Кто и как использует технологии распознавания лиц в России // URL: <https://rb.ru/longread/facial-recognition/> (дата обращения: 30.12.2024).

314. Повышение эффективности функционирования сетей связи органов внутренних дел на основе перспективных информационных технологий: учеб. пособие / Н. С. Хохлов [и др.]. Воронеж: Воронежский институт МВД России, 2022. 142 с.

315. Поздняков А. Н. Интернет и его функции в виртуальном пространстве: оперативно-розыскной аспект // Сетевое издание «Академическая мысль». 2024. № 4(29). С. 47–53.

316. Поликарпов Е. С., Толстых А. А., Цимбал В. Н. Обобщенный анализ сайтов сбыта наркотических средств анонимного сегмента сети Интернет // Вестник МосУ МВД России имени В. Я. Кикотя. 2021. № 4. С. 174–178.

317. Поляков И. С. Современные возможности программного обеспечения поиска и анализа криминалистически значимой информации в информационно-телекоммуникационных сетях // Материалы II Междунар. науч.-практ. конф. «Проблемы противодействия киберпреступности» / под общ. ред. О. Ю. Антонова, Э. Б. Хатова. Москва, 26 апреля 2024 г. М.: Московская академия Следственного комитета имени А. Я. Сухарева, 2024. С. 68–73.

318. Попов А. Ю. Кибербезопасность и искусственный интеллект: как ИИ может помочь в обеспечении безопасности и какие риски он может создать? // URL: <https://cisoclub.ru/kiberbezopasnost-i-iskusstvennyj-intellekt-kak-ii-mozhet-pomoch-v-obespechenii-bezopasnosti-i-kakie-riski-on-mozhet-sozdat/> (дата обращения: 22.01.2025).

319. Попов Э. В. Общение с ЭВМ на естественном языке. М.: Наука, 1982. 360 с.

320. Попов Э. В., Фридман Г. Р. Алгоритмические основы интеллектуальных роботов и искусственного интеллекта. М.: Наука, 1976. 456 с.

321. Поспелов Г. С. Душа и сердце новейшей информационной технологии / Будущее науки. М., 1988. Вып. 21. С. 9–32.
322. Поспелов Г. С. Искусственный интеллект – основа новой информационной технологии. М.: Наука, 1988. 280 с.
323. Поспелов Г. С. О развитии проблем искусственного интеллекта // Вестник Академии наук СССР. М., 1988. № 10. С. 134–138.
324. Поспелов Г. С. Системный анализ и искусственный интеллект для планирования и управления // Кибернетика. 1984. С. 141–151.
325. Поспелов Г. С., Ириков В. А. Программно-целевое планирование и управление. 1976. 440 с.
326. Поспелов Г. С., Поспелов Д. А. Искусственный интеллект как научно-техническая проблема // Философия и социология науки и техники: Ежегодник, 1984–1985. М., 1986. С. 29–37.
327. Поспелов Д. А. Большие системы. Ситуационное управление. М.: Знание, 1975. 66 с.
328. Поспелов Д. А. Вероятностные автоматы. М.: Энергия, 1970. 88 с.
329. Поспелов Д. А. Десять «горячих точек» в исследованиях по искусственному интеллекту // Интеллектуальные системы (МГУ). 1996. Т. 1, вып. 1-4. С. 47–56.
330. Поспелов Д. А. Знания и шкалы в модели мира. Модели мира. М.: РАИИ, 1997. С.69–84.
331. Поспелов Д. А. Игры и автоматы. М.-Л.: Энергия, 1966. 136 с.
332. Поспелов Д. А. Интеллектуальные системы: ожидания и реальность // Природа. М., 1988. № 3. С. 58–73.
333. Поспелов Д. А. История искусственного интеллекта до середины 80-х годов // История информатики в России: Ученые и их школы. М., 2003. С. 407–429.
334. Поспелов Д. А. Многоагентные системы – настоящее и будущее // Информационные технологии и вычислительные системы. 1998. № 1. С. 14–21.
335. Поспелов Д. А. Модели мира и семиотическое моделирование / Модели мира. М., 1997. С. 5–7.
336. Поспелов Д. А. Моделирование рассуждений. Опыт анализа мыслительных актов. М.: Радио и связь, 1989. 184 с.
337. Поспелов Д. А. О задачах психоники // Вопросы бионики. М.: Наука, 1967. С. 294–297.
338. Поспелов Д. А. Решение задач оперативного управления с помощью системы моделей // Труды XVIII-го Международного психологического конгресса. Симпозиум 25. М., 1966. С.108–113.
339. Поспелов Д. А. Ситуационное управление: Теория и практика. М.: Наука, 1986. 288 с.
340. Поспелов Д. А. Теория гиоматов // Проблемы бионики. М.: Наука, 1973. С.397– 402.

341. Пospelов Д. А., Пушкин В. Н. Мышление и автоматы. М.: Советское Радио, 1972. 221 с.

342. Правовые основы информационной безопасности: учеб. пособие / К. М. Бондарь [и др.]. Хабаровск: ДВЮИ МВД России, 2006. 344 с.

343. Правовые основы обеспечения защиты информации / А. П. Фисун [и др.] / под ред. А. П. Фисуна. Орел: ВИПС, 1997. 131 с.

344. Прайс М. Дж. С#7 и .NET Core: кроссплатформенная разработка для профессионалов. 3-е изд. / пер. с англ. М. Сагалович, С. Черников. СПб.: Питер, 2019. 636 с.

345. Применение современных инфокоммуникационных технологий в управленческой деятельности органов внутренних дел: учеб.-практ. пособие / К. М. Бондарь [и др.]. Хабаровск: ДВЮИ МВД России, 2017. 180 с.

346. Применение современных инфокоммуникационных технологий в управлении деятельностью подразделений органов внутренних дел: учеб.-практ. пособие / К. М. Бондарь [и др.]. М.: ДГСК МВД России, 2018. 192 с.

347. Применение современных информационных технологий в аналитической деятельности органов внутренних дел: учеб.-практ. пособие / К. М. Бондарь [и др.]. Хабаровск: РИО ДВЮИ МВД России, 2021. 137 с.

348. Проблемы автоматизации индексирования и реферирования / Н. А. Пашенко [и др.] // Итоги науки и техники. Сер. Информатика. М.: ВИНТИ, 1983. Т. 7. С. 7–164.

349. Проблемы борьбы с преступностью в условиях цифровизации // Сб. ст. XIX Междунар. науч.-практ. конф. «Уголовно-процессуальные и криминалистические чтения на Алтае», посвященной памяти Вениамина Константиновича Гавло. Вып. XVII / отв. ред. С. И. Давыдов, В. В. Поляков. Барнаул: Изд-во Алтайского университета, 2021. 500 с.

350. Проблемы информационного обеспечения деятельности правоохранительных органов // Сб. ст. 10-й Всерос. науч.-практ. конф. 19 мая 2023 г. Белгород: Белгородский юридический институт МВД России имени И. Д. Путилина, 2023. 205 с.

351. Проблемы информационного обеспечения деятельности правоохранительных органов // Сб. ст. 11-й Всерос. науч.-практ. конф. 24 мая 2024 года. Белгород: Белгородский юридический институт МВД России имени И. Д. Путилина, 2024. 245 с.

352. Проблемы противодействия киберпреступности // Материалы II Междунар. науч.-практ. конф. / под общ. ред. О. Ю. Антонова, Э. Б. Хатова. Москва, 26 апреля 2024 года. М.: Московская академия Следственного комитета имени А. Я. Сухарева, 2024. 146 с.

353. Противодействие преступлениям, совершаемым с использованием современных информационно-телекоммуникационных тех-

нологий: отдельные аспекты: учеб. пособие / В. Р. Гурьянова [и др.]. Уфа: Уфимский юридический институт МВД России, 2023. 48 с.

354. Противодействие экстремистской идеологии в социальных медиа: математические модели и методы: моногр. / В. А. Минаев, К. М. Бондарь, А. Н. Рабчевский, В. Ю. Федорович; под ред. В. А. Минаева, К. М. Бондаря. Хабаровск: РИО ДВЮИ МВД России, 2023. 232 с.

355. Путин объявил о создании в России нового рода войск беспилотных систем // URL: <https://rg.ru/2025/06/16/drony-na-sluzhbe.html> (дата обращения: 17.06.2025).

356. Путин поручил улучшить использование ИИ для расследования преступлений // URL: <https://www.rbc.ru/rbcfreenews/65a7a3359a794761a6913056> (дата обращения: 09.04.2025).

357. Рассолов М. М. Информационное право: учеб. пособие. М.: Юрист, 1999. 400 с.

358. Расторопов С. В., Прорвич В. А. Информационные основы современной уголовно-правовой защиты субъектов цифровой экономики и финансов // Право. Журнал Высшей школы экономики. 2024. Том 17. № 2. С. 143–169.

359. Расширенное заседание коллегии МВД России // URL: <http://www.kremlin.ru/events/president/news/76408> (дата обращения: 15.03.2025).

360. Рафгарден Т. Совершенный алгоритм. Алгоритмы для NP-трудных задач / пер. с англ. А. Логунова. СПб.: Питер, 2021. 300 с.

361. Рафгарден Т. Совершенный алгоритм. Жадные алгоритмы и динамическое программирование / пер. с англ. А. Логунова. СПб.: Питер, 2020. 255 с.

362. Рафгарден Т. Совершенный алгоритм. Основы / пер. с англ. А. Логунова. СПб.: Питер, 2019. 253 с.

363. Риски топливно-энергетического комплекса России: современные угрозы и управление: моногр. / В. А. Минаев [и др.]. М., 2025. 230 с.

364. Робот-полицейский. Как искусственный интеллект помогает в расследованиях преступлений // URL: <https://novayagazeta.eu/articles/2024/02/05/robot-politseiskii> (дата обращения: 09.04.2025).

365. Розенблатт Ф. Принципы нейродинамики / пер. с англ. М.: Мир, 1965. 480 с.

366. Российский разработчик «Элемент» будет выпускать радио модули для сетей 5G // URL: <https://3dnews.ru/1106699/rossiyskiy-razrabotchik-element-nachinaet-proizvodstvo-radiomoduley-dlya-setey-5g> (дата обращения: 03.05.2025).

367. Русецкий О. В. Система профилактики преступлений в информационном пространстве // Криминалист. 2024. № 2 (47). С. 113–120.

368. Свидетельство о государственной регистрации программы для ЭВМ № 2016619597 Российская Федерация. Инструментальный

комплект средств интеграции: № 2016616671: заявл. 22.06.2016: опубл. 24.08.2016 / А. В. Астрахов, Л. С. Куликов; заявитель Общество с ограниченной ответственностью «Лаборатория инновационных технологий» при МГТУ имени Н. Э. Баумана».

369. Свидетельство о государственной регистрации программы для ЭВМ № 2021617353 Российская Федерация. Программа контроля и индикации состояния бортового радиоэлектронного оборудования и бортовых информационных систем: № 2021616225: заявл. 26.04.2021: опубл. 13.05.2021 / Р. С. Быков [и др.]; заявитель Публичное акционерное общество «Авиационный комплекс имени С. В. Ильюшина».

370. Свидетельство о государственной регистрации программы для ЭВМ № 2024669798 Российская Федерация. Сервис создания и проверки сертификатов безопасности беспилотного транспорта: № 2024660147: заявл. 03.05.2024: опубл. 21.08.2024 / Р. С. Быков, А. К. Пахомов, А. С. Толпыгин.

371. Самданов Г. Б., Голиков Д. В. К вопросу об использовании беспилотных летательных аппаратов в современной криминалистике // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 378–384.

372. Севбо И. П. Структура связного текста и автоматизации реферирования. М.: Наука, 1969. 132 с.

373. Синтез цифровых двойников с применением многоаспектной рекурсивной декомпозиции / В. А. Минаев [и др.] // Вопросы радиоэлектроники. 2019. № 11. С. 26–37.

374. Системно-динамическое моделирование сетевых информационных операций / К. М. Бондарь [и др.] // Инженерные технологии и системы. 2019. Т. 29. № 1. С. 20–39.

375. Слэйгл Дж. Искусственный интеллект / пер. с англ. М.: Мир, 1973. 320 с.

376. Смотри инженерных команд Центрального федерального округа (25.06.2024). 50 с.

377. Советов Б. Я., Яковлев С. А. Моделирование систем. М.: Высш. шк., 1998. 319 с.

378. Соколова А. В. Цифровизация судебно-баллистической экспертизы: генезис и перспективы // Криминалистика наука без границ. Традиции и новации: материалы междунар. науч.-практ. конф. СПб., 2024. С. 520–523.

379. Соловьев Д. Кибербезопасность искусственного интеллекта: преимущества и риски // URL: <https://recoverit.wondershare.com.ru/windows-computer-tips/ai-cybersecurity.html> (дата обращения: 20.01.2025).

380. Специальная техника и информационная безопасность: учеб. / В. А. Минаев [и др.]. М.: Академия управления МВД России, 2000. Т. 1. 784 с.

381. Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам: учеб. пособие / Ю. И. Синешук [и др.] / под общ. ред. Ю. И. Синешука. СПб.: СПбУ МВД России, 2023. 184 с.

382. Спрингер В. Гид по Computer Science: для каждого программиста / пер. с англ. А. Павлова. СПб.: Питер, 2022. 304 с.

383. Становление и развитие системы правительственной связи в России (опыт исторического исследования) / В. И. Астрахан [и др.] / под. ред. В. В. Гусева. Орел: ВИПС, 1996. 370 с.

384. Старостенко Н. И. Криминалистическое прогнозирование хищений, совершаемых с использованием «DeepFake»-технологий // Вестник Сибирского юридического института МВД России. 2023. № 2 (51). С. 187–192.

385. Статические и динамические экспертные системы: учеб. пособие / Э. В. Попов [и др.]. М.: Финансы и статистика, 1996. 320 с.

386. Суходолов А. П., Бычкова А. М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 753–766.

387. Студитский А. С., Кекин А. Г. Повышение эффективности интегрированных многоканальных наблюдательных систем // Приборы. 2013. № 9. С. 52–55.

388. Тарасов В. Б. Д. А. Поспелов – основоположник искусственного интеллекта в СССР и России» // URL: <http://www.prosp.raai.org/data/prosp2005/Tarasov/dap.html> (дата обращения: 28.01.2025).

389. Тарасов В. Б. Искусственный интеллект: наследие профессора Д. А. Поспелова. От психоники, прикладной семиотики и псевдофизических логик к синергетическому искусственному интеллекту // Мягкие измерения и вычисления: научный журнал. 2020. Т. 29. № 4. С. 28–44.

390. Тарасов В. Б. Искусственный интеллект: от прошлого к будущему. О жизненном пути и научном наследии профессора Д. А. Поспелова // URL: http://Tarasov_Iskusstvenniy.pdf (дата обращения: 29.01.2025).

391. Тарасов В. Б. От многоагентных систем к интеллектуальным организациям: философия, психология, информатика: моногр. М.: URSS, 2002. 348 с.

392. Тегмарк М. Жизнь 3.0. Быть человеком в эпоху искусственного интеллекта / пер. с англ. Д. Баюка. М.: АСТ, 2019. 552 с.

393. Телешина Н. Н. Виртуальное пространство как новая юридическая конструкция: к постановке проблемы // Юридическая техника. 2013. № 7. Ч. 2. С. 741–744.

394. Теоретические основы информатики и информационная безопасность: учеб. / под ред. В. А. Минаева, В. Н. Саблина. М.: Радио и связь, 2000. 468 с.
395. Теория и практика обеспечения информационной безопасности / Д. П. Зегжда [и др.]; под ред. Д. П. Зегжды. М.: Изд-во Агентства «Яхстмен», 1996. 192 с.
396. Теория информационно-компьютерного обеспечения криминалистической деятельности: моногр. / под ред. Е. Р. Россинской. М.: Проспект, 2022. 256 с.
397. Терроризм и экстремизм: моделирование информационного противодействия: монография / А. А. Андреев, К. М. Бондарь, В. А. Минаев; Дальневосточный юридический институт МВД России. Хабаровск: РИО ДВЮИ МВД России, 2020. 248 с.
398. Технологические основы кибербезопасности: учеб. пособие / К. М. Бондарь [и др.]. Хабаровск: РИО ДВЮИ МВД России, 2023. 142 с.
399. Толпыгин А. С. Информационная защита управления беспилотным транспортом: проблемы и решения // «Цифропол – 2025». М., С. 143–153.
400. Толпыгин А. С. Цифровая платформа информационной защиты беспилотного транспорта // Вестник Московского университета МВД России. 2024. № 2. С. 34–43.
401. Толпыгин А. С., Куликов Л. С., Пахомов А. К. Искусственный интеллект в цифровой полиции: возможности и перспективы // Сборник научных трудов Всероссийского семинара «Применение современных информационных и телекоммуникационных технологий в раскрытии и расследовании киберпреступлений» (Хабаровск, 25 июня 2025 г.). Хабаровск: РИО ДВЮИ МВД России имени И. Ф. Шилова, 2025. С. 112–119.
402. Толпыгин А. С., Пахомов А. К. Модель киберустойчивости и управляемости флота беспилотных транспортных средств // Материалы II науч.-практ. конф. «Актуальные проблемы защиты информации: современность и перспективы. Москва, 9–10 апреля 2024 года. М.: МГТУ имени Н. Э. Баумана, 2025. С. 61–70.
403. Томас И. С., Ван Ж. Искусственный интеллект отвечает на величайшие вопросы человечества. Что делает нас людьми? / пер. с англ. М. А. Леоновича. М.: АСТ, 2023. 240 с.
404. Торопов Б. А. Моделирование ситуации информационного противодействия деструктивным влияниям в социальных сетях по резонансным общественно-политическим вопросам: моногр. М.: Академия управления МВД России, 2022. 104 с.
405. Тыгу Э. Х. Концептуальное программирование. М.: Наука, 1984. 256 с.
406. Тьюринг А. Вычислительные машины и разум / пер. с англ. К. Королева. М.: АСТ, 2018. 125 с.

407. Тьюринг А., фон Нейман Дж. Может ли машина мыслить? Общая и логическая теория автоматов / пер. с англ. 3-е изд., испр. и доп. М.: URSS, 2025. 232 с.
408. Уинстон П. Искусственный интеллект / пер. с англ. М.: Мир, 1980. 520 с.
409. Уотерман Д. Руководство по экспертным системам / пер. с англ. / под ред. В. Л. Стефанюка. М.: Мир, 1989. 388 с.
410. Фальков Э. Я. Систематика авиационных киберугроз и методов защиты от них: существующие и возможные пути решения // Навигация, наведение и управление летательными аппаратами: сб. тезисов докладов. М., 2017. С. 220–221.
411. Фальков Э. Я., Татарчук И. А., Егоров В. В. Имитационное моделирование системы определения взаимных координат между летательными аппаратами в режиме VDL 4 АЗН-В // Авиационные системы в XXI веке: сб. тезисов докладов. М., 2016. С. 275.
412. Федорович В. Ю. К вопросу о технико-криминалистическом обеспечении предупреждения преступлений / Техничко-криминалистическое обеспечение раскрытия и расследования преступлений: науч. электрон. издание. М.: МосУ МВД России имени В. Я. Кикотя, 2020. С. 11–13.
413. Федорович В. Ю. О становлении частной теории экспертной профилактики в свете научных трудов профессора Р. С. Белкина (посвящается 100-летию со дня рождения Р. С. Белкина) // Научный портал МВД России, 2022. № 3. С. 130–133.
414. Федорович В. Ю. Организационные и научно-технические основы использования автоматизированных дактилоскопических идентификационных систем в раскрытии и расследовании преступлений: автореф. дис. ... канд. юрид. наук. М., 2000. 24 с.
415. Федорович В. Ю. Реализация профилактической функции в информационных системах криминалистического назначения // Вестник МосУ МВД России, 2020. № 8. С. 185–188.
416. Федорович В. Ю. Современный взгляд на понятие сущность преступления // Актуальные проблемы учения о преступлении. Омск: Омская Академия МВД России, 2020. С. 145–149.
417. Федорович В. Ю. Технологии искусственного интеллекта в решении экспертно-профилактических задач // Сб. тр. Междунар. науч.-практ. конф. «Информатизация и информационная безопасность правоохранительных органов» / под общ. ред. А. В. Бецкова [и др.]. М.: Академия управления МВД России, 2025. С. 397–402.
418. Ферлитш Э. Шаблоны и практика глубокого обучения / пер. с англ. А. В. Логунов. М.: ДМК Пресс, 2022. 537 с.
419. Филиппов Д. Чтобы киберобман стал невозможным // Полиция России. 2025. № 1. С. 16–19.

420. Философские проблемы искусственного интеллекта: библиографический указатель / сост. А. В. Гасилин, Н. С. Скипин; отв. ред.: А. В. Гасилин. М.: ИНИОН РАН, 2023. 207 с.
421. Финн В. К. Интеллектуальные системы и общество. М.: URSS, 2006. 351 с.
422. Финн В. К. Искусственный интеллект. Методология, применения, философия. М.: Ленанд, 2023. 468 с.
423. Финн В. К. Применение интеллектуальных систем в изучении общества. М.: Ленанд, 2020. 352 с.
424. Финн В. К. Что суперкомпьютер когда-нибудь превзойдет человека – это сказки // URL: <https://www.rsuh.ru/news/detail.php?ID=265521> (дата обращения: 26.01.2025).
425. Финн В. К., Аншаков О. М. ДСМ-метод автоматического порождения гипотез: логические и эпистемологические основания / под ред. В. К. Финна. М.: URSS, 2009. 432 с.
426. Финн В. К. Автоматическое порождение гипотез в интеллектуальных системах. М.: Либроком, 2019. 528 с.
427. Финн В. К. Интеллект, информационное общество, гуманитарное знание и образование. М.: ЛЕНАНД, 2020. 464 с.
428. Фисун А. П. Информатика. Ч. 1. Информация и информационные системы, как объект обеспечения информационной безопасности: курс лекций. Орел: ВИПС, 1998. 274 с.
429. Фисун А. П., Касилов А. Н., Мешков А. Г. Информатика и информационная безопасность: учеб. пособие. Орел: ОГУ, 1999. 282 с.
430. Фокина А. И., Туровец Ю. В. ИИ для кибербезопасности: тренды и востребованность // Искусственный интеллект. Серия информационно-аналитических материалов ИСИЭЗ НИУ ВШЭ. 2024. № 7. 3 с.
431. Фомичева С. Г. Методы машинного обучения в задачах обеспечения информационной безопасности: учебное пособие. СПб: ГУАП, 2023. 135 с.
432. Форд М. Роботы наступают: Развитие технологий и будущее без работы / пер. с англ. С. Чернина. М.: Альпина нон-фикшн, 2016. 430 с.
433. Фрай Х. Hello world. Как быть человеком в эпоху машин / пер. с англ. Ю. Плискиной. М.: АСТ: CORPUS, 2021. 317 с.
434. Франсуа Ш. Глубокое обучение на Python / пер. с англ. А. Киселева. СПб: Питер, 2020. 397 с.
435. Франсуа Ш. Глубокое обучение на R / пер. с англ. А. Киселева. СПб: Питер, 2018. 399 с.
436. Хакеры слили 16 млрд паролей аккаунтов Apple, Google и других сервисов // URL: https://hi-tech.mail.ru/news/129002-hakery-slili-16-mlrd-parolej-akkauntov-apple-google-i-drugih-kompanij/-?frommail=ft_ml&mt_sub3=307 (дата обращения: 20.06.2025).
437. Хант Э. Искусственный интеллект / пер. с англ. М.: Мир, 1978. 558 с.

438. Хант Э., Мартин Дж., Стоун Ф. Моделирование процесса формирования понятий на вычислительной машине / пер. с англ. М.: Мир, 1970. 302 с.
439. Харрис Ш. Кибервойна. Пятый театр военных действий. М.: Альпина нон-фикшн, 2016. 390 с.
440. Химено-Сеговиа М., Хэрриган Н., Джонстон Э. Программирование квантовых компьютеров: базовые алгоритмы и примеры кода / пер. с англ. Е. Матвеева. СПб.: Питер, 2021. 334 с.
441. Хоффман Л. Дж. Современные методы защиты информации / пер. с англ. М.: Советское радио, 1980. 264 с.
442. Цигичко В. Н., Смолян Г. Л., Черешкин Д. С. Оценка систем информационной безопасности: препринт. М.: ИСА РАН, 1995. 43 с.
443. Цымбал В. П. Теория информации и кодирование. Киев: ВШ, 1982. 304 с.
444. Чанышев О. Г. Введение в искусственный интеллект. Ч. 1. От психофизиологической проблемы до экспертных систем. Лекция 1. Введение в предметную область ИИ. <https://yandex.ru/search/?text=deadbeef.narod.ru%2Fwork/docs/ai/01.pdf> (дата обращения: 25.01.2025).
445. Чанышев О. Г. Онтологические основания искусственного интеллекта: учеб. пособие. Омск: ОмГУ, 2004. 47 с.
446. Чень Ч., Ли Р. Математическая логика и автоматическое доказательство теорем / пер. с англ. М.: Наука, 1983. 360 с.
447. Черешнев Е. Форма жизни № 4: как остаться человеком в эпоху расцвета искусственного интеллекта. М.: Альпина, 2022. 482 с.
448. Число IT-преступлений в 2024 году достигло рекордных значений // URL: <https://expert.ru/news/chislo-it-prestupleniy-v-2024-godu-dostiglo-v-rossii-rekordnykh-765-4-tys/> (дата обращения: 15.02.2025).
449. Что такое ИИ для кибербезопасности? // URL: <https://www.microsoft.com/ru-ru/security/business/security-101/what-is-ai-for-cybersecurity> (дата обращения: 20.01.2025).
450. Что такое киберпреступность? Защита от киберпреступности // URL: <https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime?ysclid=lutxa8a3wi453780484> (дата обращения: 04.02.2025).
451. Шамис А. Л. Поведение, восприятие, мышление: проблемы создания искусственного интеллекта. М.: Едиториал URSS, 2005. 224 с.
452. Шанахан М. Технологическая сингулярность / пер. с англ. А. Врублевского. М.: Точка, 2017. 225 с.
453. Шваб К., Дэвис Н. Технологии Четвертой промышленной революции / пер. с англ. М.: Бомбора, 2022. 320 с.
454. Шенк Р. Обработка концептуальной информации / пер. с англ. М.: Энергия, 1980. 360 с.
455. Шеннон К. Работы по теории информации и кибернетике / пер. с англ. М.: Изд-во иностранной литературы, 1963. 829 с.

456. Шмидт Э, Коэн Дж. Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств / пер. с англ. М.: Манн, Иванов и Фербер, 2016. 387 с.
457. ЭВМ пятого поколения. Концепции, проблемы, перспективы. М.: Финансы и статистика, 1984. 110 с.
458. Эндрю А. Искусственный интеллект / пер. с англ. В. Л. Стефанюка; под ред. Д. А. Поспелова. М.: Мир, 1985. 265 с.
459. Этические последствия использования искусственного интеллекта в предиктивной полицейской деятельности // URL: <https://falconediting.com/ru/blog/eticheskie-posledstviia-ispolzovaniia-iskusstvennogo-intellekta-v-prediktivnoi-politseiskoi-deiatelnosti> (дата обращения: 05.04.2025).
460. Эшби У. Р. Введение в кибернетику / пер. с англ. Изд. стереотип. М.: URSS, 2023. 432 с.
461. Яковлев В. А. Защита информации на основе кодового зашумления / под ред. В. И. Коржака. СПб.: ВАС, 1993. 245 с.
462. Янин В. Л. Актовые печати древней Руси X–XV вв.: в 2 т. М.: Наука, 1970. АН СССР. Отделение истории. Т. 1. Печати X – начала XIII в. 326 с. Т. 2. Новгородские печати XIII–XV вв. 366 с.
463. Ярочкин В. И. Безопасность информационных систем. М.: «Ось-89», 1996. 320 с.
464. Ясницкий Л. Н. Введение в искусственный интеллект. М.: Академия, 2010. 176 с.
465. Autotelic agents with intrinsically motivated goal-conditioned reinforcement learning: a short survey / Colas C., Karch T., Sigaud O., and Oudeyer P.-Y. // Journal of Artificial Intelligence Research, 74. 2022. Pp.1159–1199.
466. Berry J., Stoney D. A. History and Development of Fingerprinting. In Advances in Fingerprint Technology, 2nd ed.; Lee, H. C., Gaensslen, R. E., Eds.; CRC Press: Boca Raton, FL, 2001; pp 1–40.
467. Bloomfield B. Expert systems and human knowledge: A view from the sociology // AI@Society. 1988. V. 2. № 1. Pp. 15–29.
468. Franke H. Computer Graphics – Computer Art. – Berlin, Heidelberg, New-York, Tokyo: Springer Verlag, 1985. 177 p.
469. Goertzel B., Pennachin C. (Eds.). Artificial General Intelligence. 2007. 509 p.
470. Helbig H. Knowledge Representation and the Semantics of Natural Language. 2006. 646 p.
471. Hewitt C. Viewing Control Structures as Patterns of Message Passing // Artificial Intelligence. 1977. Vol. 8, № 3. Pp. 323–364.
472. Hoffman A. G. On the Principles of Intelligence. Proceedings of the First World Conference on the Fundamentals for Artificial Intelligence (Paris, France, July 1-5, 1991). Paris: Masson, 1991. Pp. 257–266.

473. Human-timescale adaptation in an open-ended task space / Proceedings of the 40th International Conference on Machine Learning. Vol. 202. 2023. Pp. 1887–1935.
474. Lloyd J. W. Logic for Learning. Learning Comprehensive Theories from Structured Data. 2003. 256 p.
475. Machine Intelligence. Vol. 9. Ed. by J. E. Hayes, D. Michie, L. Mikulich. Chichester: Ellis Horwood Limited, 1979. 489 p.
476. Manoonpong P. Neural Preprocessing and Control of Reactive Walking Machines. Towards Versatile Artificial Perception-Action Systems. Berlin; New York. 2007. 185 p.
477. McCarthy J. From Here to Human-Level AI. Artificial Intelligence, vol. 171. 2007. Pp.1174–1182.
478. McCarthy J., Hayes P. J. Some Philosophical Problems from the Standpoint of Artificial Intelligence. Machine Intelligence. Vol 4. Ed. by B. Meltzer and D. Michie. Edinburgh: Edinburgh University Press, 1969, Pp. 463–502.
479. Namiot D., Ilyushin E., Chizov I. Artificial intelligence and cybersecurity // International Journal of Open Information Technologies. 2022. Vol. 10. № 9. Pp. 135–144.
480. Newell A. The knowledge level // Artificial Intelligence. 1982. V. 18. № 1. Pp. 87–127.
481. Nugues P. M. An Introduction to Language Processing with Perl and Prolog. An Outline of Theories, Implementation, and Application with Special Consideration of English, French, and German. 2006. 513 p.
482. Open Problems in Cooperative AI / Dafoe A., Hughes E., Bachrach Y., Collins T., McKee K. R., Leibo J. Z., Larson K., and Graepel T., Dec. 2020. URL: <https://arxiv.org/abs/2012.08630> (дата обращения: 10.01.2025).
483. Open-Endedness is Essential for Artificial Superhuman Intelligence / Hughes E., Dennis M., Parker-Holder J., Behbahani F., Mavalankar A., Shi Y., Schaul T., Rocktäschel T. Proceedings of the 41st International Conference on Machine Learning, Vienna, Austria. 2024. 20 p.
484. Pal S. K., Polkowski L., Skowron A. (Eds.). Rough-Neural Computing. Techniques for Computing with Words. 2004. 734 p.
485. Prendinger H., Ishizuka M. (Eds.). Life-Like Characters. Tools, Affective Functions, and Applications. 2004. 477 p.
486. Pupillo L. Artificial Intelligence and Cybersecurity Technology, Governance and Policy Challenges Final Report of a CEPS Task Force / L. Pupillo, S. Fantin, A. Ferreira, C. Polito. Centre for European Policy Studies (CEPS). Brussels. 2021. 122 p.
487. Reggia J. The Rise of Machine Consciousness: Studying Consciousness with Computational Models. Neural Networks. 2013. Vol. 44. Pp. 112–131.
488. Simon H.A. Artificial Intelligence: an Empirical Science. Artificial Intelligence, vol.77, 1995, pp. 95–127.

489. Stanley K. Open-Endedness: a New Grand Challenge for AI. O'Reilly Artificial Intelligence Conference. 2019.
490. Stock O., Zancanaro M. (Eds.). PEACH – Intelligent Interfaces for Museum Visits. 2007. 316 p.
491. Szymkowski M., Saeed K. Fingerprint feature extraction with artificial neural network and image processing methods // Advances in Soft and Hard Computing. Springer International Publishing, 2019. Pp. 86–97.
492. The fingerprint sourcebook // URL: https://crime-scene-investigator.net/PDF/fingerprint_sourcebook.pdf (дата обращения: 03.10.2024).
493. Torra V., Narukawa Y. Modeling Decisions: Information Fusion and Aggregation Operators. 2007. 284 p.
494. Video generation models as world simulators // URL: <https://openai.com/research/video-generation-models-as-world-simulators> (дата обращения: 10.01.2025).
495. Vision-language models as a source of rewards. Baumli K., Baveja S., Behbahani F., Chan H., Comanici G., Flennerhag S., Gazeau M., Holsheimer K., Horgan D., Laskin M., et al. ArXiv preprint, abs/2312.09187, 2023 // URL: <https://arxiv.org/abs/2312.09187> (дата обращения: 10.01.2025).
496. Wahlster W. (Ed.) SmartKom: Foundations of Multimodal Dialogue Systems. 2006. 644 p.
497. Wang P. Cognitive Logic vs Mathematical Logic. Lecture Notes of the 3rd International Seminar on Logic and Cognition, Guangzhou, China. 2004. 10 p.
498. Wang P., Goertzel B. Theoretical Foundations of Artificial General Intelligence. Beijing: Atlantis Press. 2012. 331 p.
499. Wilson D. C. Cybersecurity. The MIT Press, 2021. 160 p.
500. Xiang-Xin Z., Chun-Ge L. The Historical Application of Hand Prints in Chinese Litigation. J. Forensic Ident. 1988. 38 (6). Pp. 277–284.
501. Yampolskiy R. V., Spellchecker M. S. Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures // Computer Engineering and Computer Science. URL: https://www.researchgate.net/publication/309424933_Artificial_Intelligence_Safety_and_Cybersecurity_a_Timeline_of_AI_Failures (дата обращения: 20.01.2025).

Научное издание

Минаев Владимир Александрович, д-р техн. наук, проф.;

Бондарь Константин Михайлович, канд. техн. наук, доц.;

Дунин Вадим Сергеевич, канд. техн. наук;

Толпыгин Алексей Сергеевич, канд. техн. наук;

Федорович Василий Юрьевич, канд. юрид. наук, доц.

**Искусственный интеллект:
противодействие киберпреступности**

Дизайн обложки: *И. В. Минаева*

Подписано в печать 20.10.2025.

Формат 60 × 84 ¹/₁₆. Усл. печ. л. 14,8.

Тираж 500 экз. (1-й завод – 1–70 экз.). Заказ № 42.

Дальневосточный юридический институт МВД России
имени И. Ф. Шилова. Редакционно-издательский отдел. Типография.
680020, г. Хабаровск, пер. Казарменный, 15.