

**БЕЛГОРОДСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ
ИМЕНИ И.Д. ПУТИЛИНА**

**ОСНОВЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И КИБЕРБЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТИ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Учебно-методическое пособие

**Белгород
Белгородский юридический институт МВД России имени И.Д. Путилина
2026**

УДК 004:351.74
ББК 32.97
О 75

Печатается по решению
редакционно-издательского совета
Бел ЮИ МВД России
имени И.Д. Путилина

Авторы: Акапьев В.Л., канд. пед. наук; **Ковалева Е.Г.,** канд. техн. наук; **Борисенко А.В.,** канд. физ.-мат. наук; **Федосеев А.Э.,** канд. физ.-мат. наук; **Панарин В.В.**

О 75 Основы информационных технологий и кибербезопасности в деятельности органов внутренних дел Российской Федерации : учебно-методическое пособие / В. Л. Акапьев, Е. Г. Ковалева, А. В. Борисенко [и др.]. – Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2026. – 88 с.
ISBN 978-5-91776-669-0

Рецензенты:

Матросова Л.Д., кандидат юридических наук, доцент (Орловский юридический институт МВД России имени В.В. Лукьянова);

Дубинина Н.М., кандидат юридических наук, доцент (Московский университет МВД России имени В.Я. Кикотя).

В учебно-методическом пособии содержатся дидактические элементы, методическое сопровождение процесса формирования информационно-технологической компетентности сотрудников правоохранительных органов, элементы обратной связи и рефлексии.

На сегодняшний день общество переживает колоссальный рывок в развитии квантовых технологий, методов сбора и анализа больших данных, нейросетей и искусственного интеллекта. Необходимо понимать, что внедрять и разрабатывать информационные технологии в правоохранительной деятельности следует постепенно, с соблюдением всех мер информационной и технической безопасности, так как существуют значительные риски потерять контроль над разрабатываемыми техническими решениями и допустить необратимые критические ошибки.

Пособие способствует формированию информационно-технологической компетентности у обучающихся, способности осуществлять профессиональную деятельность с использованием современных информационных технологий в условиях обязательного соблюдения мер обеспечения кибербезопасности; содействует формированию знаний, умений, навыков и путей их реализации в области современных информационных технологий как составного элемента профессиональной компетентности.

Предназначено для курсантов, слушателей, профессорско-преподавательского состава образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации.

УДК 004:351.74
ББК 32.97

ISBN 978-5-91776-669-0

© Белгородский юридический институт
МВД России имени И.Д. Путилина, 2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	5
1. ОПЕРАЦИОННЫЕ СИСТЕМЫ СЕМЕЙСТВ WINDOWS И UNIX	6
Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы	6
Основные понятия и термины	14
Вопросы и задания для оценки теоретических знаний	14
2. ОБРАБОТКА ТЕКСТОВОЙ, ТАБЛИЧНОЙ И ГРАФИЧЕСКОЙ ИНФОРМАЦИИ	15
Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы	15
Основные понятия и термины	28
Вопросы и задания для оценки теоретических знаний	28
3. НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ	29
Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы	29
Основные понятия и термины	32
Вопросы и задания для оценки теоретических знаний	34
4. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ	35
Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы	35
Основные понятия и термины	44
Вопросы и задания для оценки теоретических знаний	44
5. ПОНЯТИЕ ОБ ИСТОЧНИКАХ И КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ	45
Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы	45
Основные понятия и термины	49
Вопросы и задания для оценки теоретических знаний	50
6. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ	51
Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы	51
Основные понятия и термины	57
Вопросы и задания для оценки теоретических знаний	58

7. ОСОБЕННОСТИ ОБРАЗОВАНИЯ СЛЕДОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ	59
Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы	59
Основные понятия и термины	71
Вопросы и задания для оценки теоретических знаний	71
8. ОСОБЕННОСТИ ФИКСАЦИИ СЛЕДОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ	72
Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы	72
Основные понятия и термины	82
Вопросы и задания для оценки теоретических знаний	82
ЗАКЛЮЧЕНИЕ	83
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	84

ВВЕДЕНИЕ

Роль информационных технологий в предотвращении и выявлении преступлений невозможно переоценить. Благодаря таким инструментам, как предиктивная аналитика и передовые системы наблюдения, правоохранные органы могут выявлять потенциальную преступную деятельность до того, как она произойдет, что позволяет принимать упреждающие меры. Более того, такие технологии, как распознавание лиц и автоматизированные считыватели номерных знаков, значительно ускоряют отслеживание и задержание подозреваемых.

Технологические инновации значительно упрощают административные процессы в правоохранительных органах. Автоматизированные системы для составления отчетов, ведения документации и отслеживания дел повышают эффективность работы, позволяя сотрудникам правоохранительных органов большую часть служебного времени ориентировать на борьбу с преступностью, а не заниматься бумажной работой. Такая оптимизация процессов снижает количество человеческих ошибок и повышает скорость реагирования на противоправную деятельность.

Информационные технологии также играют ключевую роль в обучении и профессиональном развитии сотрудников правоохранительных органов. Виртуальная реальность и передовые технологии моделирования создают реалистичную и захватывающую среду для обучения, которая помогает сотрудникам развивать навыки, необходимые в сложных ситуациях, без реальных рисков.

Правоохранительным органам следует своевременно адаптироваться к изменяющимся условиям, формируемым технологическими процессами информатизации решаемых ими задач, что невозможно без наличия сформированной информационно-технологической компетентности сотрудников органов внутренних дел.

1. ОПЕРАЦИОННЫЕ СИСТЕМЫ СЕМЕЙСТВ WINDOWS И UNIX

Вопросы для самостоятельного изучения

- 1.1. Понятие и эволюция операционных систем.
- 1.2. Работа с интерфейсом ОС Astra Linux и ОС Windows.

Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы

При рассмотрении **первого вопроса** необходимо уяснить понятие операционной системы, определить функции ОС, проследить эволюцию развития операционных систем.

Первая популярная ОС была из семейства *Windows*. Вышедшая в 1995 году версия отличалась узнаваемым интерфейсом и облегчала работу пользователей. Раньше для работы с ПК им было нужно знать набор команд. *Windows 95* предполагала работу с мышью, обеспечивала легкое взаимодействие с программами и сделала компьютеры доступными для большого количества новых пользователей. Сейчас *Windows* часто критикуют за активное расходование ресурсов компьютера или низкую стабильность работы, но при этом ОС считается наиболее популярной у пользователей ПК [23].

В ближайшие 10 лет *Windows* будет еще более тесно интегрирована с различными типами устройств, начиная от настольных компьютеров и ноутбуков и заканчивая мобильными устройствами и интернетом вещей. Пользовательский интерфейс будет еще более мобильным и адаптивным, а искусственный интеллект станет помощником, предлагающим персонализированные рекомендации на основе наших предпочтений и поведения [24].

Linux – это ОС, созданная на базе *Unix* и имеющая существенные отличия от *Windows*. Главное и ключевое – расположение системных файлов. В *Windows* каждая программа и приложение имеет свою папку, в которой находятся все файлы, отвечающие за их работу. *Linux* использует другую сортировку: файлы распределяются в зависимости от задачи, которую они выполняют. *Linux*, несомненно, продукт культуры *Unix*. *Unix* как набор операционных систем с общими свойствами возник задолго до появления настольных компьютеров. Он был разработан в середине 70-х гг., когда нормой в корпоративном мире было использование мини-компьютеров и мэйнфреймов.

В настоящее время *Unix* используется в корпоративной среде, а также нередко применяется в системах клиент-сервер. Исторический недостаток *Unix* – недоступность системы для программистов, работающих вне промышленных вычислительных центров. Именно указанная недоступность способствовала рождению *Linux* – широкодоступной операционной системы, аналогичной *Unix* [29].

Задание 1. Заполните таблицу 1.1. Особенности ОС семейства Windows и ОС семейства Unix.

Таблица 1.1. Особенности ОС семейства Windows и ОС семейства Unix

Операционная система	Достоинства ОС	Недостатки ОС
ОС семейства Windows		
ОС семейства Unix		

Задание 2. Приведите классификацию ОС и обозначьте основные перспективы их развития.

Задание 3. Перечислите основные функции операционной системы.

Любая операционная система имеет графическую оболочку для комфортного взаимодействия пользователя с техникой. Современные вычислительные системы состоят из процессоров, памяти, таймеров, дисков, сетевой коммуникационной аппаратуры, принтеров и других устройств [25]. Функцией ОС является распределение процессоров, памяти, устройств и данных между процессами, конкурирующими за эти ресурсы. ОС должна управлять всеми ресурсами вычислительной машины таким образом, чтобы обеспечить максимальную эффективность ее функционирования. Критерием эффективности может быть, например, пропускная способность или реактивность системы.

Задание 4. Заполните таблицу 1.2. Определите, разновидностью системного или прикладного программного обеспечения является каждый из приведенных ниже видов программного обеспечения (соедините стрелками).

Таблица 1.2. Системное и прикладное программное обеспечение

Системное программное обеспечение	Системы автоматизированного проектирования	Прикладное программное обеспечение
	Антивирусные программы	
	Архиваторы	
	Операционные системы	
	Мультимедиапроигрыватели	
	Системы управления базами данных	
	Бухгалтерские программы	
	Офисные пакеты	
	Операционные оболочки	
	Программы управления локальной сетью	
	Программы оптимизации диска	
	Текстовые процессоры	
	Табличные процессоры	

Архитектура ОС – это структурная и функциональная организация ОС на основе некоторой совокупности программных модулей [26]. Архитектура определяет принципы действия, информационные связи и взаимодействие основных компонентов ОС. Большинство современных ОС представляют собой хорошо структурированные модульные системы, способные к развитию, расширению и переносу на новые платформы.

Вся информация, размещаемая на компьютере, имеет некоторую структуру, цель которой состоит в обеспечении удобства в ориентации пользователя. Эта структура представляет собой упорядоченность дисков, папок (каталогов) и файлов. В качестве дисков выступают: гибкий диск, или дискета, жесткий диск, или винчестер (как правило, разделенный на несколько логических дисков), лазерный диск, съемные (флеш-носители) и сетевые диски. Вся информация, представляющая собой программы, документы, изображения и т.д., хранится на дисках в виде записей, которые называются файлами. Для различия одних файлов от других им присваиваются имена. В файлах хранятся программы и данные. Чтобы отличить тип данных (например, текст от графики), в структуре уникального имени файла различают две составляющие: собственно имя и расширение, указывающее на формат представления данных. Для поддержания порядка на дисках и удобства поиска нужных файлов предусмотрены папки или каталоги. Папка, так же как и файл, имеет уникальное имя и может содержать в своей структуре папки и файлы. Любая папка на компьютере имеет символьное

обозначение , которое следует различать с обозначениями других файлов (например, файлов архива  и файлов текстовых документов  и т.д.). Для работы с файлами и папками в операционной системе Windows используется ряд программ, среди них наибольшую популярность получила программа «Проводник».

В ходе раскрытия **второго вопроса** следует обратить особое внимание на основные принципы работы с ОС Windows. Определить особенности интерфейса данной ОС.

Astra Linux (Astra – звезда) – операционная система на базе ядра Linux, которая внедряется в России в качестве альтернативы Microsoft Windows в государственных организациях [38].

Во время загрузки операционной системы на экран выводятся диагностические сообщения – бегущие строки на черном фоне. По окончании загрузки системы на экран выводится приглашение к началу работы (см. рис. 1.1).

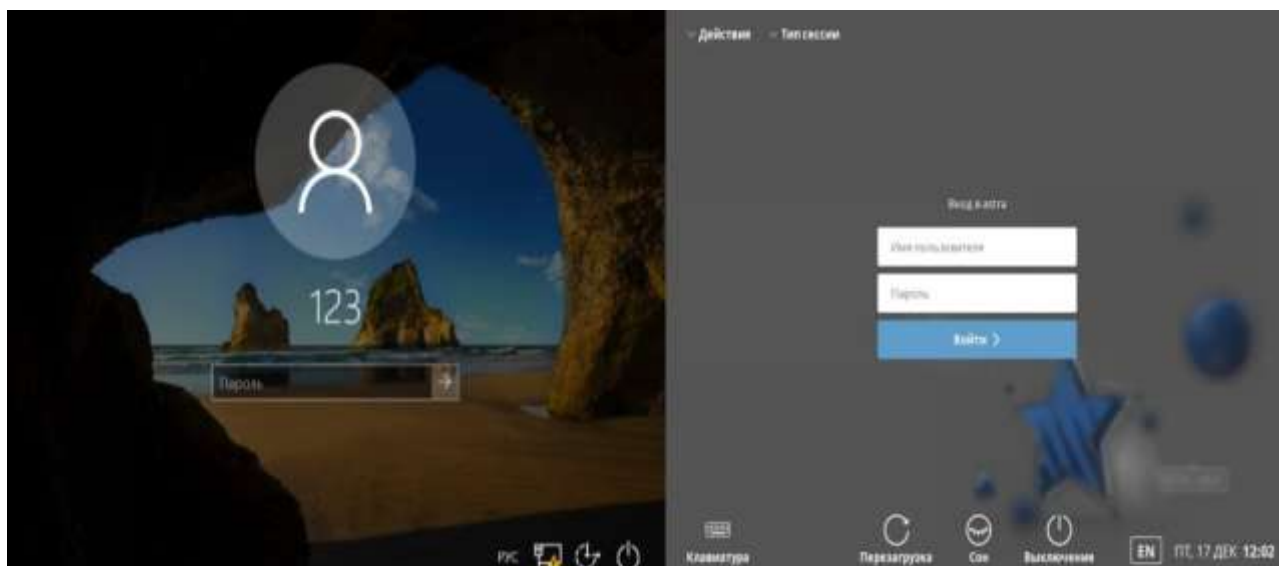


Рисунок 1.1. Окно входа в операционную систему

На этом этапе пользователь компьютера вводит свое имя, под которым он работает в системе, и пароль.

1. Astra Linux обладает интуитивно-понятными элементами управления и знакомым по Windows интерфейсом.

2. В ОС Astra Linux точно так же присутствуют:

- окно входа в систему;
- рабочий стол;
- кнопка «Пуск»;
- панель управления;
- файловый менеджер.

3. Форма входа в Astra Linux напоминает аналогичную в Windows. Также доступна экранная клавиатура, возможность выключить или перезагрузить компьютер, выбор раскладки. В Astra Linux существует две основные версии: Common Edition и Special Edition. Версия Common Edition предназначена для общего пользования, а Special Edition – для специализированного. В свою очередь, в ОС Astra Linux Special Edition существуют следующие модификации по уровню защищенности: Воронеж (усиленная) и Смоленск (максимальная) [36; 37].

4. После правильного ввода логина и пароля открывается рабочий стол Fly (см. рис. 1.2), на котором, как правило, присутствуют:

1) специальные папки «Мой компьютер» и «Корзина»;

2) в нижней части экрана находится панель задач (полоса со значками в самой нижней части экрана), в которой располагаются:

- меню «Пуск»;
- переключатель рабочих столов (если его активировали);
- значки для запуска менеджера файлов и браузера;
- значки с информацией о сети, заряде батареи, звуке, раскладке и текущем времени.

Задание 5. Изучите работу горячих клавиш.

Порядок выполнения задания:

ОС Windows:

Win + D – свернуть все окна.

Ctrl + C / Ctrl + V – копировать/вставить.

Alt + Tab – переключение между окнами.

Win + R – открыть окно «Выполнить».

ОС Linux:

Ctrl + Alt + T – открыть терминал.

Ctrl + C/Ctrl + V – копировать/вставить (в графическом интерфейсе).

Alt + Tab – переключение между окнами.

Ctrl + Alt + L – заблокировать экран.

5. При нажатии кнопки «Пуск» (см. рис. 1.2) на рабочем столе Fly (имеющей вид звезды в круге – логотипа Astra Linux) в операционной системе Astra Linux будет открыто меню «Пуск».

Примечание: аналогично в Windows, при нажатии кнопки «Пуск» (имеющей вид окошка – логотипа Windows) открывается меню «Пуск».

6. В панели «Пуск» присутствуют «Завершение работы», «Поиск», «Панель управления», раздел «Последние» с последними запущенными программами и папки-категории с установленным программным обеспечением: «Офис», «Сеть», «Графика», «Мультимедиа», «Утилиты», «Системные» и т.д.

Примечание: аналогично в Windows, она содержит кнопки выключения системы, параметры, профиль, ссылки на папки «Документы» и «Изображения» текущего пользователя, программы, сгруппированные по папкам-категориям.

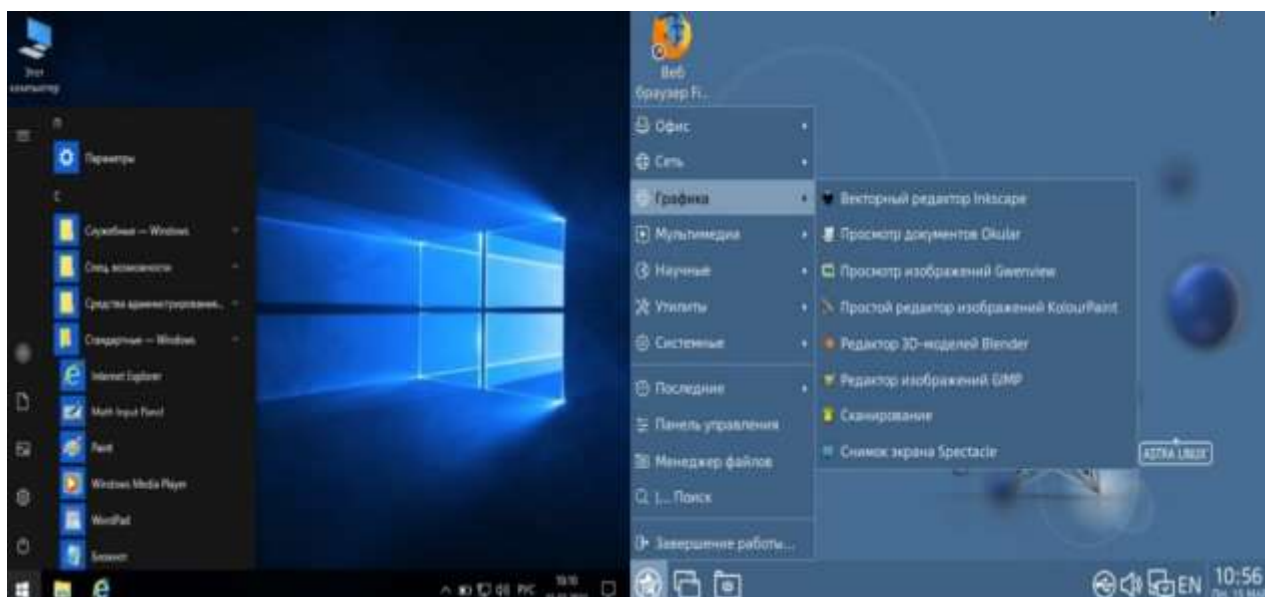


Рисунок 1.2. Меню «Пуск»

7. Аналогом «Проводника» в Windows в Astra Linux выступает «Менеджер файлов» (см. рис. 1.3). Точно так же, как и в Windows, в Astra Linux «Менеджер файлов» запускается по нажатию на панели задач значка «Менеджер файлов» или двойным щелчком по значку «Мой компьютер» на рабочем столе.

8. При открытии «Мой компьютер» в Astra Linux открывается «Менеджер файлов» с открытой специальной папкой «Мой компьютер», вид и назначение которой в целом совпадает с таковой же в Windows.

9. Папка «Мой компьютер» содержит:

- папку «Домашняя» (которая в Windows отображается сразу в развернутом виде в разделе «Папки»);
- папки «Рабочий стол», где сохраняются файлы и папки, создаваемые на рабочем столе, «Корзина»;
- папку «Накопители», которая содержит съемные устройства (аналог «Устройств и дисков» в Windows);
- папку «Файловая система», которая во многом является аналогом системного диска Windows C.

Задание 6. Используя контекстное меню на значке «Мой компьютер», определите свойства операционной системы.

Задание 7. Измените вид папки и атрибуты файлов.

1) Используя папку «Мой компьютер», откройте диск D и установите (открыть) папку OUR.

2) Рассмотрите типовое окно папки. Изучите все ее элементы.

3) Рассмотрите панель инструментов и определите назначение всех ее значков.

Установите сортировку файлов в режиме «таблица по типу, затем дате, имени и размеру». Включите на панели «Область просмотра» (см. рис. 1.3).

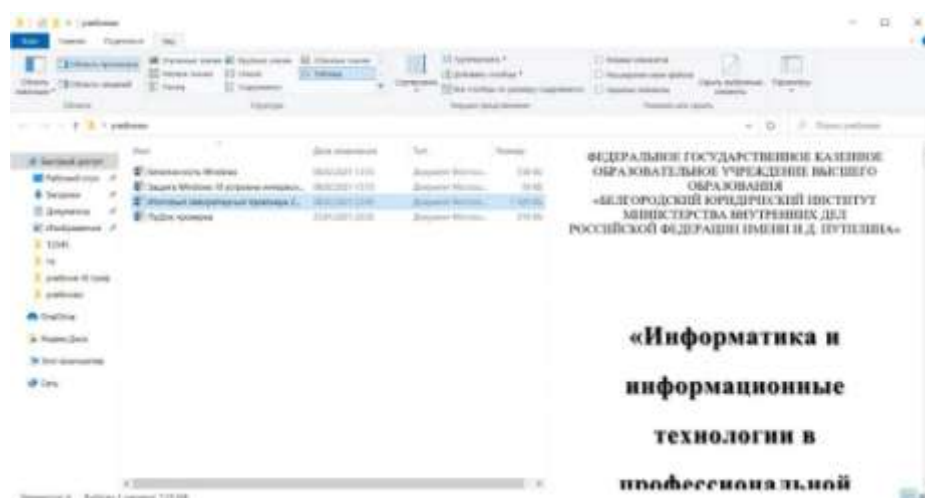


Рисунок 1.3. Окно проводника

10. При запуске «Менеджера файлов» (см. рис. 1.4) с панели задач Astra Linux он открывается с развернутой папкой «Домашняя».

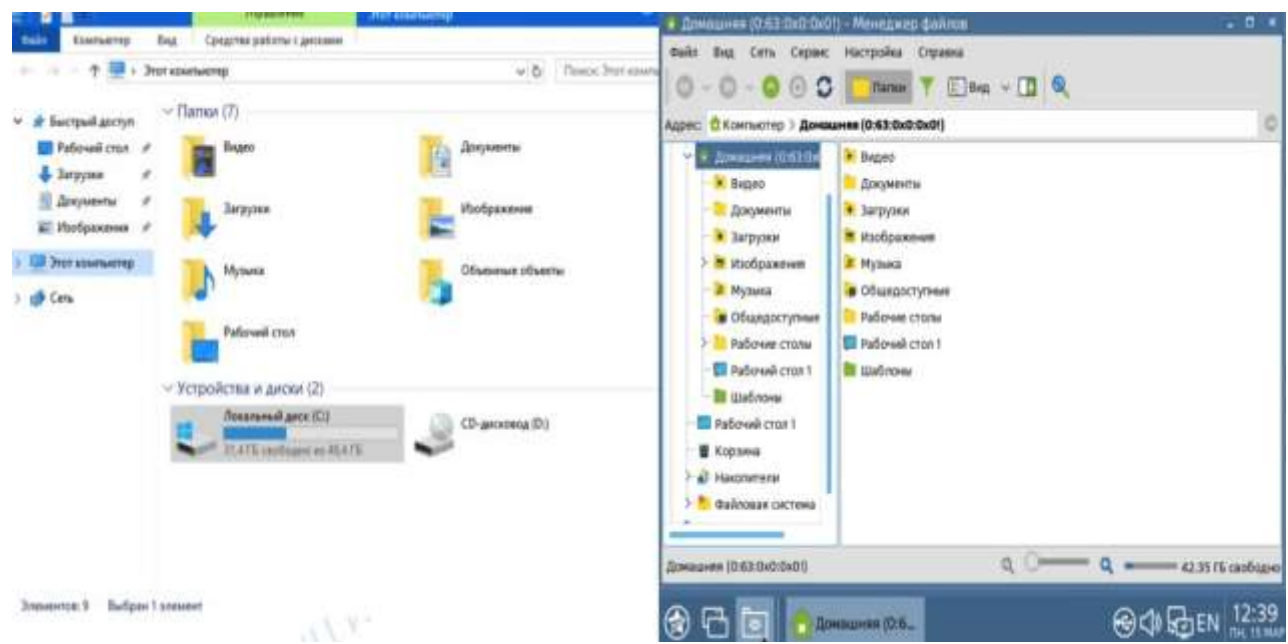


Рисунок 1.4. Менеджер файлов

11. Программа «Панель управления» предоставляет централизованный доступ к графическим программам настройки и администрирования системы. Для вызова привилегированных действий запрашивается авторизация.

Задание 8. Заполните таблицу 1.3, определив примеры программного обеспечения, используемого в операционных системах.

Таблица 1.3. Программное обеспечение, используемое в операционных системах

Программное обеспечение	Пример в ОС Windows	Пример в ОС Astra Linux
Архиватор		
Антивирусная программа		
Текстовый редактор		
Графический редактор		
Редактор презентаций		
Табличный процессор		

12. Командная строка (cmd) – это простой и универсальный инструмент для управления операционными системами. Она подходит в первую очередь для профессионалов, а также для любителей тонкой персональной настройки устройств. Выполняет следующие основные функции:

– диагностика персонального компьютера. Под этим термином понимается комплексная проверка всех систем и приложений так, чтобы можно было выявить самые различные проблемы и эффективно их решить;

– проверка активных процессов. Помогает при необходимости оценить быстродействие системы, позволяет просмотреть все запущенные процессы в реальном времени;

– восстановление системы. Эта функция применяется для перезапуска устройства или отката системы и приложений к заданным ранее параметрам. В современных операционных системах для этого используется так называемая точка восстановления.

Также сюда входит работа с файлами, папками и программами, проверка Интернета, оценка качества соединения и многие другие возможности.

Для запуска командной строки в ОС Windows: нажать Win + R (либо перейти в меню «Пуск» и выбрать пункт «Выполнить»), в появившемся окне набрать cmd и нажать ОК.

Открыть командную строку в Linux-системах можно через консоль или терминал. Его можно запустить набрав слово «терминал» в поисковой строке ОС или через комбинацию клавиш Ctrl + Alt + T. Для работы в операционных системах удобно использовать горячие клавиши.

Задание 9. Работа в командной строке ОС.

При помощи командной строки провести анализ конфигурации ОС по следующим данным: сбор информации о системе, о жестком диске, о сетевой конфигурации; системные настройки (установленные программы, службы и обновления), информация о процессах (см. табл. 1.4).

Таблица 1.4. Примеры команд

Категория	Команда (Windows)	Описание	Команда (Astra Linux)	Описание
Общие свойства системы	systeminfo	Отображает подробную информацию о системе: версию ОС, аппаратные компоненты, установленные обновления и т.д.	uname -a	Показывает информацию о системе, ядре, архитектуре и версии ОС
Анализ дисков	wmic diskdrive list brief	Показывает информацию о жестких дисках, включая их размер, тип и состояние	lsblk	Показывает информацию о подключенных устройствах хранения и их разделах
Сетевая конфигурация	ipconfig	Отображает настройки сети, включая IP-адрес	ip a	Показывает информацию о сетевых интерфейсах

Установленные программы	wmic product get name,version	Отображает список установленных программ с их версиями	dpkg -- list	Выводит список установленных пакетов на системе, используя пакетный менеджер dpkg
-------------------------	-------------------------------	--	--------------	---

Итоговый отчет оформить текстовым файлом (WordPad/nano).

Основные понятия и термины

Операционная система – это комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.

Ядро операционной системы – это основа системы. Ядро – это резидентная часть операционной системы (постоянно находится в оперативной памяти), работающая в привилегированном режиме.

Защита информации – это комплекс мер, направленных на создание и дальнейшее обеспечение информационной безопасности.

Архитектура ОС – это структурная и функциональная организация ОС на основе некоторой совокупности программных модулей. Архитектура определяет принципы действия, информационные связи и взаимодействие основных компонентов ОС. Большинство современных ОС представляют собой хорошо структурированные модульные системы, способные к развитию, расширению и переносу на новые платформы.

Вопросы и задания для оценки теоретических знаний

1. Что такое операционная система?
2. Что представляет собой структура операционной системы?
3. Каковы функции операционной системы?
4. Каковы основные компоненты операционной системы?
5. Какие типы архитектур операционных систем Вы можете назвать?
6. Какие модули выполняют основные функции операционной системы?
7. Какова классификация операционных систем в зависимости от способа организации вычислений?
8. Какова классификация операционных систем в зависимости от типа ядра?
9. Какова классификация операционных систем в зависимости от возможности работы в компьютерной сети?
10. Какие наиболее важные принципы закладываются в основу построения операционных систем?
11. Каков набор методов (функций), который программист может использовать при разработке собственных программ?
12. Что такое Astra Linux Special Edition?
13. Перечислите основные этапы установки операционной системы Astra Linux.
14. Что означает уровень защищенности?
15. Приведите примеры «надежного» и «ненадежного» пароля.

2. ОБРАБОТКА ТЕКСТОВОЙ, ТАБЛИЧНОЙ И ГРАФИЧЕСКОЙ ИНФОРМАЦИИ

Вопросы для самостоятельного изучения:

- 2.1. Изучение функциональных возможностей текстовых процессоров.
- 2.2. Изучение функциональных возможностей табличных процессоров.
- 2.3. Изучение функциональных возможностей графических процессоров.

Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы

При рассмотрении **первого вопроса** необходимо уяснить понятие текстового редактора, а также рассмотреть возможности офисных пакетов приложений.

LibreOffice является профессиональным инструментом для подготовки текстовых документов, электронных таблиц, создания бизнес-графики, презентаций и ведения офисных баз данных. LibreOffice включает в себя следующие компоненты:

1. Writer – многофункциональный текстовый процессор.
2. Calc – табличный процессор, включающий в себя продвинутые средства для анализа, построения диаграмм и принятия решений.
3. Impress обеспечивает все средства для создания мультимедиапрезентаций, включая специальные элементы, анимацию и средства для рисования.
4. Draw – это инструмент для создания векторной графики, с помощью которого можно создавать все – от простых диаграмм и блок-схем до сложной 3D-графики.
5. Math – это инструмент для создания и редактирования формул в LibreOffice.

6. Base – это компонент LibreOffice, предназначенный для создания баз данных. Источники данных, или база данных, – это массив информации, организованный особым образом для обеспечения более легкого доступа, управления и обновления [28]. Модуль Base обеспечивает инструментальные средства для ежедневной работы с базами данных в пределах простого интерфейса. Он может создавать и редактировать формы, отчеты, запросы, таблицы, представления и отношения так, чтобы управление связанной базой данных было удобно пользователю.

Для обработки текстовой информации применяется текстовый редактор Writer. Writer – многофункциональный текстовый процессор, входящий в состав пакета LibreOffice.

Главная рабочая область окна Writer, как уже говорилось, схожа в элементах с текстовым процессором Microsoft Word [25] (см. рис. 2.1).

Заголовок окна отображает имя обрабатываемого файла и компонент пакета, в котором производится работа.

Главное меню – унифицированная часть всего пакета, ее панель представлена следующими элементами:

1. Файл – содержит подменю применимых ко всему документу команд (открыть, сохранить или экспорт в PDF).
2. Правка – содержит подменю команд редактирования (копировать, вырезать, вставить, найти).
3. Вид – содержит подменю команд организации отображения документа на экране (режим, масштаб).
4. Вставка – содержит подменю команд импортирующих в документ элементов (колонтитулы, изображение).
5. Формат – содержит подменю команд форматирования элементов документа (нумерация, интервалы, взаиморасположение внедренных объектов).
6. Стили – содержит подменю команд групповых элементов форматирования (текстовые стили, стили списков, стили страниц).
7. Таблица – содержит подменю команд организации работы с таблицами в документе (вставки строк/столбцов, форматы ячеек).
8. Форма – содержит подменю команд для реализации элементов языка гипертекстовой разметки документа (HTML).
9. Сервис – содержит такие функции, как «Орфография и грамматика», «Настройка», «Параметры».
10. Окно – содержит подменю команд настройки представления пользовательского окна (открыть копию окна, переключаться между окнами).
11. Справка – содержит ссылки на файл справки LibreOffice, помощь по пакету в Интернете и информацию о программе.

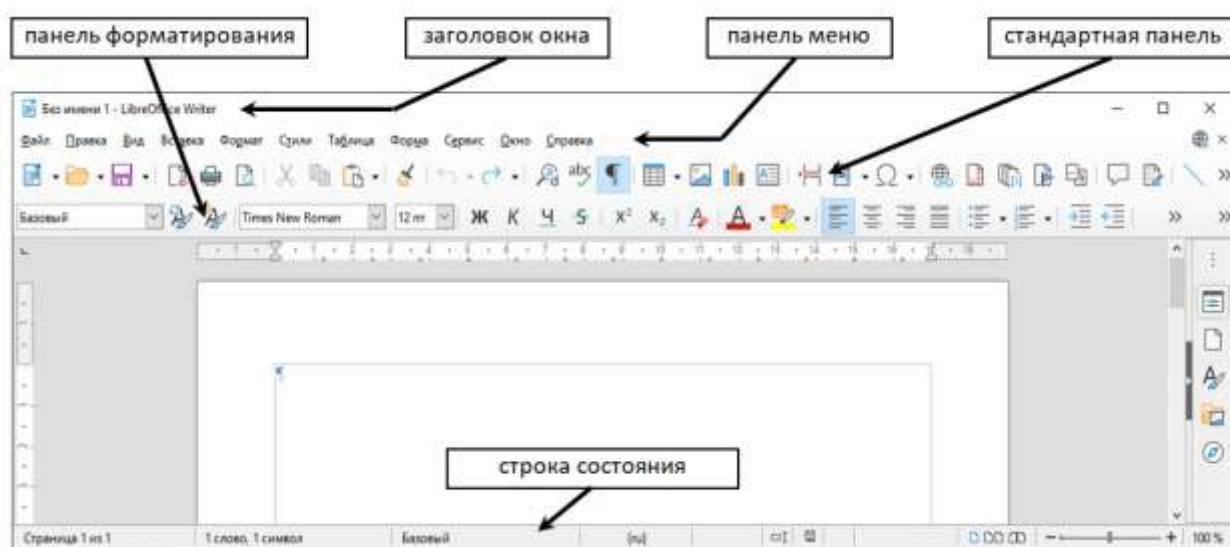


Рисунок 2.1. Главная рабочая область окна Writer

Под главным меню закреплена стандартная панель инструментов, она является типовой (унифицированной) для всех компонентов LibreOffice. Панель посредством кнопок реализует быстрый доступ к наиболее используемым элементам управления и форматирования компонента Writer. Их оформление дублирует графическое оформление команд, соответствующих меню.

По умолчанию в качестве следующей панели размещается панель инструментов «Форматирование». Она способна видоизменяться в зависимости от положения курсора или выбранного объекта. Например, показываются инструменты для работы с графическими объектами при нахождении курсора на изображении или инструменты для форматирования текста при нахождении курсора в тексте.

Строка состояния Writer, размещенная в нижней части рабочей области, содержит информацию о текущем документе, а также позволяет получить быстрый доступ к некоторым настройкам (см. рис. 2.2.).



Рисунок 2.2. Строка состояния Writer

Элементы строки состояния:

1. Номер страницы – показывает порядковый номер текущей страницы и общее количество страниц в документе (либо сегменте, если нумерация внутри заново повторяется в разделах документа). При нажатии правой кнопки мыши на этом поле будет вызван список закладок (если они были определены). Двойной щелчок левой кнопкой мыши по полю откроет окно «Навигатор» для быстрого перехода к нужной странице документа.

2. Количество слов динамически отображает количество слов в документе. При выделении курсом фрагмента текста поле отобразит статистику в отношении выделенного фрагмента.

3. Стиль страницы – показывает стиль текущей страницы. Нажатие правой кнопкой мыши позволит перейти в список стилей страниц, аналогично «Стили».

4. Язык – отображает язык выделенного фрагмента текста, используемый для проверки орфографии.

5. Режим вставки – отображает активный режим «вставка/замена».

6. Режим выделения – отображает режимы выделения (обычное, расширяемое, добавляемое, блочное).

7. Изменение статуса документа – отображает наличие в документе несохраненных изменений.

8. Цифровая подпись – отображается в случае содержания цифровой подписи в документе.

9. Информация о выделенном элементе или объекте – отображает свойства выделенного фрагмента текста (заголовок, список, таблица).

10. Режим отображения страниц – удобство представления многостраничного документа на экране (одна страница, «бок о бок», макет книги).

11. Масштаб – отображение и изменение (при помощи ползунка или ввода числового значения) масштаба отображения страницы документа.

В пакете LibreOffice реализована и прикрепляемая боковая панель элементов (см. рис. 2.3), позволяющая упростить доступ к дополнительным функциям. Она также доступна во всех компонентах пакета. Ее удобство ощутимо при использовании широкоформатных мониторов. Включить ее отображение можно используя пункт меню Вид → Боковая панель. В Writer она содержит команды разделов «Меню конфигурации боковой панели», «Свойства», «Стили и форматирование», «Галерея», «Навигатор», дублирующие соответствующих разделов главного меню.

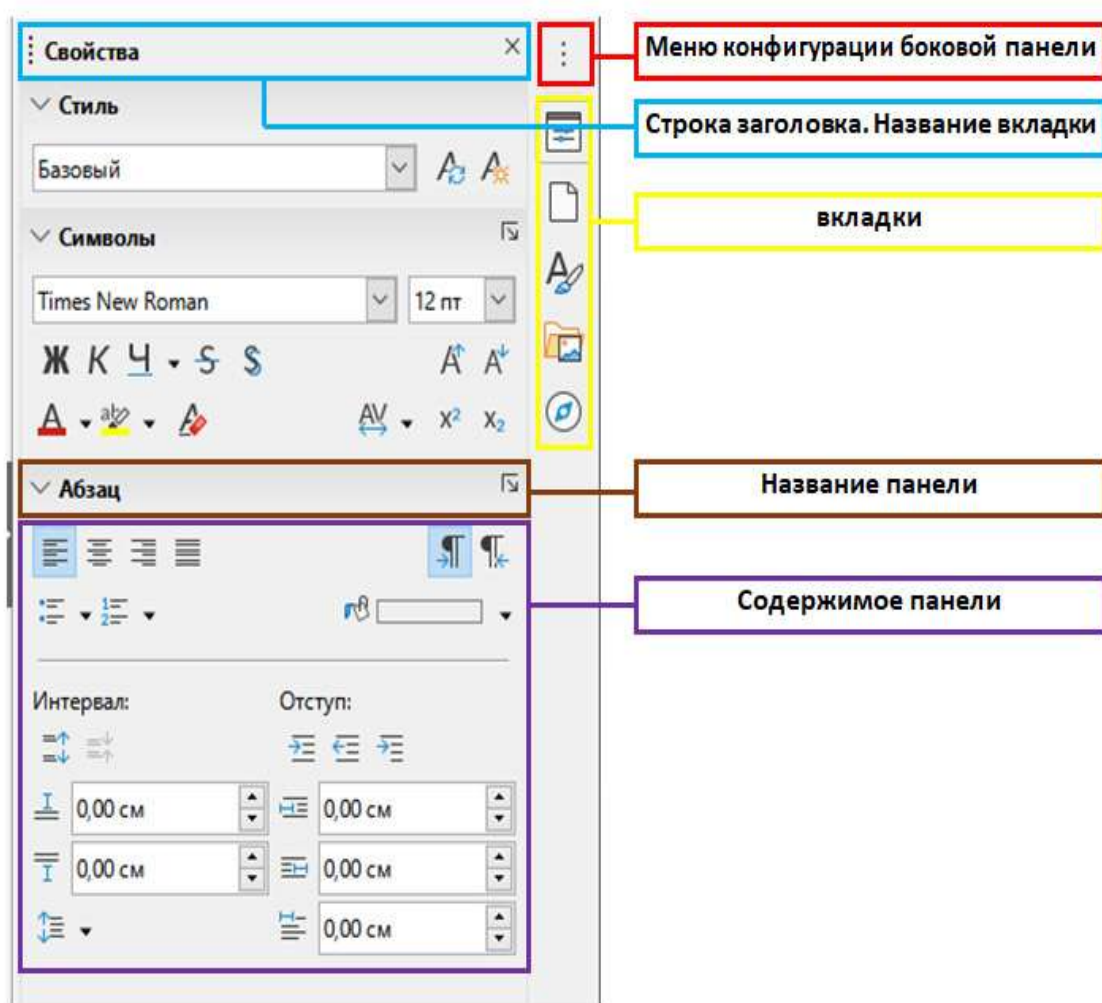


Рисунок 2.3. Боковая панель Writer

К оформлению документов предъявляются требования, установленные регламентирующими нормативными правовыми актами [33]. В частности, в системе МВД России требования вводит приказ МВД России от 02.09.2024 № 515. Эти требования реализуются инструментами текстового процессора. Начальные параметры документа, такие как формат бумаги либо нестандартные размеры, ориентация листа, поля документа, можно задать и впоследствии изменить командами категории «Стиль страницы».

Для доступа к ним откройте пункт главного меню Формат→Стиль страницы... (см. рис. 2.4).

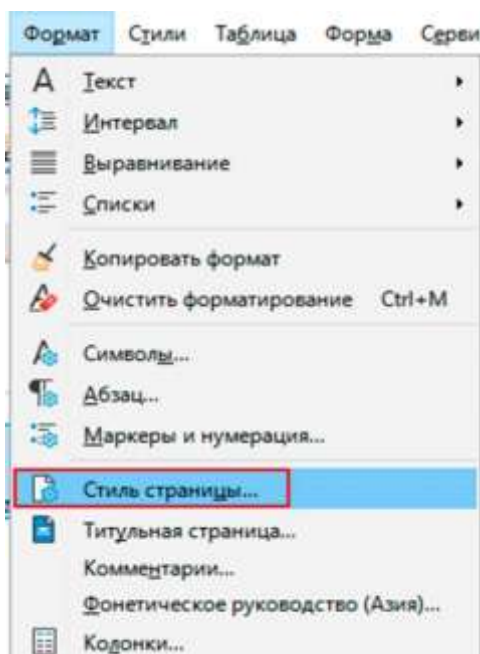


Рисунок 2.4. Команда «Стиль страницы...», меню «Формат»

В открывшемся окне на вкладке «Страница» доступны для изменения параметры формата бумаги, ориентации, полей... (см. рис. 2.5).

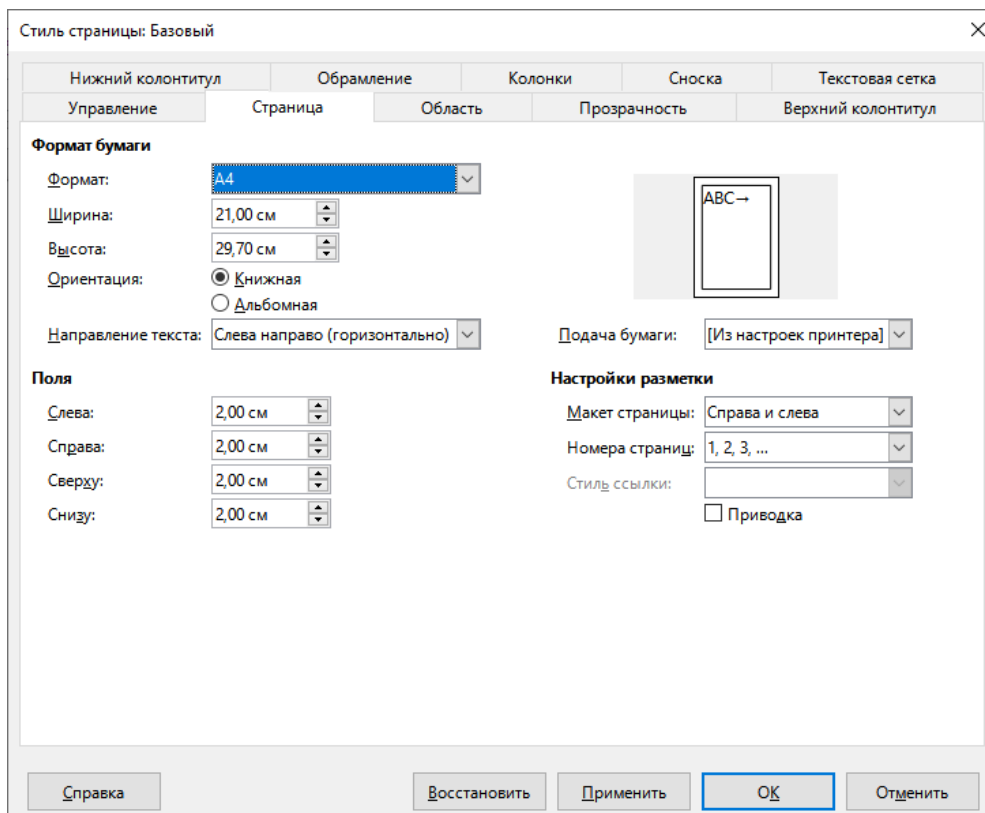


Рисунок 2.5. Окно команд «Стиль страницы...», вкладка «Страница»

В дополнительных вкладках доступны элементы управления параметрами колонтитулов, сносок, оформлением обрамления и области документа. Доступ к таким же элементам управления возможен через боковую панель Writer, а именно через вкладку «Стиль» (см. рис. 2.6).

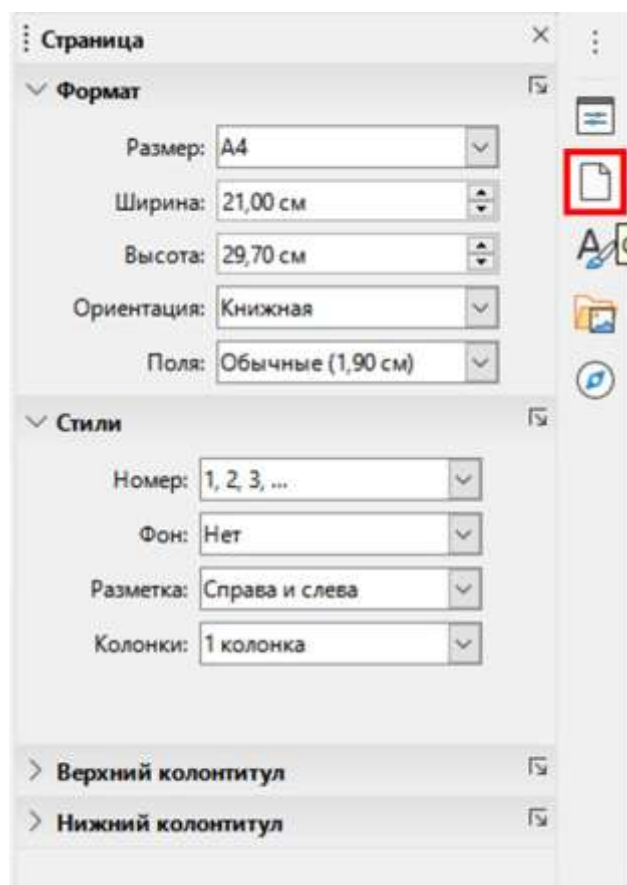


Рисунок 2.6. Меню вкладки «Стиль» боковой панели

Требования к используемым шрифтам, отступам, интервалам реализуются соответствующими командами панели подменю «Формат» главного меню, кнопками панели форматирования или вкладки «Стиль» боковой панели, которые также состоят из групп форматирования шрифтов, абзацев и интервалов.

Аналогично пакету Microsoft доступными командами можно реализовать нужные элементы форматирования [31]. Только перечислим некоторые наиболее используемые из них (смысл элемента понятен из названия команды):

- форматирование абзаца – выровнять по левому краю, выровнять по центру, выровнять по правому краю, выровнять по ширине;
- междустрочный интервал – одинарный, полуторный, двойной, задать интервал;
- списки – маркированные, нумерованные;
- отступы – уменьшить, увеличить;
- форматирование символов – название шрифта, размер шрифта, жирный, курсив, подчеркнутый, верхний индекс, нижний индекс, увеличить шрифт, уменьшить шрифт, цвет шрифта, выделение цветом, цвет фона.

Часто используемые операции по обработке фрагментов текста из других документов, такие как копирование, вырезание и вставка текста, в Writer схожи по реализации с другими приложениями. Их выполнение доступно с использованием мыши и(или) клавиатуры: копирование или перемещение текста методом перетаскивания при помощи пунктов меню, кнопки панели инструментов, а также определенных сочетаний клавиш клавиатуры.

Использование пунктов меню «Правка», равно как дублирующих их кнопок стандартной панели, соответствует названию пункта или ниспадающей подсказки при наведении курсора на нужную кнопку: копировать, вырезать, вставить. Без использования этих пунктов выделенный текст перемещается простым его перетягиванием с зажатой левой кнопкой мыши. Если при этом удерживать нажатой клавишу Ctrl, произойдет не перемещение, а копирование выделенного фрагмента текста. Вместо свойств кнопок можно использовать определенные сочетания клавиш клавиатуры, опять же аналогичные сочетаниям, используемым при работе в Word. Сочетание Ctrl + C позволяет скопировать выделенный фрагмент текста, рисунок, диаграмму в буфер, сочетание Ctrl + X – вырезать, а Ctrl + V – вставить выделенные скопированный или вырезанный объект или фрагмент в место расположения курсора.

Таблица является структурированной интерпретацией массива данных в удобном для восприятия формате. Она легче воспринимается пользователями, чем последовательность чисел, позволяет наглядно провести сравнение, лишает обычный текст монотонности.

Создание таблицы и работа с ними в текстовом процессоре Writer пакета LibreOffice схожа с работой в Word, поэтому уверенным пользователям пакета Microsoft эти задачи не составят труда.

При создании таблицы первоначальным этапом является определение ее структуры и размерности, несмотря на то, что последующее добавление строк, столбцов или ячеек не проблема для редактора.

2. Для создания необходимо перейти в меню Таблица → Вставить таблицу (см. рис. 2.7) или использовать комбинацию клавиш Ctrl + F12, после чего программа откроет соответствующее окно (см. рис. 2.8) с параметрами.

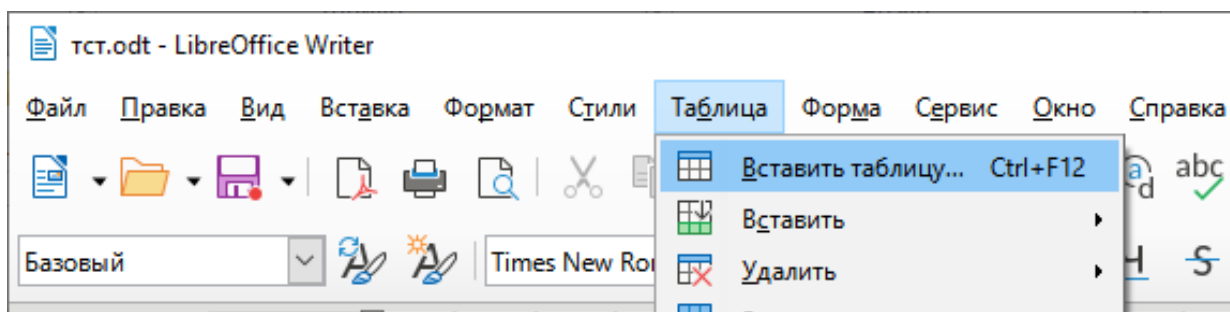


Рисунок 2.7. Выбор пункта меню для создания таблицы

Вставить таблицу

Общие

Имя:

Столбцов: Строк:

Параметры

☐ Заголовок

☒ Повторять строки заголовка на новых страницах

Строк заголовка:

☐ Не разбивать таблицу по страницам

Стили

Нет

Базовый

Трёхмерный

Синий

Коричневый

Фиолетовый

Жёлтый

Серый

	Янв	Фев	Мар	Сумм
Севе	6	7	8	21
Сере	11	12	13	36
Юг	16	17	18	51
Сумм	33	36	39	108

Рисунок 2.8. Меню параметров создаваемой таблицы

В качестве настраиваемых элементов на этапе создания являются имя таблицы, количество столбцов и строк, дополнительно можно указать строку (или строки) для использования в качестве заголовка и стиля оформления из заготовок программы. Созданная таблица будет пустая, без наполнения ячеек, что будет являться уже следующей задачей.

Создать таблицу также можно от обратного – на основе имеющихся данных наполнения ячеек. Главное, чтобы исходные данные были структурированы и понятны программе (см. рис. 2.9):

- строка исходного текста – это элементы одной строки будущей таблицы;
- строка заканчивается знаком переноса строки (Enter);
- элементы в строке разделяются одинаковыми символами-разделителями, тем самым разбивая элементы строки на столбцы будущей таблицы;
- если в подготовленных строках будет разное количество элементов, то они будут внесены в первые столбцы.

```
Стр 1-1; Стр 1-2; Стр 1-3; Стр 1-4;
Стр 2-1; Стр 2-2; Стр 2-3; Стр 2-4;
Стр 3-1; Стр 3-2; Стр 3-3; Стр 3-4;
```

Рисунок 2.9. Пример подготовленного текста для создания таблицы

Подготовленный текст выделяем и переходим в меню Таблица → Преобразовать → Текст в таблицу, в появившемся окне выбираем использованный для элементов таблицы разделитель → Ок (см. рис. 2.10).

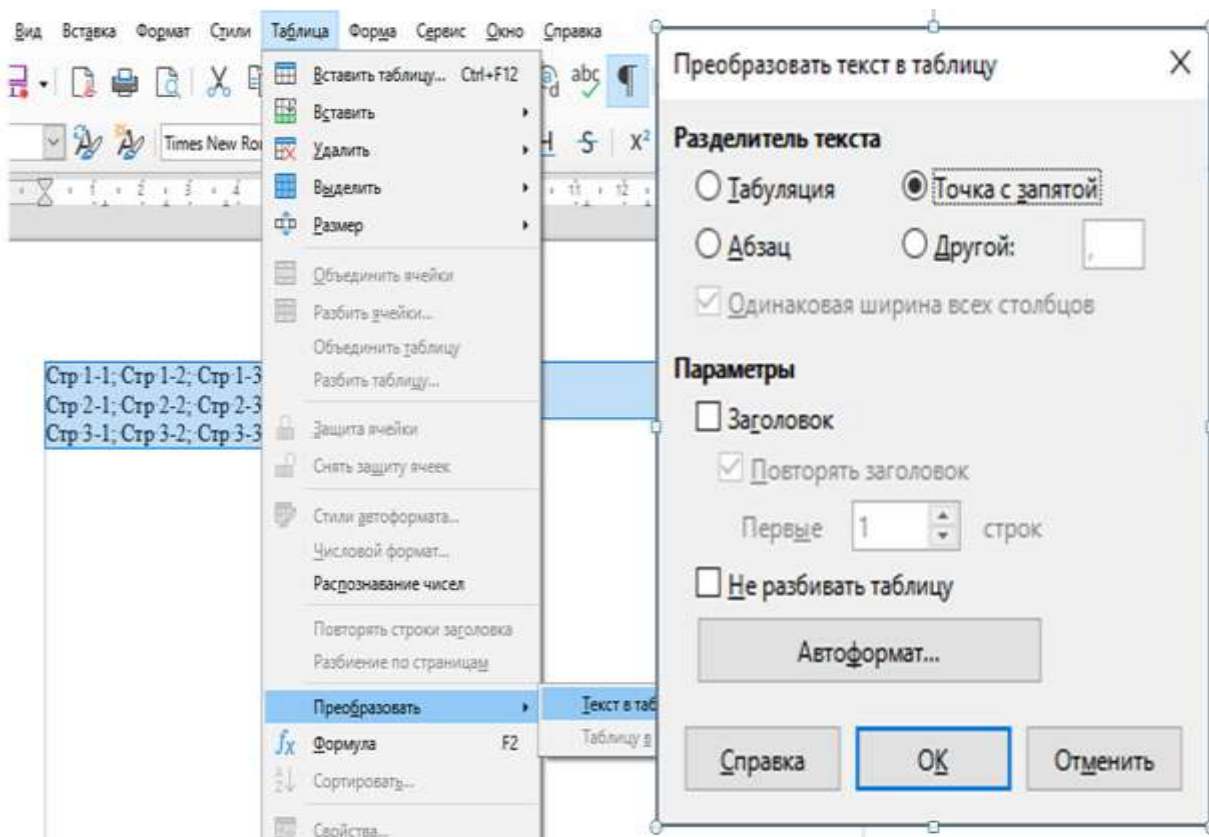


Рисунок 2.10. Меню преобразования текста в таблицу

В результате получится таблица (см. рис. 2.11) размером в три строки на пять столбцов. Почему пять, если в подготовленном тексте было по четыре элемента в строке? Потому, что после четвертого элемента стоял символ-разделитель в виде точки с запятой, который указывает на разделение в строке между ячейками и наличие следующего элемента, а окончанием строки является символ перевода строки **↵**. Тем самым при формировании исходных данных указаны пять ячеек в строке, из которых первые четыре заполнены, а пятая является пустой.

Стр 1-1↵	Стр 1-2↵	Стр 1-3↵	Стр 1-4↵	↵
Стр 2-1↵	Стр 2-2↵	Стр 2-3↵	Стр 2-4↵	↵
Стр 3-1↵	Стр 3-2↵	Стр 3-3↵	Стр 3-4↵	↵

Рисунок 2.11. Таблица, полученная преобразованием текста

В текстовом процессоре используют таблицы, как правило, для разбавле-

ния буквенного массива наглядной информацией. Для реализации расчетов лучше использовать табличный процессор, например Calc из пакета LibreOffice. Поэтому рассмотрим лишь некоторые возможности форматирования таблиц с точки зрения оформления.

После создания таблицы станут доступными инструменты панели инструментов «Таблица», пункты меню «Таблица», а также меню, вызываемое нажатием правой кнопкой мыши на таблице. Они схожи с реализованными в Word [25]. Как востребованную функцию следует отметить возможность вертикального отображения текста в ячейках. Для ее реализации необходимо выделить ячейки, по отношению к которым будет производиться это форматирование, затем необходимо вызвать меню «Свойства таблицы». Это можно сделать нажав правой кнопкой мыши на выделенных ячейках, в появившемся меню выбрать последний пункт «Свойства», или зайти в меню «Таблица», последний пункт «Свойства», также кнопка «Свойства» доступна на панели инструментов «Таблица».

В меню «Свойства таблицы» возможность выбора ориентации текста находится на вкладке «Положение на странице» (см. рис. 2.12).

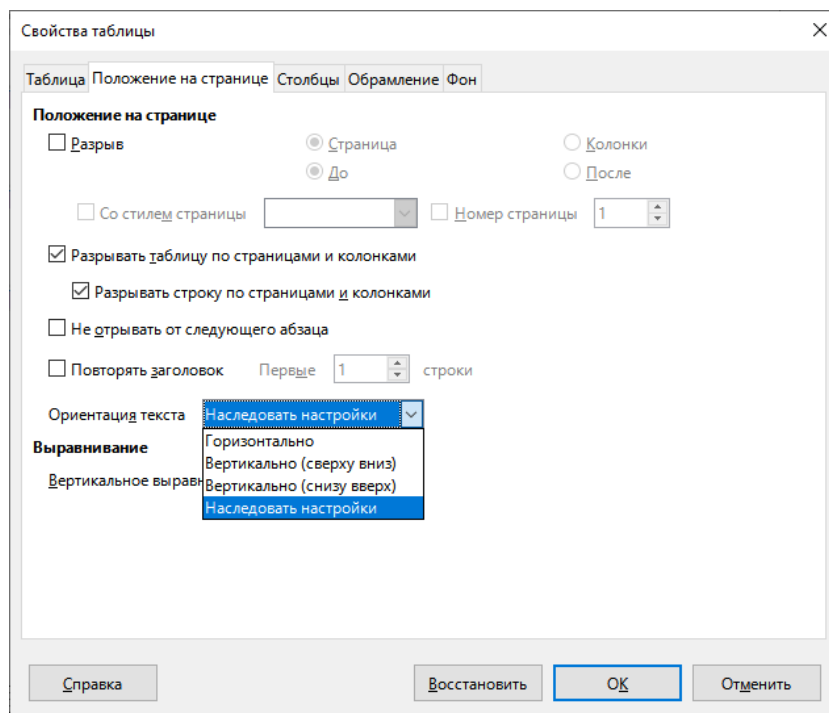


Рисунок 2.12. Выбор ориентации текста в меню «Свойства таблицы» на вкладке «Положение на странице»

На других вкладках меню «Свойства таблицы» также можно выбрать необходимые варианты формата, цвета, толщины линий границ таблицы, цветовой заливки ячеек, интервалов между текстом и границами ячеек, выравнивание текста внутри ячеек таблицы.

Задание 1. Создайте текстовый документ «Рапорт» в Writer. Тема созда-

ваемого документа – рапорт на предоставление дополнительных дней отдыха.

Задание 2. В созданном документе расставьте абзац, шрифт.

1. Установите абзац с отступом 1,25.
2. Установите шрифт PT Astra Serif.
3. Установите размер шрифта – 14.
4. Установите начертание шрифта – нормальное.
5. Установите следующие поля: верхнее – 2 см, нижнее – 2 см, правое – 1 см, левое – 3 см. Ориентация книжная.

Второй вопрос предполагает необходимость изучения функциональных возможностей табличных процессоров. Для обработки табличной информации может быть использован табличный процессор Calc.

Основные функциональные возможности табличных процессоров:

1. Ввод, редактирование и хранение данных.
2. Представление данных в удобной для пользователя форме.
3. Поиск, сортировка и фильтрация данных.
4. Проведение арифметических вычислений.
5. Обработка данных с помощью встроенных математических, логических и иных функций.
6. Выполнение функций баз данных.
7. Статистический анализ данных.
8. Создание диаграмм.

Задание 3. Создайте таблицу.

Порядок выполнения задания:

1. Запустите приложение – табличный процессор Calc (см. рис. 2.13). Calc – это компонент для работы с электронными таблицами из состава LibreOffice. В электронную таблицу можно вводить данные (обычно числа) и обрабатывать их для получения определенного результата.

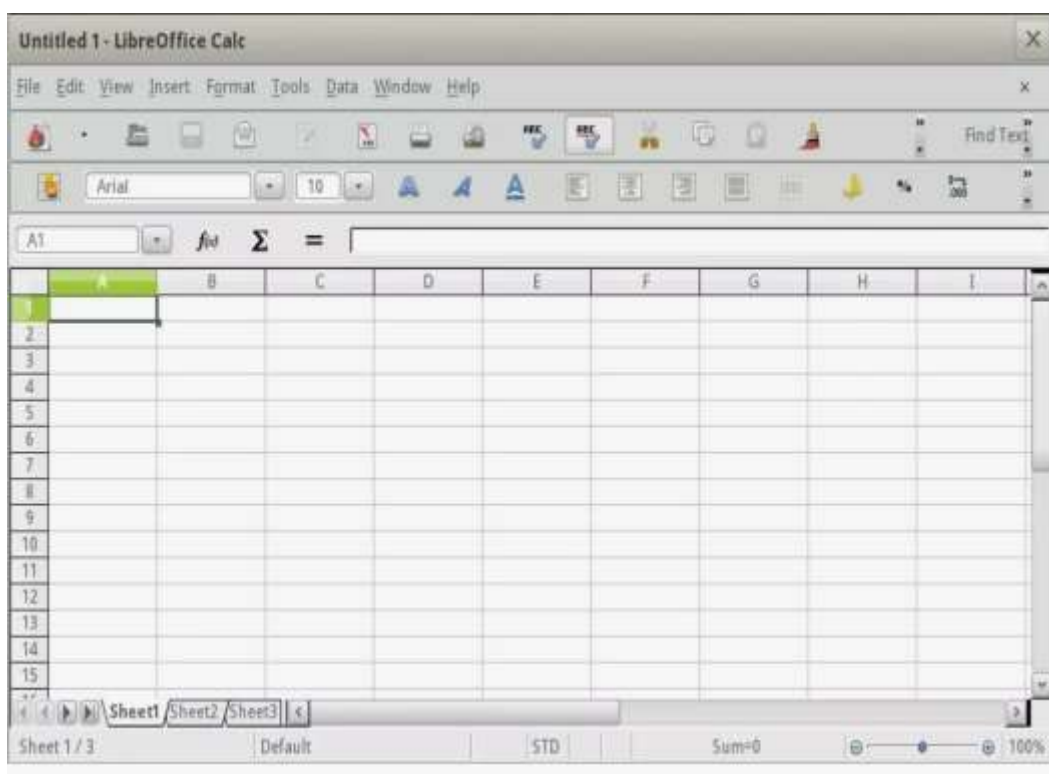


Рисунок 2.13. Главная рабочая область окна Calc

2. Изучите интерфейс (сверху – лента инструментов; рабочая область представлена ячейками; строки обозначены цифрами; столбцы обозначены буквами латинского алфавита; активная ячейка выделена жирной рамкой).

3. Создайте простую таблицу.

Введите текст в ячейку A1: «Товар». В ячейку B1: «Количество». В ячейку C1: «Цена». Заполните строки 2–4 данными о товарах.

4. Выполните базовые операции.

Форматирование: выделите диапазон A1:C1. Нажмите ПКМ и выберите «Формат ячеек». Установите жирный шрифт.

Вычисления: в ячейку D1 введите: «Итого». Далее в ячейку D2 введите формулу: $= B2 * C2$.

Для копирования формулы выделите ячейку D2. Наведите курсор на нижний правый угол и перетащите вниз до строки 4.

5. Постройте диаграмму по составленной таблице. Диаграммы позволяют наглядно представить данные, содержащиеся в таблицах, в графическом виде. Создание диаграммы:

- 1) выберите данные для диаграммы;
- 2) на вкладке «Вставка» нажмите кнопку «Диаграммы»;
- 3) нажмите кнопку ОК;

6. Сохраните работу.

Нажмите Файл → Сохранить как. Выберите папку. Введите имя файла и выберите формат (рекомендуется. ods). Нажмите «Сохранить».

7. Дополнительные советы – можно использовать горячие клавиши:

- Ctrl + C – копировать;
- Ctrl + V – вставить;
- F2 – редактировать ячейку;
- Ctrl + Z – для отмены действия;
- Ctrl + Y – для повтора.

При изучении **третьего вопроса** необходимо акцентировать внимание на функциональных возможностях графических процессоров. Компьютерная графика (англ. computer graphics, или CG) – способ создания графических изображений и визуальной информации с помощью специальных программ [23].

Задание 4. Назовите основные виды компьютерной графики, заполнив таблицу 2.1.

Таблица 2.1. Виды компьютерной графики

Виды компьютерной графики	Описание
	
	
	
	

Задание 5. Обработка графической информации.

1. Сделайте скриншот экрана рабочего стола ОС. Для этого необходимо нажать комбинацию клавиш CTRL + PrtSc. Затем продолжите в ОС Windows. Запустите приложение Paint (Пуск – Все программы – Стандартные – Paint). Вставьте изображение скриншота в программу Paint комбинацией CTRL + V.

2. Сохраните полученное изображение на рабочем столе в ОС под именем, содержащим первые три буквы вашей фамилии (*Файл – Сохранить как... – Выбрать рабочий стол – Тип файла – «ВМР» – Имя файла* (первые три буквы фамилии)). Закройте документ и убедитесь, что он появился на рабочем столе.

3. Внесите следующие *изменения* в рисунок: поверх картинki вставьте прямоугольные блоки, текст в которых описывает выбранные элементы рабочего стола и сохраните изменения.

Основные понятия и термины

Текстовый процессор – компьютерная программа, используемая для набора, сохранения, редактирования и печати текста. Современные текстовые процессоры имеют также функции компоновки макета текста и предварительного просмотра документов в том виде, в котором они будут напечатаны.

Табличный процессор – это прикладное программное обеспечение для создания, изменения и печати различных таблиц. Такая программа используется для управления электронной таблицей.

Электронная таблица – компьютерный эквивалент обычной таблицы, в ячейках которой записаны данные различных типов (текст, числа, даты, формулы и т.д.).

Информационная безопасность – состояние защищенности личности, организации и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве.

Киберпространство – сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства).

Критическая информационная инфраструктура (далее – КИИ) – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электро-связи, используемые для организации их взаимодействия [3].

Объект КИИ – информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, принадлежащие субъекту КИИ [10; 14].

Вопросы и задания для оценки теоретических знаний

1. Дайте определение термину «табличный редактор информации».
2. Дайте определение термину «текстовый редактор информации».
3. Приведите примеры офисных приложений.
4. Приведите примеры «надежного» и «ненадежного» пароля.
5. В чем разница между абсолютным и относительным адресом ячейки?

3. НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

Вопросы для самостоятельного изучения:

- 3.1. Нормативно-правовое регулирование в сфере кибербезопасности.
- 3.2. Порядок и особенности поиска нормативных правовых актов в справочно-правовых системах.

Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы

При рассмотрении **первого вопроса** следует разъяснить необходимость нормативного регулирования в сфере кибербезопасности.

Задача нормативно-правового регулирования обеспечения кибербезопасности в Российской Федерации является органичным компонентом государственной политики развития национального сектора применения информационных технологий [5; 6; 27].

Задание 1. Перечислите основные нормативные правовые акты в области кибербезопасности.

Задание 2. Приведите примеры использования международной нормативной практики обеспечения кибербезопасности.

Задание 3. Что такое справочно-правовая система (далее – СПС)? Приведите примеры СПС.

Раскрывая содержание **второго вопроса**, нужно определить порядок и особенности поиска нормативных правовых актов в СПС «КонсультантПлюс».

Задание 4. Запустите СПС «КонсультантПлюс».

4.1. Перейдите по ссылке: <https://student2.consultant.ru/cgi/online.cgi?req=home&rnd=7kMyWOUXYljJeGfB>

4.2. Изучите интерфейс СПС «КонсультантПлюс» (см. рис. 3.1).

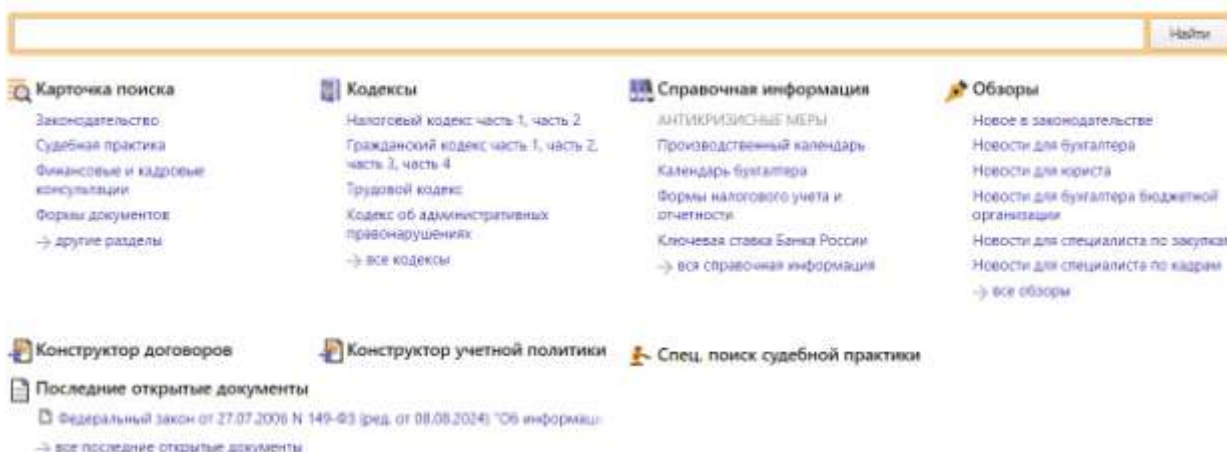


Рисунок 3.1. Интерфейс СПС «КонсультантПлюс»

Задание 5. Используя СПС «КонсультантПлюс», дайте определение понятию «информация». Приведите классификацию информации согласно Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2].

Задание 6. Используя СПС «КонсультантПлюс», найдите Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» и перечислите виды персональных данных [9; 19].

Задание 7. Запустите СПС «КонсультантПлюс». Перейдите в раздел «Карточка поиска» (см. рис. 3.2). Заполните карточку реквизитов для поиска писем МВД России. Запишите, сколько документов найдено и в каком разделе.

Порядок выполнения задания:

1. Очистите карточку, нажав CTRL-DEL
2. Щелчком по строке «Вид документа».
3. Наберите «ПИСЬМО».
4. Выберите ПИСЬМО из словаря.

5. Аналогичным образом в реквизите «Принявший орган» выберите «МВД России».

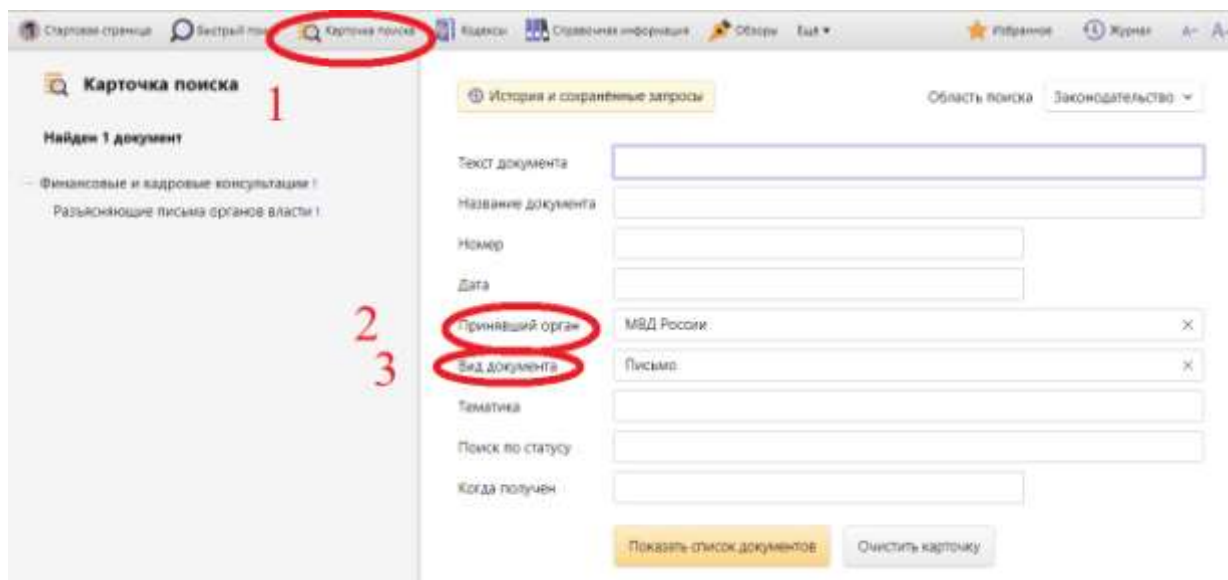


Рисунок 3.2. Карточка поиска

Задание 8. Найдите Федеральный закон от 30.11.2011 «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Запишите его номер.

Задание 9. Найдите указы Президента Российской Федерации за первую половину 2023 г. с использованием корешка «Диапазон» пункта «Дата» карточки поиска. Законспектируйте количество найденных документов.

Задание 10. Изучите Кодекс Российской Федерации об административных правонарушениях и выявите статьи КоАП РФ, в соответствии с которыми предусмотрено наказание за правонарушения в Интернете.

Порядок выполнения задания.

В открытом Кодексе Российской Федерации об административных правонарушениях во вкладке «Оглавление» введите в поисковой строке слово «Интернет», найдите и изучите 10 статей КоАП РФ.

Задание 11. Изучите Уголовный кодекс Российской Федерации и выявите статьи УК РФ, в соответствии с которыми предусмотрено наказание за преступления в сфере компьютерной информации.

Порядок выполнения задания.

Для поиска документов воспользуйтесь вкладкой «Кодексы». Выберите Уголовный кодекс Российской Федерации. В открывшемся кодексе найдите вкладку «Оглавление», затем перейдите в раздел IX, главу 28 «Преступления в сфере компьютерной информации». Изучите 5 статей УК РФ. Определите, что такое компьютерная информация и в каких случаях наказания за преступления ужесточаются.

Задание 12. Найдите, используя СПС «КонсультантПлюс», нормативные правовые акты, регламентирующие майнинг цифровой валюты.

Основные понятия и термины

Комитет Государственной Думы по безопасности и противодействию коррупции – структура в Государственной Думе Федерального Собрания Российской Федерации [1], в ведении которой находятся рассмотрение и подготовка законопроектов по вопросам безопасности государства и граждан.

Совет Безопасности Российской Федерации – совещательный орган, осуществляющий подготовку решений Президента Российской Федерации по вопросам обеспечения защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, проведения единой государственной политики по обеспечению национальной безопасности.

Служба внешней разведки Российской Федерации (СВР России) – основной орган внешней разведки Российской Федерации.

Министерство обороны Российской Федерации (Минобороны России) – федеральный орган исполнительной власти (федеральное министерство), проводящий государственную политику и осуществляющий государственное управление в области обороны, а также координирующий деятельность федеральных министерств, иных федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по вопросам обороны.

Министерство внутренних дел Российской Федерации (МВД России) – федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, а также по выработке государственной политики в сфере миграции.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) – федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы.

В области технической защиты информации ключевыми органами является ФСБ России и ФСТЭК России.

Совет Федерации и Государственная Дума, составляющие Федеральное Собрание Российской Федерации, разрабатывают законодательную базу страны. Основные федеральные законы, касающиеся обеспечения безопасности информации, представлены далее.

Сертификация – это процедура подтверждения соответствия результата производственной деятельности, товара, услуги нормативным требованиям, посредством которой третья сторона документально удостоверяет, что продукция, работа (процесс) или услуга соответствует заданным требованиям.

Сертификатом соответствия называется документ, подтверждающий соответствие сертифицированной продукции установленным требованиям. Срок его действия не должен превышать пяти лет.

Сертификация базируется на стандартах (технических регламентах), и в ее основе лежат испытания по нормам сертификации.

Система сертификации (организационная система сертификации) – второе по важности после сертификации понятие процедуры подтверждения соответствия. Термин «система сертификации», согласно Руководству ИСО/МЭК, определяется как «система, имеющая свои собственные правила, процедуры и руководства для проведения сертификации соответствия». Основным в этом определении является то, что сертификация в рамках системы должна проводиться по единым правилам и в определенном составе участников процесса сертификации.

Основной функцией сертификации является защита человека, его имущества и природной среды от отрицательных последствий современного научно-технического развития, от недобросовестных производителей и продавцов, создание условий для честной конкурентной борьбы.

Законодательством в целях обеспечения безопасности товаров (работ, услуг) предусматривается **обязательная сертификация**:

- товаров (работ, услуг), на которые в законодательных актах (технических регламентах), государственных стандартах установлены требования, направленные на обеспечение безопасности жизни, здоровья потребителей, охраны окружающей среды, а также на предотвращение причинения вреда имуществу потребителей;

- средств, обеспечивающих безопасность жизни и здоровья потребителей.

Добровольной сертификации подлежит продукция, на которую отсутствуют обязательные к выполнению требования по безопасности. В то же время ее проведение ограничивает доступ на рынок некачественных изделий за счет проверки таких показателей, как надежность, эстетичность, экономичность и др. При этом добровольная сертификация не подменяет обязательную, и ее результаты не являются основанием для запрета (поставки) продукции. Она в первую очередь направлена на борьбу за клиента и преследует маркетинговые цели. Это в полной мере касается и добровольной сертификации услуг.

Добровольная сертификация проводится на условиях договора между заявителем и органом по сертификации.

Основными органами сертификации в области технической защиты информации являются ФСБ России и ФСТЭК России. При этом ФСБ России действует в области криптографической защиты информации [18], а ФСТЭК России – в области технической защиты информации некриптографическими методами [13; 14; 15].

Вопросы и задания для оценки теоретических знаний

1. Перечислите задачи, которые необходимо решить для достижения цели информационной безопасности Российской Федерации.
2. Опишите основное содержание Доктрины информационной безопасности Российской Федерации.
3. Опишите основное содержание Стратегии национальной безопасности Российской Федерации.
4. Опишите основное содержание Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».
5. В чем суть Закона Российской Федерации от 21.07.1993 № 5485-1-ФЗ «О государственной тайне»?
6. Охарактеризуйте основное содержание Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
7. В чем заключается основное содержание Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»?
8. В чем заключается основное содержание Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»?
9. В чем заключается основное содержание Указа Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности»?
10. Сформулируйте понятие и приведите классификацию стандартов в области информационной безопасности.
11. Дайте характеристику стандартов группы ISO/IEC 27000.
12. Какие органы исполнительной власти являются ключевыми в области технической защиты информации?
13. Что такое сертификация? Что такое сертификат соответствия?
14. Дайте определение понятию системы сертификации.
15. Перечислите участников системы сертификации.
16. Дайте определение понятию обязательной и добровольной сертификации.
17. В соответствии с каким стандартом осуществляется сертификация системы управления (менеджмента) информационной безопасности?

4. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Вопросы для самостоятельного изучения:

4.1. Обеспечение кибербезопасности конечных устройств.

4.2. Основные способы защиты от вредоносного программного обеспечения при совершении кибератак на средства хранения, обработки и передачи данных.

Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы

При рассмотрении **первого вопроса** необходимо уяснить, какие устройства выступают в качестве конечных, их основные свойства и связанные с ними уязвимости.

Конечные устройства – это устройства, способные подключаться к сети Интернет и работающие с компьютерным аппаратным обеспечением через сеть. Конечные устройства в информационно-коммуникационных технологиях – это общий термин для устройств, подключенных к сетевому терминалу сети передачи данных или телекоммуникационной сети [34].

Задание 1. Перечислите примеры конечных устройств.

Архитектура EDR-решений

Обнаружение инцидентов на конечных устройствах и реагирование на них (EDR) – это растущая область, в которой решения для обеспечения безопасности конечных устройств пользуются большим спросом, что обусловлено расширением традиционных корпоративных сетей с централизованным управлением [11; 22].

В общем случае система класса Endpoint Detection & Response состоит из агентов, устанавливаемых на конечные точки, и серверной части. Агент ведет мониторинг запущенных процессов, действий пользователя и сетевых коммуникаций и передает информацию на локальный сервер или в облако [39; 40].

Серверный компонент анализирует полученные данные при помощи технологий машинного обучения, сопоставляет их с базами индикаторов компрометации (IoC) и другой доступной информацией о сложных угрозах. Если EDR-система обнаруживает событие с признаками киберинцидента [13], она оповещает об этом сотрудников службы безопасности (см. рис. 4.1).

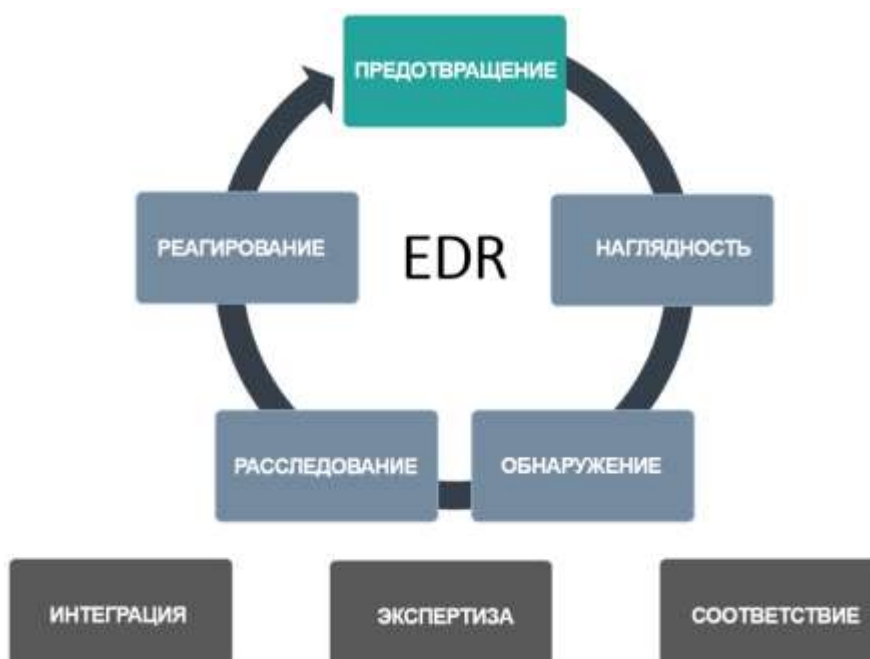


Рисунок 4.1. Основные функциональные блоки решений класса EDR

Наглядность. Детальный мониторинг всех процессов, запущенных на рабочих станциях и серверах, а также их взаимодействие, например с исполняемыми файлами и корпоративными приложениями, позволяют получать наглядную картину всего происходящего. В случае инцидента можно проверить эти данные и понять, на каких пользователей была направлена атака и какая информация могла пострадать.

Обнаружение. Крайне важно обнаружить развивающуюся атаку как можно быстрее, до того, как она нанесет серьезный ущерб. Решения EDR позволяют обнаружить сложносоставные атаки на их ранних стадиях при помощи комбинации различных механизмов поиска и методов анализа неизвестных угроз, в том числе построенных на базе машинного обучения и поведенческого анализа.

Расследование. Быстрый доступ ко всем данным с конечных точек и к информации об активностях позволяет аналитикам выполнять комплексное расследование и глубокий анализ источников угроз.

Реагирование. Широкий набор инструментов позволяет специалистам по информационной безопасности просматривать события, оценивать масштаб нарушений и определять все затронутые конечные точки. В случае обнаружения вредоносной активности информация об инциденте оперативно передается администратору. Используя централизованную консоль управления, специалист может принять следующие ответные меры: остановка работающих вредоносных процессов; карантин файлов; изолирование зараженных рабочих станций; проведение необходимых удаленных действий с файлами и реестром; блокировка подключений конечных точек к злонамеренным доменам, URL- и IP-адресам; сбор криминалистических артефактов (образ оперативной памяти, образ жесткого диска); восстановление рабочих мест в предынфекционное состояние.

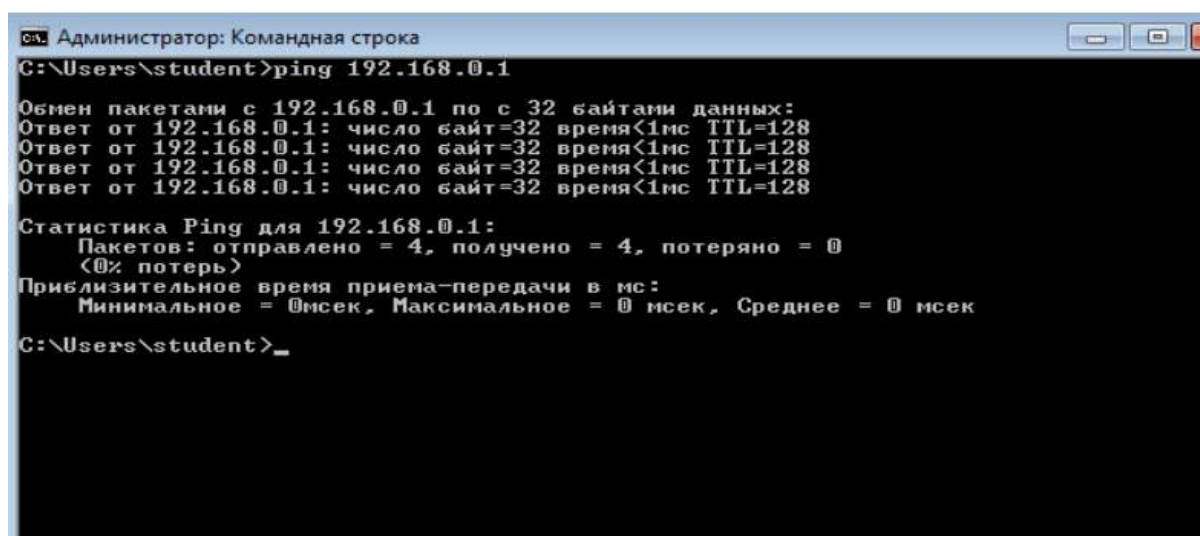
Предотвращение. Наличие решений класса EPP, построенных на базе превентивных технологий, ориентированных на обнаружение и автоматическую блокировку известных угроз, помогает устранить необходимость анализа большого количества инцидентов, которые не имеют отношения к сложным атакам, тем самым повышая эффективность EDR-платформ, направленных на обнаружение сложных угроз.

Интеграция. Решения по обнаружению сложных угроз на конечных точках и реагирования на них, кроме взаимодействия с решениями класса EPP, должны быть способны встраиваться в более широкую инфраструктуру информационной безопасности организаций. Поддержка возможности взаимодействия с существующими средствами информационной безопасности, например с системами по обнаружению сложных угроз на сети, с инструментами по расследованию и т.д.

Экспертиза. Важно иметь инструменты, необходимые для надлежащего обнаружения и реагирования. Усиление экспертизы внутри организации может строиться на прохождении различных обучающих программ по повышению квалификации специалистов информационной безопасности, а также путем доступа к информационному порталу угроз, получения потоков данных об угрозах и различных аналитических отчетов, которые обычно предоставляют производители решений по противодействию передовым угрозам.

Соответствие. Решения данного класса призваны помочь организациям в соблюдении требований внутренних служб информационной безопасности, внешних регулирующих органов и действующего законодательства в сфере информационной безопасности.

Для проверки сетевого взаимодействия между оконечными устройствами, например IP-адреса компьютера, следует использовать команду `ipconfig` (см. рис. 4.2). Если добавить переключатель `/all` в команду `ipconfig`, появится дополнительная информация: информация о DNS, MAC (контроль доступа к мультимедиа) (в поле «Физический адрес») и другая информация о каждом сетевом компоненте.



```
Администратор: Командная строка
C:\Users\student>ping 192.168.0.1

Обмен пакетами с 192.168.0.1 по 32 байтами данных:
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\student>_
```

Рисунок 4.2. Выполнение команды `ping`

Задание 2. Выведите диагностическую информацию о конфигурации сети TCP/IP при помощи командной строки и утилиты `ipconfig`.

Ipconfig – это утилита, которая позволяет просмотреть текущую конфигурацию IP-адресов компьютеров сети.

Синтаксис утилиты **ipconfig**:

`ipconfig [/all | /renew [адаптер] | /release [адаптер]]`,

где `all` выводит сведения о имени хоста, DNS (Domain Name Service), типе узла, IP-маршрутизации и др. Без этого параметра команда `ipconfig` выводит только IP-адреса, маску подсети и основной шлюз;

`/renew [адаптер]` обновляет параметры конфигурации DHCP (Dynamic Host Configuration Protocol – автоматическая настройка IP-адресов). Эта возможность доступна только на компьютерах, где запущена служба клиента DHCP. Для задания адаптера используется имя, выводимое командой `ipconfig` без параметров;

`/release [адаптер]` очищает текущую конфигурацию DHCP. Эта возможность отключает TCP/IP на локальных компьютерах и доступна только на клиентах DHCP. Для задания адаптера используется имя, выводимое командой `ipconfig` без параметров. Эта команда часто применяется перед перемещением компьютера в другую сеть. После использования утилиты `ipconfig /release` IP-адрес становится доступен для назначения другому компьютеру.

Запущенная без параметров команда `ipconfig` выводит полную конфигурацию TCP/IP, включая IP-адреса и маску подсети.

Пример использования **ipconfig** без параметров:

`C:\Documents and Settings\Администратор>ipconfig`

Задание 3. Проверьте соединение с удаленным хостом при помощи команды `ping`.

Пример использования утилиты **ping** с параметром:

`C:\Documents and Settings\Администратор>ping mail.ru`

Задание 4. Выведите имя локального компьютера (хоста) при помощи команды `hostname`.

Пример вызова команды **hostname**:

`C:\Documents and Settings\Администратор>hostname`

Второй вопрос предполагает рассмотрение рекомендаций по обеспечению кибербезопасности конечных устройств. В ходе раскрытия вопроса следует обратить особое внимание на виды вредоносных программ и меры противодействия им. Раскрывая содержание вопроса, нужно отметить, что без принятой в организации политики безопасности невозможно обеспечить эффективное противодействие угрозам. Должны быть разработаны все необходимые ру-

ководства пользователям, инструкции и методики для грамотной эксплуатации автоматизированных рабочих мест и информационной системы в целом.

По информации телеканала RT, американцы и англичане рассматривают диверсию на «Северных потоках» в качестве одного из многих методов продвижения своих экономических интересов. Под их удар могут попасть новые объекты инфраструктуры, в том числе морские оптоволоконные кабели, обеспечивающие связь во всем мире. С учетом того, что общая длина всех кабелей превышает 1,3 млн км, пространство для маневра, мягко говоря, огромное. Нарушение связи между континентами будет иметь серьезные последствия для мировой торговли и экономики в целом. И последствия эти могут быть сильнее, чем после подрыва «Северных потоков», поскольку разом пострадают от такой диверсии смогут целые континенты и десятки государств».

Однако влиять на компьютерные сети можно не только физически, ограничивая к ним доступ, достаточно использовать вредоносные программы, распространяемые в системах связи.

Задание 5. Проведите анализ актуальных угроз, представленных на веб-сайте Касперского.

Порядок выполнения задания:

5.1. Перейдите по ссылке на сайт Касперского <https://cybermap.kaspersky.com/> (см. рис. 4.3).

5.2. Проанализируйте веб-интерфейс, ознакомьтесь с пунктами меню.

5.3. Проанализируйте интенсивность атак в дружественных и недружественных странах (по 3 варианта). Сделайте выводы.

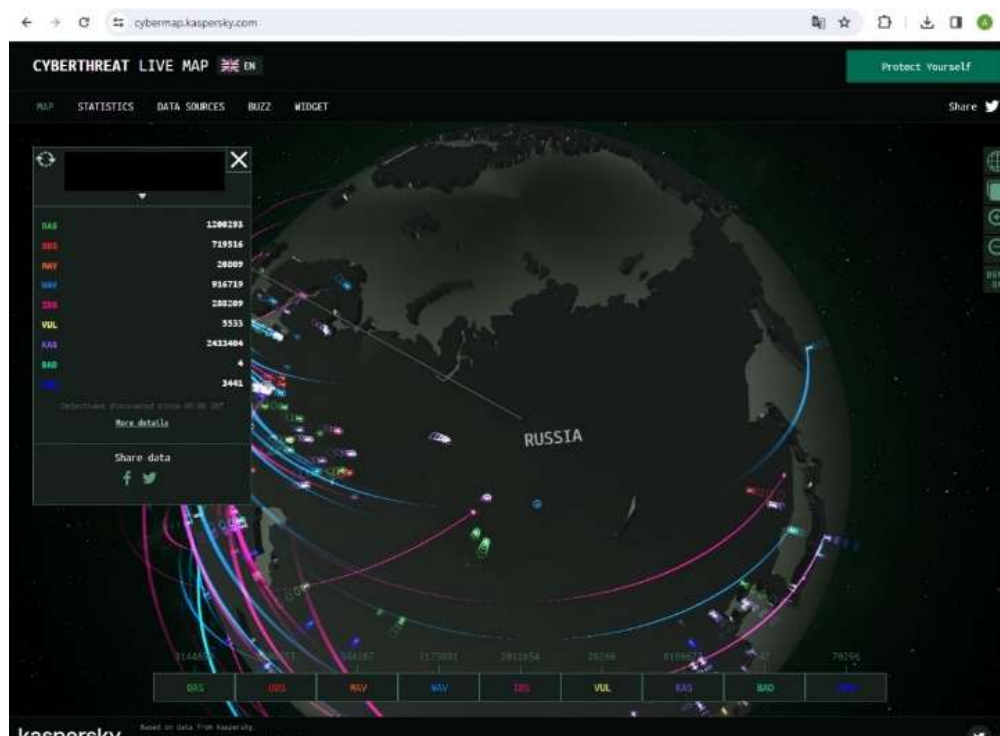


Рисунок 4.3. Веб-сайт Касперского

Задание 6. Заполните таблицу 4.1. Современные способы совершения кибератак. Приведите примеры вредоносных программ.

Таблица 4.1. Современные способы совершения кибератак

№	Название способа совершения кибератак	Описание способа совершения кибератак
1		Вид интернет-мошенничества, цель которого получение доступа к конфиденциальным данным пользователя (логинам и паролям). Пользователь думает, что переходит на заявленный сайт, однако фактически его перенаправляют на подставной сайт. Как правило, жертвами становятся клиенты банков и платежных систем [12]
2	Фишинговые сайты	
3	Вредоносная программа	
4		Тип вредоносных программ, основной целью которых является вредоносное воздействие по отношению к компьютерной системе. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблагоприятных целях
5	Сетевой червь	
6	Ботнет	
7		Программа может содержать различные вредоносные инструменты, такие как клавиатурный шпион, вор сохраненных паролей, сканер данных о банковских карточках [12], дистанционно управляемый бот для осуществления DDoS-атак, а также функции для отключения антивирусов. Некоторые примеры актуальных сегодня руткитов: TDSS, ZeroAccess, Alureon and Necurs
8	Отказ от обслуживания (DDoS-атака)	

Задание 7. Изучите алгоритм процесса реализации DDoS-атаки.

7.1. Отобразите расширение имен файлов. Для этого необходимо зайти в проводник (*Этот компьютер*). Выбрать пункт меню «Вид», в открывшейся вкладке выделить пункт «Расширение имен файлов» (см. рис. 4.4).

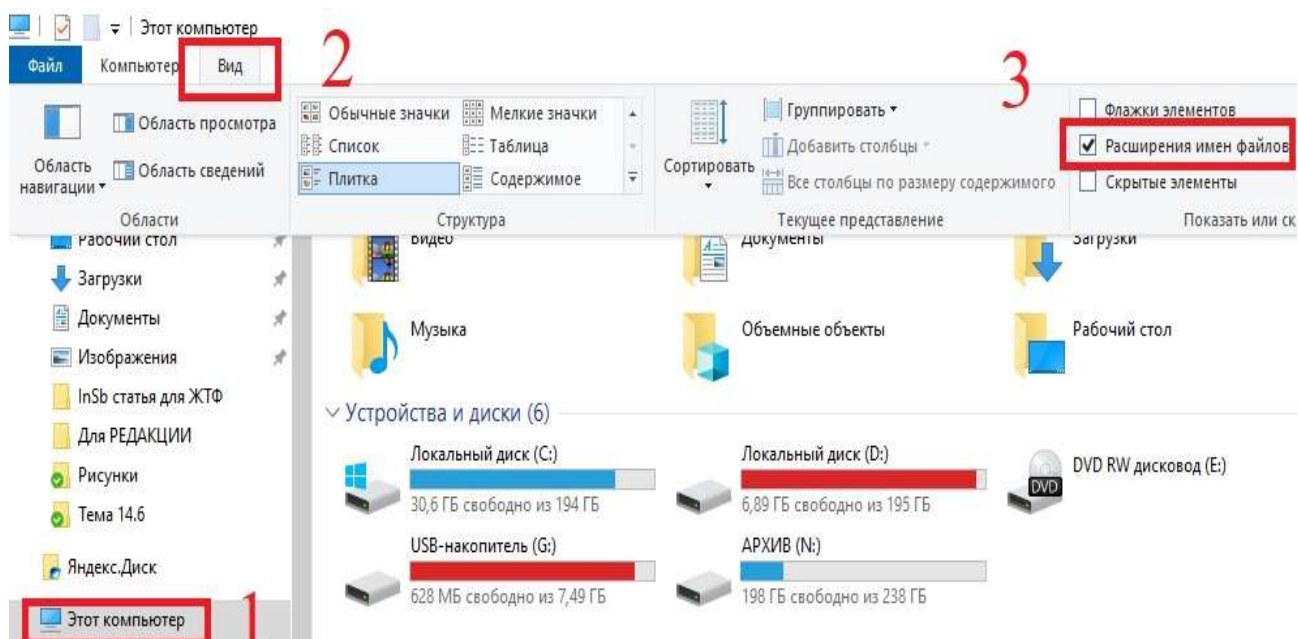


Рисунок 4.4. Окно проводника

7.2. Создайте файл Симулятор.txt.

На рабочем столе нажмите *правой кнопкой мыши*. В появившемся окне выберите пункт «Создать *текстовый документ*». Назовите его Симулятор.txt (см. рис. 4.5).



Рисунок 4.5. Файл блокнота

7.3. Наберите текст, приведенный на рис. 4.6, в файле Симулятор.txt и сохраните его.

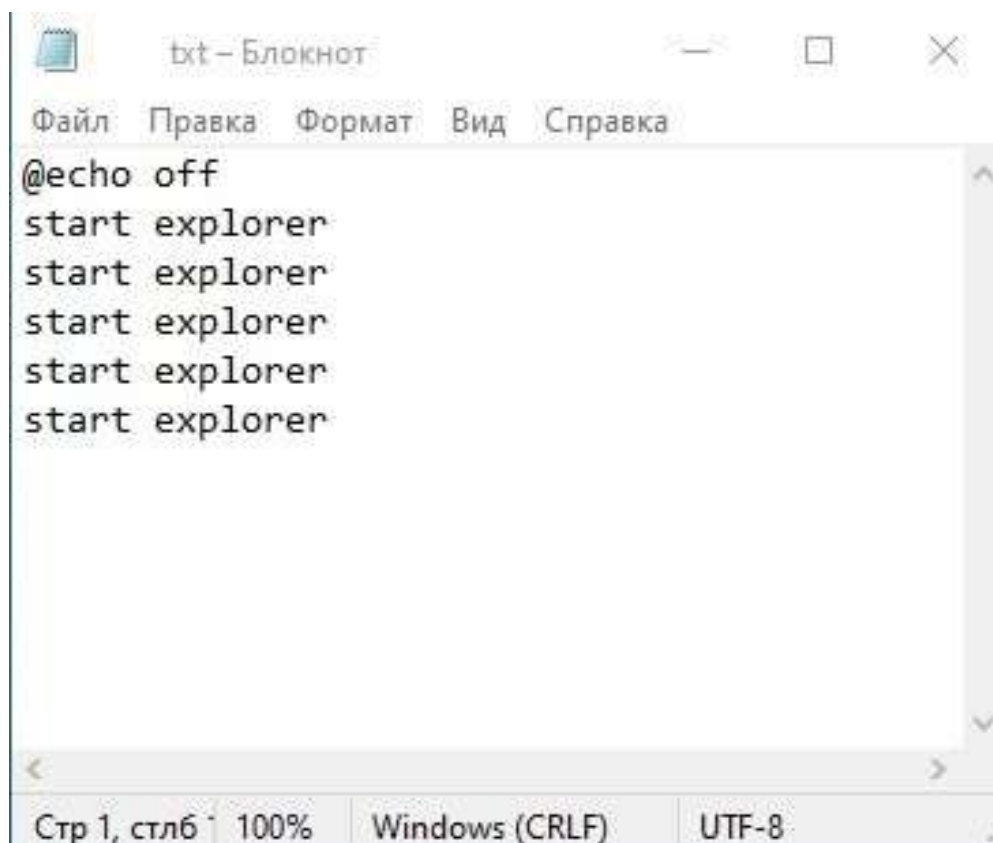


Рисунок 4.6. Текст в файле Симулятор.txt

7.4. Измените расширение файла Симулятор.txt на Симулятор.bat.

Для этого необходимо нажать правой кнопкой мыши на файл Симулятор.txt, изменить расширение на Симулятор.bat и подтвердить изменение (см. рис. 4.7).

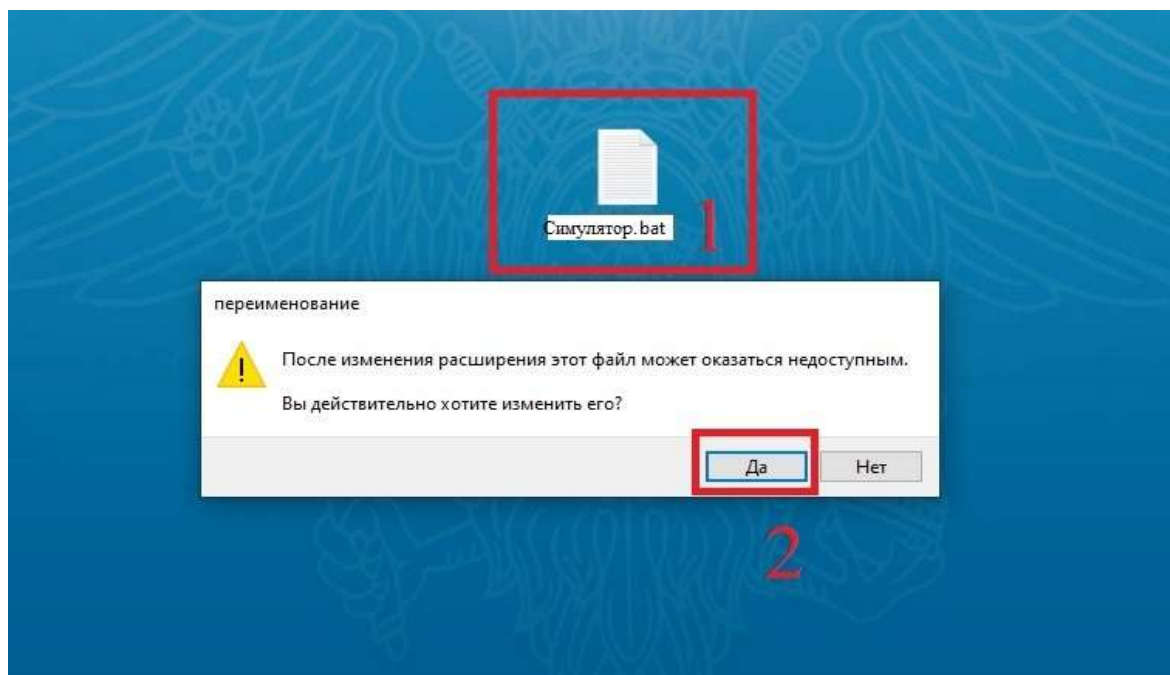


Рисунок 4.7. Смена расширения файла «Симулятор»

7.5. Запустите файл Симулятор.bat и проанализируйте результат (см. рис. 4.8).

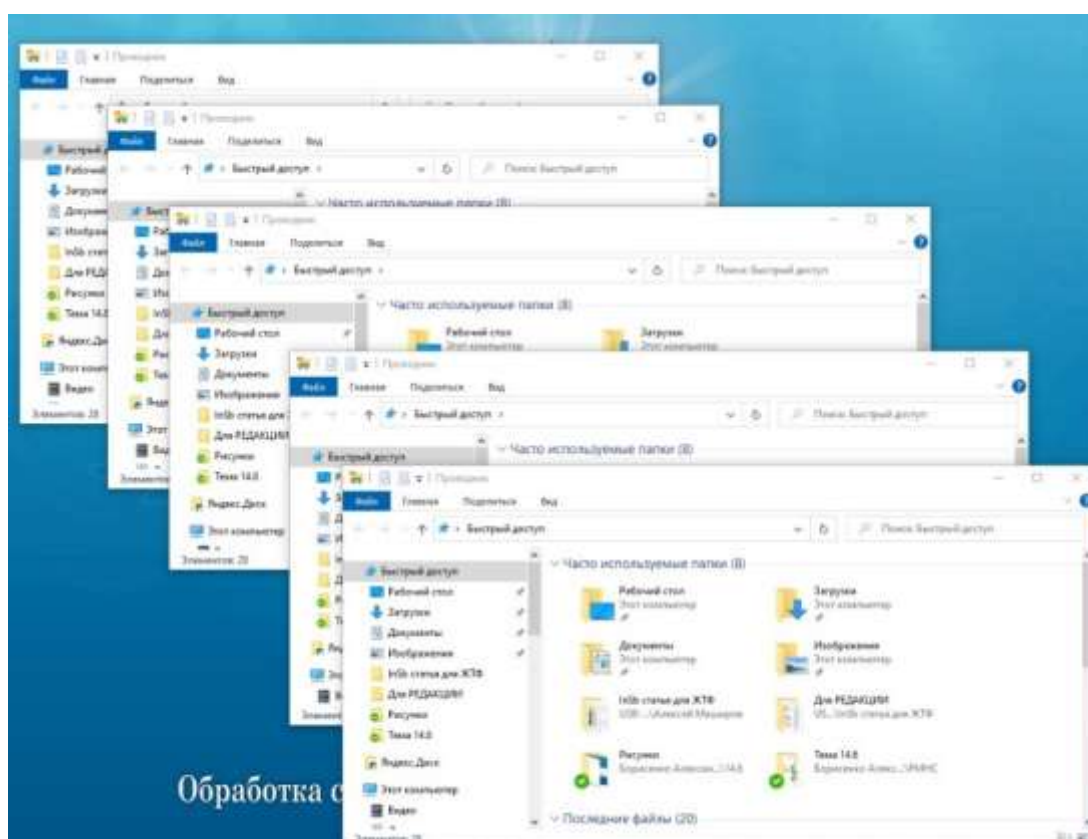


Рисунок 4.8. Результат выполнения файла «Симулятор»

7.6. Проанализируйте полученный результат. Сделайте и запишите выводы осуществления атаки типа «отказ в обслуживании».

Задание 8. Сформулируйте и запишите основные способы защиты от вредоносного программного обеспечения.

Основные понятия и термины

Брандмауэр – это программа, которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил.

Принципы, реализованные для правил обработки информации:

- использовать только те программы и файлы, которым доверяешь, происхождение которых известно;
- все данные, поступающие из внешних источников – с внешних носителей или по сети, тщательно проверять.

Принципы, реализованные для правил использования программ:

- использовать наиболее актуальные версии защитных программ;
- не мешать антивирусным и другим защитным программам выполнять свои функции.

Основополагающие принципы обеспечения безопасности сети:

- защита устройств, подключенных к сети;
- сетевые устройства должны быть стойкими к отказам и предусматривать возможность быстрого восстановления;
- пропускная способность сети должна непрерывно контролироваться;
- локальная сеть предприятия должна быть отказоустойчивой и предусматривать возможность быстрого восстановления в случае необходимости.

Вопросы и задания для оценки теоретических знаний

1. Что называют оконечными устройствами? Приведите примеры.
2. В чем заключаются причины некорректной работы антивирусной программы?
3. Укажите организационные методы обеспечения безопасности информации.
4. Укажите технические методы обеспечения безопасности информации (понятие).
5. Сформулируйте правила обработки информации.
6. Перечислите правила использования программ.
7. Сформулируйте понятие политики безопасности организации.
8. В чем состоит необходимость обновления используемых на компьютере программ?
9. Дайте определение понятию брандмауэра (межсетевого экрана).
10. Укажите средства защиты от нежелательной корреспонденции.
11. Перечислите принципы обеспечения безопасности сети.

5. ПОНЯТИЕ ОБ ИСТОЧНИКАХ И КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ

Вопросы для самостоятельного изучения:

5.1. Анализ угроз информации, обрабатываемой на объекте информатизации «Защищаемое помещение».

5.2. Разработка системы защиты информации объекта информатизации «Защищаемое помещение».

Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы

При рассмотрении **первого вопроса** необходимо определить угрозы информации, обрабатываемой на объекте информатизации «Защищаемое помещение».

Современный этап развития общества характеризуется значительным возрастанием понимания роли и актуальности проблемы обеспечения информационной безопасности во всех сферах деятельности общества. Научный прогресс, современные достижения в развитии информационных технологий заставляют задуматься о защите не только материальных объектов, но и информации как таковой. В связи с этим на первое место выходит сохранность информации, обрабатываемой в органах внутренних дел. Оперативная информация, имеющаяся в распоряжении подразделений органов внутренних дел, дает неоспоримые преимущества в борьбе со злоумышленниками. Но как только данная информация становится открытой, под угрозой оказывается безопасность самого подразделения, ведомства и национальная безопасность государства [4].

Задание 1. Дайте определение термина «объект информатизации». Приведите примеры объектов информатизации, предназначенных для обработки информации в органах внутренних дел.

Задание 2. Дайте определение терминов «основные технические средства обработки информации (ОТСС)» и «вспомогательные технические средства обработки информации (ВТСС)». Приведите примеры ОТСС и ВТСС.

Задание 3. Составьте описание **защищаемого помещения** территориального органа МВД России (этаж, площадь, наличие окон, батарей и т.д.) и нарисуйте **структурную схему**.

Рассматриваемый объект является теоретическим макетом помещения для ведения конфиденциальных переговоров, на базе которого возможно построение реальной системы защиты речевой информации от утечки по акустическому каналу связи.

Пример выполненного задания.

Защищаемое помещение находится на втором этаже здания. Доступ в защищаемое помещение осуществляется через входную дверь, оборудованную магнитоуправляемым извещателем открытия двери, который ограничивает круг лиц, имеющих доступ к данному объекту. В помещении находится ВТСС. Окно 1 шт. – не открывающееся, напротив от входной двери (см. рис. 5.1).

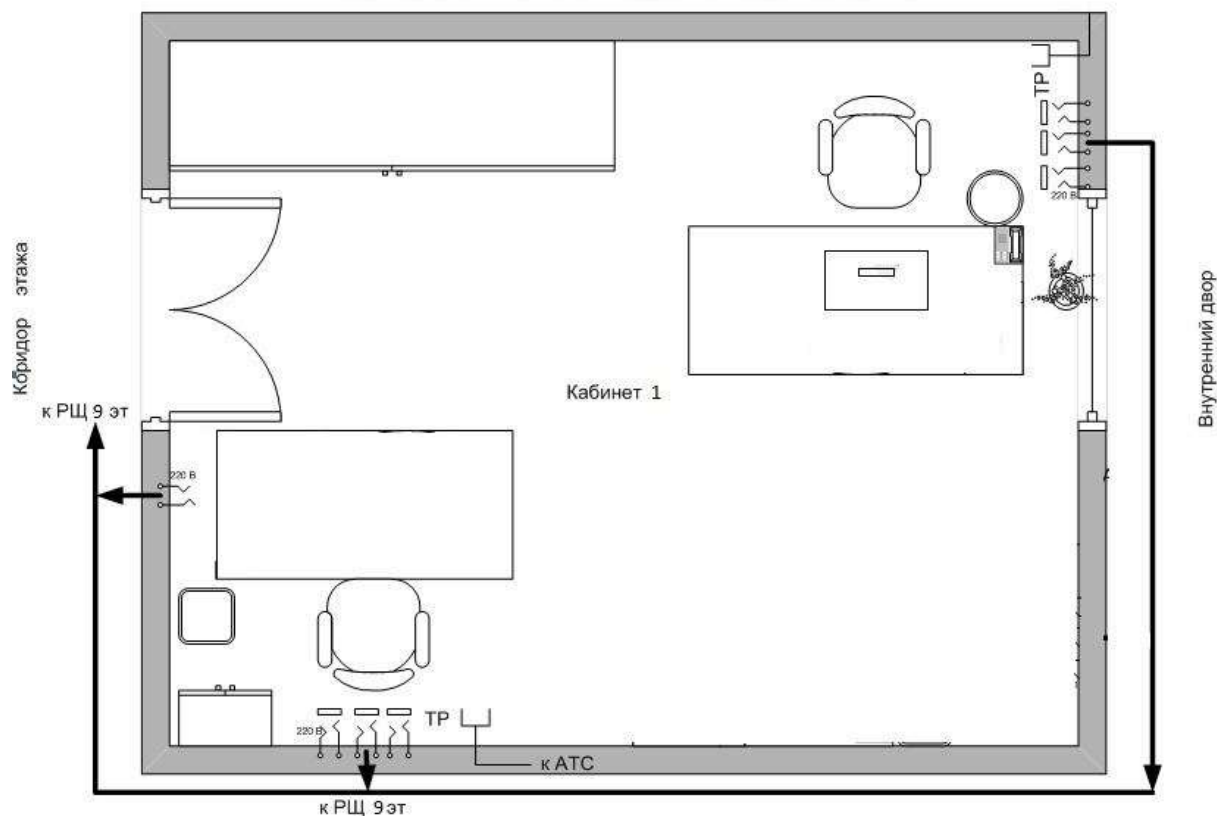


Рисунок 5.1. Схема защищаемого помещения

При рассмотрении **второго вопроса** важно разработать систему защиты информации объекта информатизации «Защищаемое помещение».

В том случае, когда источником информации является голосовой аппарат человека, информация называется речевой. Речевой сигнал – сложный акустический сигнал, основная энергия которого сконцентрирована в диапазоне частот от 300 до 3400 Гц. Голосовой аппарат человека является первичным источником акустических колебаний, которые представляют собой возмущения воздушной среды в виде волн сжатия и растяжения (продольных волн). Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания. Итак, в своем начальном состоянии речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний. Вторичными же источниками являются различного рода преобразователи акустических и вибрационных колебаний. К данным устройствам относятся громкоговорители, телефоны, микрофоны, акселерометры и др.

Задание 4. Изобразите структурную схему технического канала утечки информации.

Задание 5. Определите местоположение технических каналов утечки речевой информации (прямой акустический, виброакустический, электроакустический, оптико-электронный, параметрический) на **составленной схеме**.

Задание 6. Заполните таблицу, сопоставив технические каналы утечки информации и используемые технические средства.

Технические каналы утечки информации	Специальные технические средства, используемые для перехвата информации
1. Прямой акустический	
2. Виброакустический	
3. Электроакустический	
4. Параметрический	
5. Оптико-электронный	

а) лазерные акустические локационные системы, установленные в близлежащих строениях и на транспортных средствах, находящихся за границей контролируемой зоны;

б) электронные стетоскопы, установленные в смежных помещениях, принадлежащих другим организациям;

в) направленные микрофоны, установленные в близлежащих строениях и на транспортных средствах, находящихся за границей контролируемой зоны;

г) электронные устройства перехвата речевой информации с датчиками контактного типа, установленные на инженерно-технических коммуникациях (трубы водоснабжения, отопления, канализации, воздуховоды и т.п.) и внешних ограждающих конструкциях (стены, потолки, полы, двери, оконные рамы и т.п.) выделенного помещения, при условии неконтролируемого доступа к ним посторонних лиц;

д) специальные высокочувствительные микрофоны, установленные в воздуховодах или в смежных помещениях, принадлежащих другим организациям;

е) аппаратура «высокочастотного навязывания», подключаемая к соединительным линиям ВТСС, обладающим «микрофонным» эффектом, за пределами контролируемой зоны;

ж) электронные устройства перехвата речевой информации с датчиками микрофонного типа, установленные в воздуховодах, при условии неконтролируемого доступа к ним посторонних лиц;

з) специальные радиоприемные устройства, установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны, перехватывающие ПЭМИ на частотах работы высокочастотных генераторов, входящих в состав ВТСС, обладающих «микрофонным» эффектом;

и) аппаратура «высокочастотного облучения», установленная в ближайших строениях или смежных помещениях, находящихся за пределами контролируемой зоны;

к) прослушивание разговоров, ведущихся в выделенном помещении, без применения технических средств посторонними лицами (посетителями, техническим персоналом) при их нахождении в коридорах и смежных с выделенным помещениям (непреднамеренное прослушивание);

л) специальные низкочастотные усилители, подключаемые к соединительным линиям ВТСС, обладающим «микрофонным» эффектом, за пределами контролируемой зоны.

Задание 7. Определите активные и пассивные методы защиты речевой информации применительно к рассматриваемому объекту информатизации – **защищаемому помещению.**

Задание 8. Определите способы получения **видовой** информации по оптическим каналам утечки информации применительно к рассматриваемому объекту информатизации – **защищаемому помещению.**

Использование этих каналов получения информации часто сопряжено с неосторожностью владельца информационных активов. При внимательном отношении к хранению документов, перемещению секретного оборудования большинства рисков удастся избежать. Оптический сигнал распространяется в воздухе или безвоздушном пространстве, если съемка ведется со спутника.

Видеокамеры и фотоаппараты могут быть установлены в помещении и вне его, например в окнах соседнего здания, на спутниках, самолетах и дронах, на проезжающем транспорте, могут находиться при себе у посетителя офиса. Современные микроустройства автоматически фокусируются и настраиваются на резкость, использовать их могут непрофессионалы.

В практике конкурентных разведок используется три способа получения информации по оптическим каналам:

- наблюдение. Для него в целях улучшения видимости используются бинокли, телескопы, телевизионное оборудование. В ночное время применяются приборы ночного видения и тепловизоры. Полученное изображение передается на компьютер управления по прямому каналу или по радиосвязи;

- фотографирование объектов. Целью становятся здания, люди, секретное или являющееся ноу-хау компании оборудование, коллекции модных домов до показов, тайные переговоры и встречи. Разведчики и папарацци могут использовать микрофотоаппараты, закамуфлированные под аксессуары, и воспользоваться возможностями съемки со спутника;

- съемка документов. Для качественного разборчивого снимка нужна специальная фототехника, требующая опыта от использующего ее агента или инсайдера.

Задание 9. Определите методы защиты **видовой** информации по оптическим каналам утечки информации применительно к рассматриваемому объекту информатизации – **защищаемому помещению** и укажите их на схеме.

Задание 10. Используя таблицу «Государственный реестр сертифицированных средств защиты информации», размещенную на официальном сайте ФСТЭК России, определите **технические средства защиты речевой информации** от утечки по техническим каналам (прямой акустический, виброакустический, акустоэлектрический, оптико-электронный) применительно к рассматриваемому объекту информатизации – **защищаемому помещению** и разместите их на схеме.

Основные понятия и термины

Защита информации – это целенаправленная деятельность по предотвращению утечки защищаемой информации, а также по недопущению несанкционированных и непреднамеренных воздействий на нее.

Технический канал утечки информации (ТКУИ) представляет собой совокупность объекта разведки, технического средства разведки (ТСР), используемого для получения информации об этом объекте, и физической среды, в которой происходит распространение информационного сигнала.

Несанкционированный доступ к информации – это доступ к информации, осуществляемый с нарушением установленных правил разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Защита информации от утечки – это комплекс мер, направленных на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на создание существенных препятствий для получения защищаемой информации иностранными разведками и другими заинтересованными субъектами.

Защита информации от несанкционированного доступа – это защита информации, нацеленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами прав или правил разграничения доступа к защищаемой информации.

Техническая защита информации – это защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Вопросы и задания для оценки теоретических знаний

1. Сформулируйте свой подход к понятию «информационная безопасность».
2. В чем, с Вашей точки зрения, заключается необходимость защиты информации?
3. Дайте определение техническим каналам утечки информации.
4. В чем, с Вашей точки зрения, заключается сущность несанкционированного доступа к информации?
5. Какие меры, с Вашей точки зрения, направлены на предотвращение неконтролируемого распространения защищаемой информации?
6. В чем сущность технической защиты информации?
7. Сформулируйте свое видение безопасности информации.
8. Каким образом выделить защищаемый объект информатизации?
9. В чем заключается сущность угрозы безопасности информации?
10. Как определить демаскирующий признак объекта защиты?
11. В чем заключается принципиальная разница между понятиями «информационная безопасность» и «кибербезопасность»?
12. Определите фактор, воздействующий на защищаемую информацию.
13. Какая информация подлежит защите?
14. Классифицируйте информацию, подлежащую защите.
15. Перечислите задачи, которые необходимо решить для достижения цели информационной безопасности Российской Федерации.
16. Опишите основное содержание Доктрины информационной безопасности Российской Федерации.
17. Опишите основное содержание Стратегии национальной безопасности Российской Федерации.

6. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Вопросы для самостоятельного изучения:

6.1. Анализ угроз информации, обрабатываемой на объекте информатизации «Автоматизированное рабочее место сотрудника органов внутренних дел».

6.2. Разработка системы защиты информации объекта информатизации «Автоматизированное рабочее место сотрудника органов внутренних дел».

Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы

При рассмотрении **первого вопроса** необходимо определить угрозы информации, обрабатываемой на объекте информатизации «Автоматизированное рабочее место сотрудника органов внутренних дел».

Цифровизация всех сфер человеческой жизни предъявляет определенные требования к осуществлению правоохранительной деятельности в области информационной безопасности и поднимает вопросы актуализации обеспечения необходимого уровня информационной безопасности структурных элементов системы МВД России.

В рамках развития стратегий информационной безопасности выработаны средства и способы борьбы с каждым из видов технических каналов. Основные стандарты и технологии рекомендуют МВД России и ФСТЭК России [15]. Общеизвестно, что защита сложных телекоммуникационных систем определяется прежде всего комплексным подходом к созданию системы защиты информации. Безопасность информации, обрабатываемой на ведомственных объектах информатизации, обеспечивается применением организационных [30], технических [17] и правовых мер [7; 8], направленных на предотвращение ущерба интересам органов внутренних дел в результате нарушения конфиденциальности, целостности и доступности обрабатываемой информации.

Задание 1. Дайте определение термину «защита информации». Приведите основные виды защиты информации.

Задание 2. Составьте описание **автоматизированного рабочего места** сотрудника органов внутренних дел (этаж, площадь, состав АРМ, наличие элементов ОТСС и ВТСС) и нарисуйте **структурную схему**.

Рассматриваемый объект является теоретическим макетом помещения для ведения конфиденциальных переговоров, на базе которого возможно построение реальной системы защиты речевой информации от утечки по акустическому каналу связи.

Пример выполненного задания.

Автоматизированное рабочее место сотрудника органов внутренних дел находится на втором этаже здания. Доступ в помещение осуществляется через входную дверь, оборудованную магнитоуправляемым извещателем открытия двери, который ограничивает круг лиц, имеющих доступ к данному объекту. В помещении находятся элементы ОТСС и ВТСС. К ОТСС относится _____. К ВТСС относится _____. Окно 1 шт. – не открывающееся, расположено напротив входной двери (см. рис. 6.1).

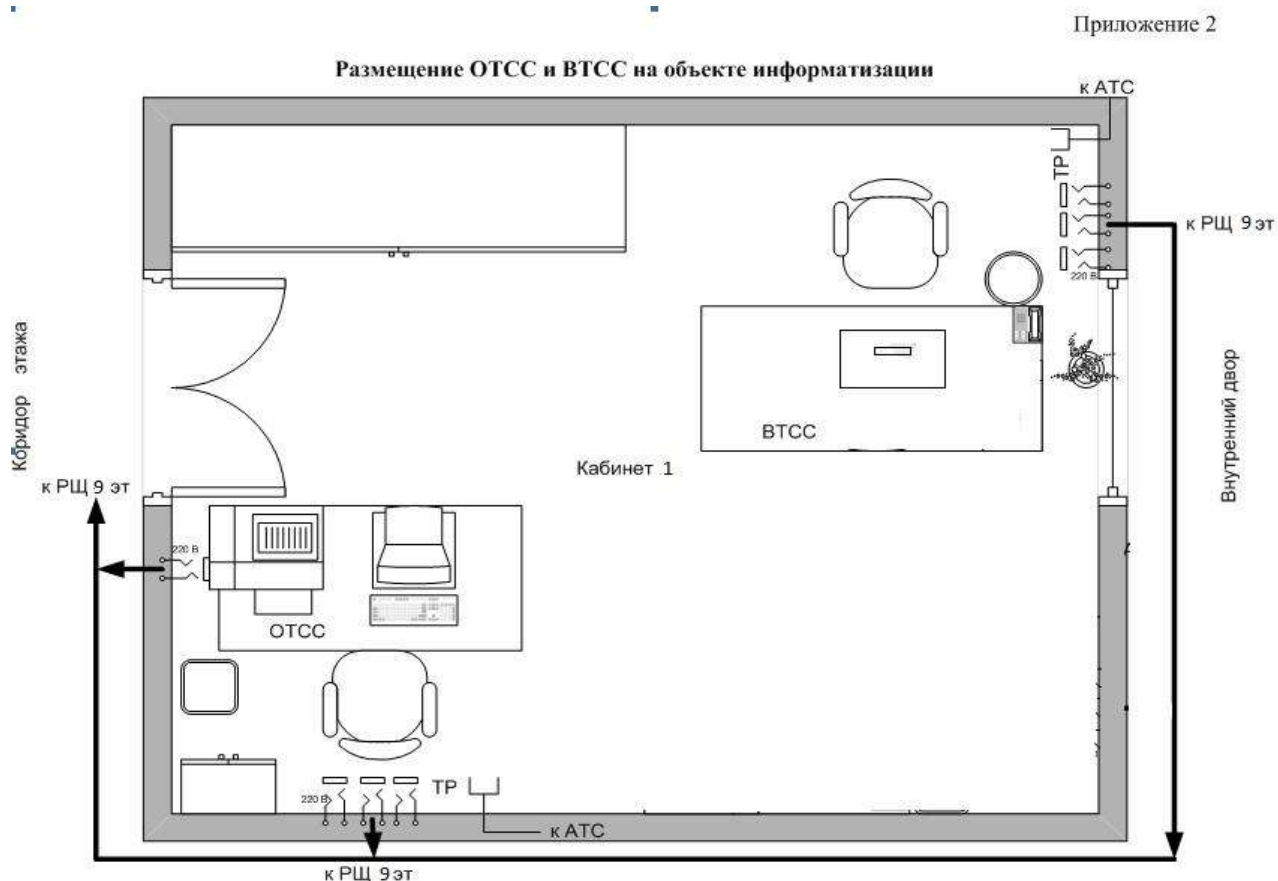


Рисунок 6.1. Схема защищаемого помещения

Задание 3. Составьте перечень угроз непосредственно для рассматриваемого объекта информатизации.

Для оценки защищенности объекта информатизации [20] от утечки информации через побочные электромагнитные излучения и наводки (ПЭМИН) используется программно-аппаратный комплекс «Навигатор-П5Г» (см. рис. 6.2).



Рисунок 6.2. Состав ПАК «Навигатор»

В ПАК «Навигатор» реализованы различные методы поиска ПЭМИН. Представленные методы отличаются по степени участия в них пользователя. Даже самые слабые сигналы должны исследоваться для достижения максимальной полноты и достаточности результатов. Их корректно возможно разобрать лишь оператору, обладающему достаточным опытом и профессиональной интуицией. Поэтому на практике удобнее пользоваться не одним методом, а комбинировать для получения наиболее точного результата исследования. Исследованию ПЭМИН подлежат различные элементы ПК. Однако практический опыт показал, что наибольшее излучение формирует монитор. Соответственно, обнаружив ПЭМИН монитора и выполнив мероприятия по защите информации от утечки по данному каналу, можно обеспечить защиту от утечки по каналу ПЭМИН других элементов и устройств. Порядок проведения работы состоит в последовательности выполнения следующих действий: поисковой этап и исследование ПЭМИН.

Результаты расчета зон R_2 , r_1 , r_1' для ОИ I категории, полученные с помощью ПАК «Навигатор», приведены в таблице 6.1.

Таблица 6.1. Результаты расчета R_2 , r_1 , r_1' для I категории

№	Интервал, МГц	Частоты, МГц	R_2 для стационарных средств, м	R_2 для во- зимых средств, м	R_2 для но- симых средств, м	r_1 , м	r_1' , м
1	0.0100000– 64.800710	32.400355	15.0	15.0	15.0	2.2	0.7
2	64.800710– 129.601420	97.201352	15.0	9.0	6.0	1.5	0.4
3	518.405680– 583.206390	550.808335	15.0	5.0	3.0		
4	583.206390– 648.007100	615.609333	30.0	10.0	5.0		
5	648.007100– 712.807810	680.313655	3.0	2.0	1.0		
Итого			30.0	15.0	15.0	2.2	0.7

Результаты расчета зон R2, r1, r1' для ОИ II категории, полученные с помощью ПАК «Навигатор», приведены в таблице 6.2.

Таблица 6.2. Результаты расчета R2, r1, r1' для II категории

№	Интервал, МГц	Частоты, МГц	R2 для стационарных средств, м	R2 для воздушных средств, м	R2 для носимых средств, м	r1, м	r1', м
1	0.0100000–64.800710	32.400355	9.0	9.0	9.0	1.6	0.6
2	64.800710–129.601420	97.201352	10.0	7.0	4.0	1.1	0.3
3	518.405680–583.206390	550.808335	8.0	3.0	2.0		
4	583.206390–648.007100	615.609333	15.0	5.0	3.0		
5	648.007100–712.807810	680.313655	2.0	2.0	1.0		
Итого			15.0	9.0	9.0	1.6	0.6

Результаты расчета зон R2, r1, r1' для ОИ III категории, полученные с помощью ПАК «Навигатор», приведены в таблице 6.3.

Таблица 6.3. Результаты расчета R2, r1, r1' для III категории

№	Интервал, МГц	Частоты, МГц	R2 для стационарных средств, м	R2 для воздушных средств, м	R2 для носимых средств, м	r1, м	r1', м
1	0.0100000–64.800710	32.400355	8.0	8.0	8.0	1.4	0.5
2	64.800710–129.601420	97.201352	8.0	6.0	4.0	0.9	0.2
3	518.405680–583.206390	550.808335	5.0	3.0	2.0		
4	583.206390–648.007100	615.609333	12.0	4.0	3.0		
5	648.007100–712.807810	680.313655	2.0	1.0	1.0		
Итого			12.0	8.0	8.0	1.4	0.5

Задание 4. Проанализируйте полученные результаты. Согласно исходным данным об объекте информатизации минимальное расстояние до границы контролируемой зоны составляет 14 м. Для какой категории объекта информатизации возникает необходимость применения средств защиты информации от утечки информации через побочные электромагнитные излучения и наводки?

При рассмотрении **второго вопроса** важно разработать систему защиты информации объекта информатизации «Автоматизированное рабочее место сотрудника органов внутренних дел».

К электромагнитным относятся каналы утечки информации, возникающие из-за наличия различного вида побочных электромагнитных излучений (ПЭМИ) ОТСС. Возникновение угрозы утечки по каналам ПЭМИ возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке информации в ОТСС [21].

Задание 5. Определите технические каналы утечки информации, обрабатываемой техническими средствами.

Задание 6. Составьте перечень возможных вариантов внедрения закладных устройств съема информации и опишите их принципы работы.

Задание 7. Определите пассивные методы защиты информации, обрабатываемой техническими средствами, применимые к рассматриваемому **автоматизированному рабочему месту** сотрудника органов внутренних дел.

Задание 8. Определите активные методы защиты информации, обрабатываемой техническими средствами, применимые к рассматриваемому **автоматизированному рабочему месту** сотрудника органов внутренних дел.

Пример сертифицированного ФСТЭК генератора белого шума «Соната-РС2», предназначенного для защиты объектов вычислительной техники от утечки информации за счет наводок на линии электропитания и заземления (см. рис. 6.3).



Рисунок 6.3. Генератор шума «Соната-РС2»

Существуют устройства блокирования работы системы цифровой связи и передачи данных. Например, «Квартет-2» (см. рис. 6.4) предназначено для блокирования работы устройств, использующих каналы цифровой связи стандартов: GSM-900, GSM-1800, E-GSM, IMT-MC-450 (NMT-450i), CDMA-2000, IMT-2000/UMTS (3G), DECT, Wi-Fi 2,4 ГГц, Bluetooth, 4G-LTE. Изделие представляет собой комплект модулей, выполненных в едином корпусе со встроенной антенной системой. Дальность подавления – 0...50 м.



Рисунок 6.4. Устройство блокирования работы системы цифровой связи и передачи данных «Квартет-2»

Задание 9. Используя устройства блокирования работы системы цифровой связи и передачи данных «Квартет-2», определите принципы защиты информации от утечки информации по радиоэлектронному каналу. Проанализируйте результаты функционирования устройства блокирования работы системы цифровой связи и передачи данных «Квартет-2».

Порядок выполнения задания.

На лицевой панели расположены ручки регулировки уровня сигнала, обозначенные латинскими буквами (А – F). Ручка «F» является также выключателем прибора. Рядом с выключателем размещен индикатор. Его свечение свидетельствует о работе прибора. Питание устройства осуществляется через адаптер от сети переменного тока 220 В. В зависимости от расстояния до ближайшей базовой станции сотовой связи дальность блокирования абонентских терминалов составляет до 25 м. Соответствие ручек регулировки, расположенных на лицевой панели изделия, различным стандартам связи указано в таблице 6.4. Ручки-регуляторы требуемых (блокируемых) диапазонов вращением по часовой стрелке выставляются в крайнее положение.

При необходимости радиус действия устройства уменьшается (для каждого диапазона отдельно) путем вращения ручек-регуляторов против часовой стрелки. Оценка радиуса действия проводится при использовании устройств цифровой связи соответствующих стандартов.

Если какой-либо стандарт не нуждается в блокировании, ручка- регулятор устанавливается в крайнее левое положение путем вращения против часовой стрелки.

Таблица 6.4. Технические характеристики «Квартет-2»

Обозначение диапазона	Стандарт связи	Частотный диапазон, МГц	Мощность*, Вт
A	NMT-450i, CDMA-2000	462,5–467,5	4,0
B	Wi-Fi 2,4 ГГц, Bluetooth	2400,0–2483,5	2,4
C	4G - LTE	2500,0–2700,0	2,4
D	IMT-2000/UMTS (3G)	2110,0–2180,0	3,5
E	GSM-900, E-GSM	925,0–960,0	4,0
F	GSM-1800, DECT	1805,0–1900,0	4,0

Изделие размещается в центре зоны, внутри которой необходимо блокировать работу радиотелефонов.

Для защиты помещений с большей площадью необходимо размещение нескольких блокираторов с расстоянием 20–40 метров между соседними устройствами.

Вариант размещения может быть как горизонтальным (на поверхности мебели), так и вертикальным (стены, строительные конструкции, мебель). Соедините адаптер с гнездом питания изделия (гнездо находится на задней панели прибора и обозначено знаком DC) и подключите адаптер к сети.

Задание 10. Определите методы защиты информации от несанкционированного доступа к информации для рассматриваемого **автоматизированного рабочего места** сотрудника органов внутренних дел.

Задание 11. Определите методы защиты информации от утечки информации по визуально-оптическому каналу для рассматриваемого **автоматизированного рабочего места** сотрудника органов внутренних дел.

Задание 12. Используя таблицу «Государственный реестр сертифицированных средств защиты информации», размещенную на официальном сайте ФСТЭК России [16], определите защиту **автоматизированного рабочего места сотрудника органов внутренних дел** от утечки по техническим каналам (электрическому, электромагнитному, визуально-оптическому); от осуществления несанкционированного доступа к информации.

Основные понятия и термины

В **радиоэлектронном канале** носителем информации является электрический ток и электромагнитное поле с частотами колебаний от звукового диапазона до десятков гигагерц.

В **радиоэлектронных каналах утечки информации** источниками сигналов могут быть:

- передатчики функциональных каналов связи;
- источники опасных сигналов;
- объекты, отражающие электромагнитные волны в радиодиапазоне.

Побочные электромагнитные излучения (ПЭМИ) – электромагнитные излучения технических средств, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях [21].

Параметрический ТКУИ образуется за счет «высокочастотного облучения» ОТСС.

Электрические каналы утечки образуются из-за просачивания информационных сигналов в цепи заземления и электропитания ОТСС, а также за счет наводок, которые мы рассмотрели ранее, на линии электропитания ВТСС и другие проводники, выходящие за пределы контролируемой зоны [32].

Выделяют три вида паразитной связи:

- емкостная – образуется в результате воздействия электрического поля;
- индуктивная – образуется в результате воздействия магнитного поля;
- гальваническая – через общее активное сопротивление.

Вопросы для оценки теоретических знаний

1. Что такое защита информации от несанкционированного доступа?
2. Что такое защищаемое помещение?
3. Дайте определение понятию контролируемой зоны.
4. Что такое основные технические средства и системы (ОТСС)?
5. Что такое вспомогательные технические средства и системы (ВТСС)?
6. Приведите примеры ОТСС.
7. Приведите примеры ВТСС.
8. Что такое канал связи?
9. Что представляет собой электромагнитный ТКУИ?
10. Что представляет собой электрический ТКУИ?
11. Что представляет собой индукционный ТКУИ?
12. Что такое стетоскоп?
13. Как классифицируют технические каналы утечки информации, обрабатываемой основными техническими средствами и системами?
14. Как образуется параметрический ТКУИ?
15. Как образуются электрические каналы утечки?
16. Дайте понятие акустоэлектрическим преобразователям.
17. Какие случайные акустоэлектрические преобразователи относятся к наиболее распространенным?
18. Назовите три вида паразитной связи.

7. ОСОБЕННОСТИ ОБРАЗОВАНИЯ СЛЕДОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Вопросы для самостоятельного изучения:

7.1. Криминалистические и уголовно-процессуальные особенности фиксации и изъятия цифровой информации.

7.2. Использование инструментов цифровой криминалистики в ходе расследования уголовного дела на первоначальном этапе.

Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы

При рассмотрении **первого вопроса** необходимо уяснить криминалистические и уголовно-процессуальные особенности фиксации и изъятия цифровой информации.

Задание 1. Укажите, как законодательно регулируется порядок изъятия электронных носителей информации и копирования с них информации при производстве следственных действий.

Задание 2. Определите действия следователя и специалиста в области информационно-коммуникационных технологий, которые должны приступить к осмотру компьютера.

Задание 3. Назовите, от чего зависит порядок осмотра компьютера.

Задание 4. Перечислите виды компьютерной экспертизы.

Во **втором вопросе** важно довести обучающимся, как использовать инструменты цифровой криминалистики в ходе расследования уголовного дела на первоначальном этапе [35].

Для проведения экспертизы данных и фиксации (изъятия) цифровой информации используется специализированное криминалистическое оборудование и программное обеспечение.

Для поиска и фиксации цифровых следов специалист использует апробированное экспертным сообществом лицензионное программное обеспечение. Например, можно применять программные комплексы «Мобильный криминалист», UFED Touch или XRY.

«**Мобильный криминалист**». Сегодня это одна из лучших программ для анализа данных, извлеченных из мобильных устройств. «Мобильный криминалист» – это многофункциональный инструмент для высокоскоростной и эффективной работы с данными из мобильных устройств, дронов, облачных сервисов и ПК.

Программа поддерживает извлечение информации из широкого ряда цифровых источников, среди которых:

1. Более 40 000 смартфонов и планшетов различных брендов (Apple, Samsung, Huawei и др.) под управлением iOS, Android и KaiOS, а также карты памяти и сим-карты.

2. Персональные компьютеры под управлением Windows, macOS и GNU/Linux, физические образы жестких дисков в форматах E01, EX01, RAW (DD, BIN, IMG, 001, 000, 0000, 0001), DMG, ISO; логические образы ПК в форматах L01, LX01, AD1, ZIP, 7Z, RAR, TAR; файлы виртуальной машины VirtualBox, VMware; диски виртуальной машины в форматах VDI, VHD, VMDK, а также резервные копии Time Machine для macOS. Поддерживаемые файловые системы: NTFS, FAT16, FAT32, EXFAT, EXT2, EXT3, EXT4, HFS, HFS+ и APFS.

3. Более 700 уникальных приложений и больше 34 000 их версий: WhatsApp, Telegram, TenChat, Signal, Silent Phone, Zoom, Wickr Pro, Spark, Burner, Kufar, ДругВокруг, Runkeeper, GiveAway, Craigslist и др.

Для того чтобы извлечь информацию из мобильного устройства, необходимо запустить модуль «Мастер извлечения данных» (см. рис. 7.1), выбрав соответствующий блок на домашнем экране программы (вызывается кликом по значку домика в левом верхнем углу) или соответствующий пункт в выпадающем меню (вызывается кликом по иконке в виде двух горизонтальных линий и стрелки под ними в верхнем правом углу).

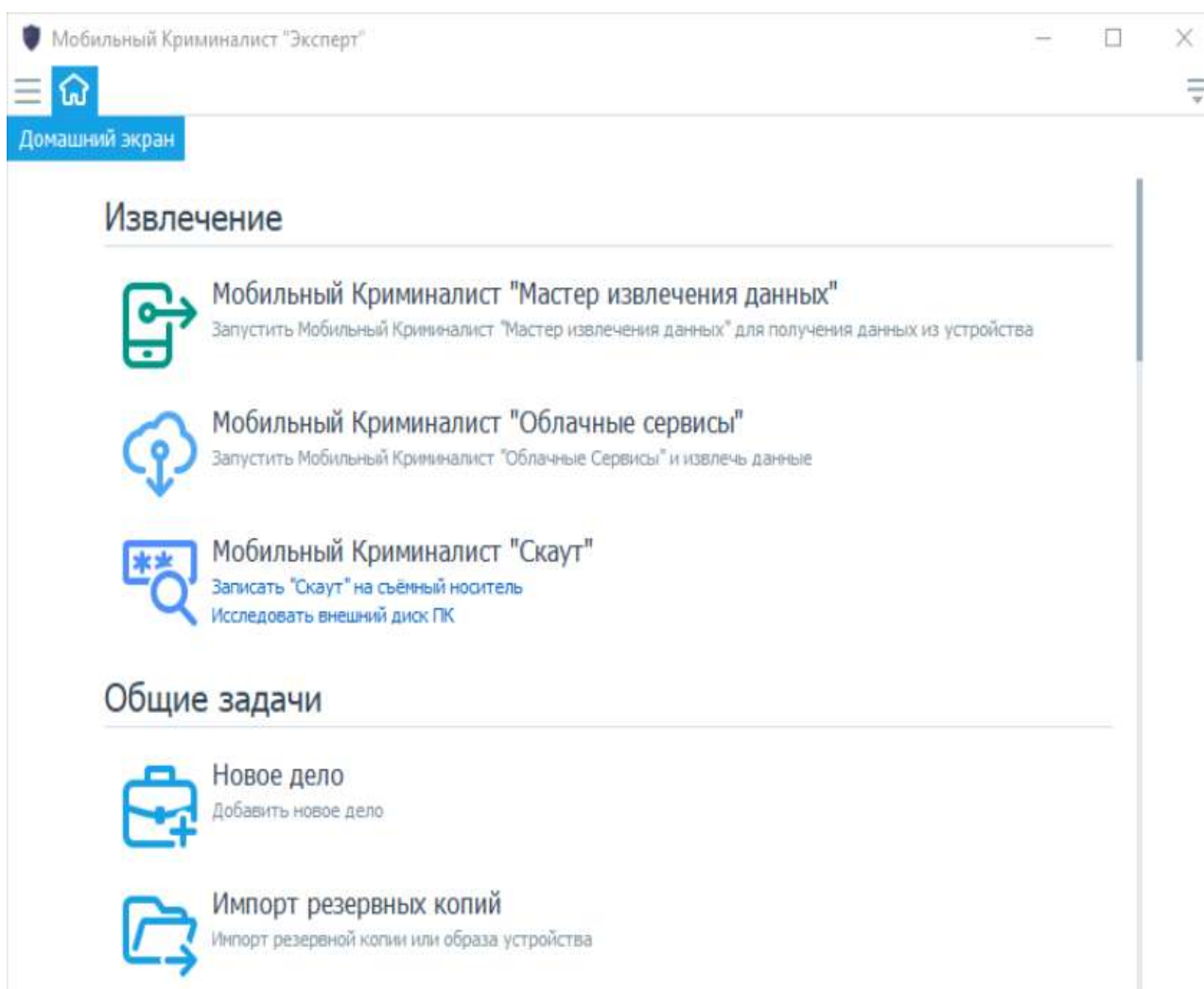


Рисунок 7.1. «Мастер извлечения данных»

Далее для работы с устройством в появляющемся окне необходимо выбрать метод извлечения. В модуле все методы разделены на блоки: iOS-извлечения, Android-извлечения и другие извлечения (см. рис. 7.2).

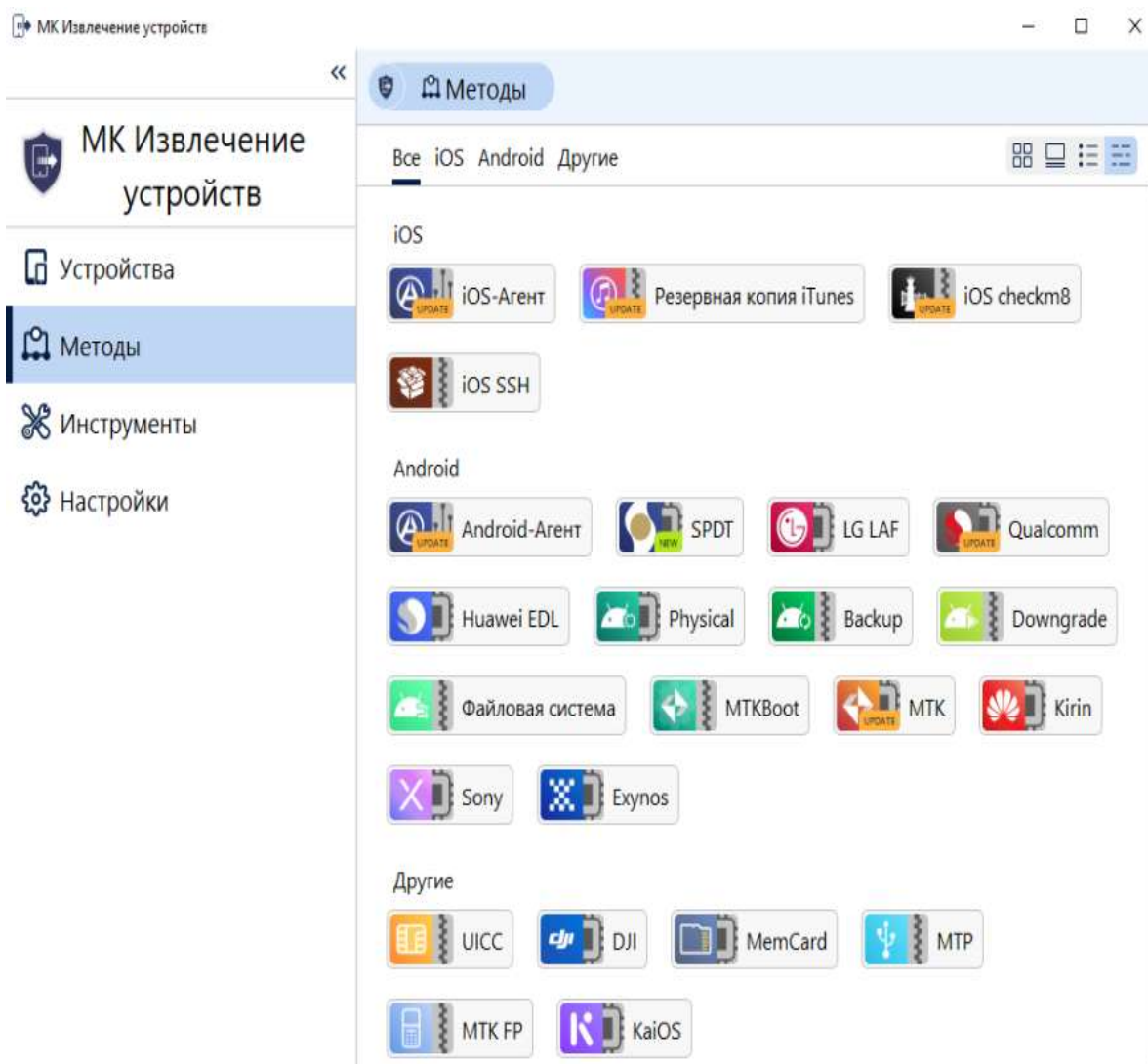


Рисунок 7.2. Метод извлечения

«Мобильный криминалист» восстановит все необходимое сразу после снятия физического образа и продемонстрирует всю переписку, включая удаленные сообщения, по результатам анализа извлеченных данных.

При нажатии на «Просмотр извлеченных данных» в «Мобильный криминалист-эксперт» будет доступна форма с различными инструментами для последующего анализа данных (см. рис. 7.3).

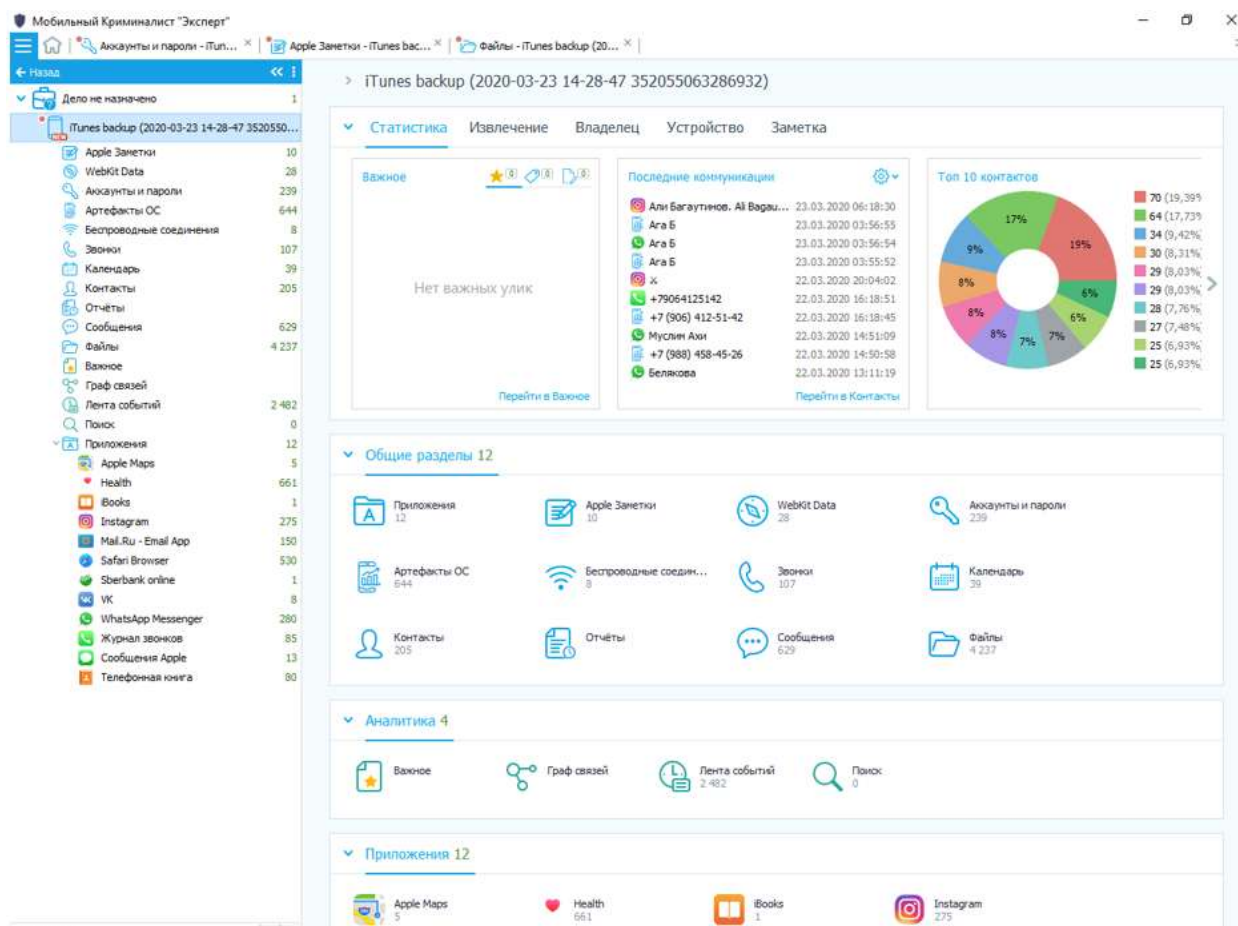


Рисунок 7.3. Форма просмотра извлеченных данных

Для проведения аппаратно-компьютерной и программно-компьютерной экспертизы информации используется специальное программное обеспечение, например программные утилиты. Примером такой программы может служить **AIDA64**.

AIDA64 – приложение (утилита), позволяющее идентифицировать все компоненты персонального компьютера, который управляется Windows. Утилита предоставляет исчерпывающую информацию об аппаратной составляющей, программном обеспечении и текущем состоянии компьютера (данные с огромного количества датчиков). Приложение позволяет тестировать железо, проводить диагностику мониторов и осуществлять проверку системы на устойчивость при длительной работе под значительной нагрузкой.

Интерфейс состоит из нескольких функциональных частей (см. рис. 7.4):

- главного меню, предоставляющего доступ ко всем функциям, которые дублируются посредством выпадающих контекстных меню;
- вкладки в виде дерева, где можно выбрать необходимый инструмент;
- окна с информацией;
- панели инструментов.

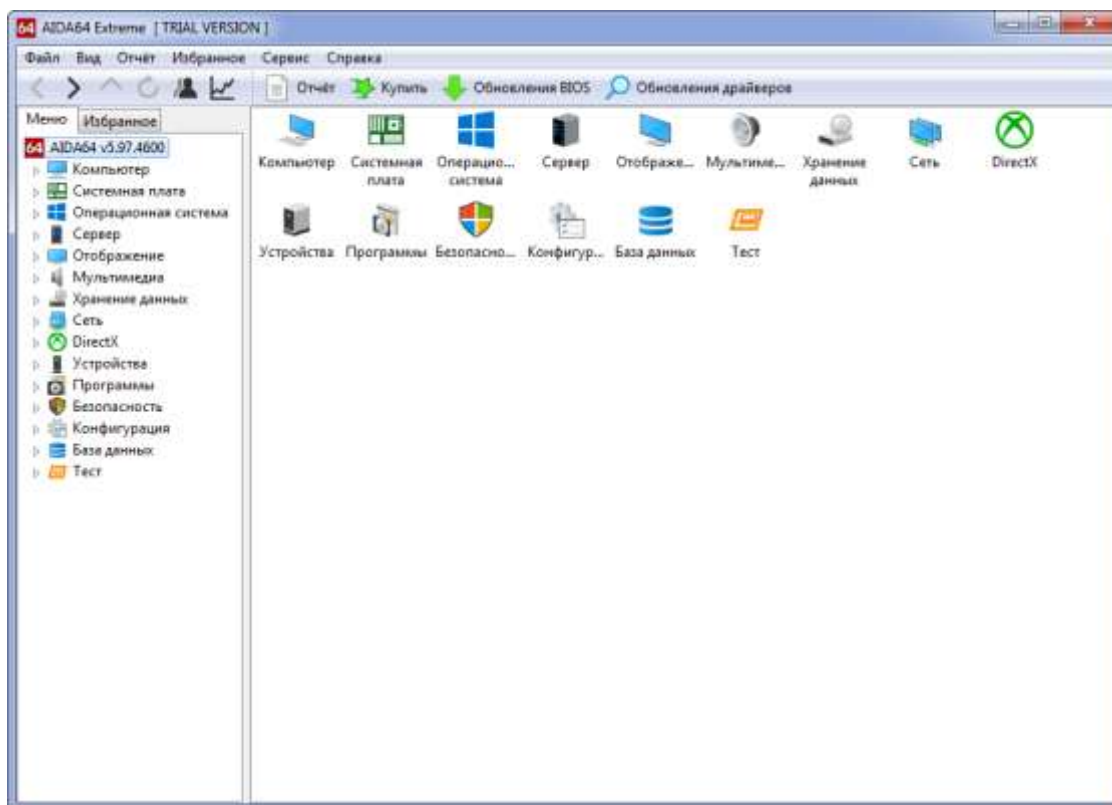


Рисунок 7.4. Интерфейс программного средства

Компьютер – здесь отображается суммарная информация о вашей машине, данные со всех датчиков и основные сведения о конфигурации, все запротоколированные системные события, отчеты об ошибках и предупреждениях, сведения о разгоне, если он осуществлялся.

Системная плата – все о материнской плате, ее спецификации, чипсете, оперативной памяти и центральном процессоре, а также BIOS.

Операционная система – больше данных об используемой ОС. Вы не найдете даже в штатном диспетчере задач. Здесь находятся данные обо всех программах, процессах, службах, драйверах устройств, динамических библиотеках, сертификатах безопасности и многое другое, в том числе статистика работы ОС: когда была установлена, сколько находилась в работе.

Сервер – касается использования сети (различные ресурсы, группы, в которых состоит учетная запись, информация о созданных аккаунтах).

Отображение – профессиональный информационный модуль для извлечения данных о графической составляющей:

- сведения о мониторе, графическом ускорителе и его компонентах (память, процессор);
- используемые драйверы;
- свойства и эффекты проводника;
- поддерживаемые видеорежимы и технологии (CUDA, PhysX, DirectX) и все о них.

Мультимедиа содержит данные о звуковой подсистеме компьютера, в том числе установленные кодеки и используемые аудиоустройства.

Хранение данных – перечень характеристик и текущего состояния устройств для долговременного хранения цифровой информации: физические, логические, съемные, оптические (дисководы), сетевые, а также SMART-данные.

Сеть – сведения о сетевой карте, используемые в сетях и ресурсах, Интернете, портах.

Устройства – дополнительная информация о физических, логических устройствах, PCI и USB.

Программы – показывают автозагрузку, установленный на ПК-софт, содержимое планировщика заданий, присутствующие на компьютере лицензии и зарегистрированные расширения файлов.

Каждый из разделов предоставляет отдельный спектр информации о компьютере. Кратко узнать параметры, производителя и модель своей системной платы можете в разделе «Компьютер», в ветке «Суммарная информация» (см. рис. 7.5).

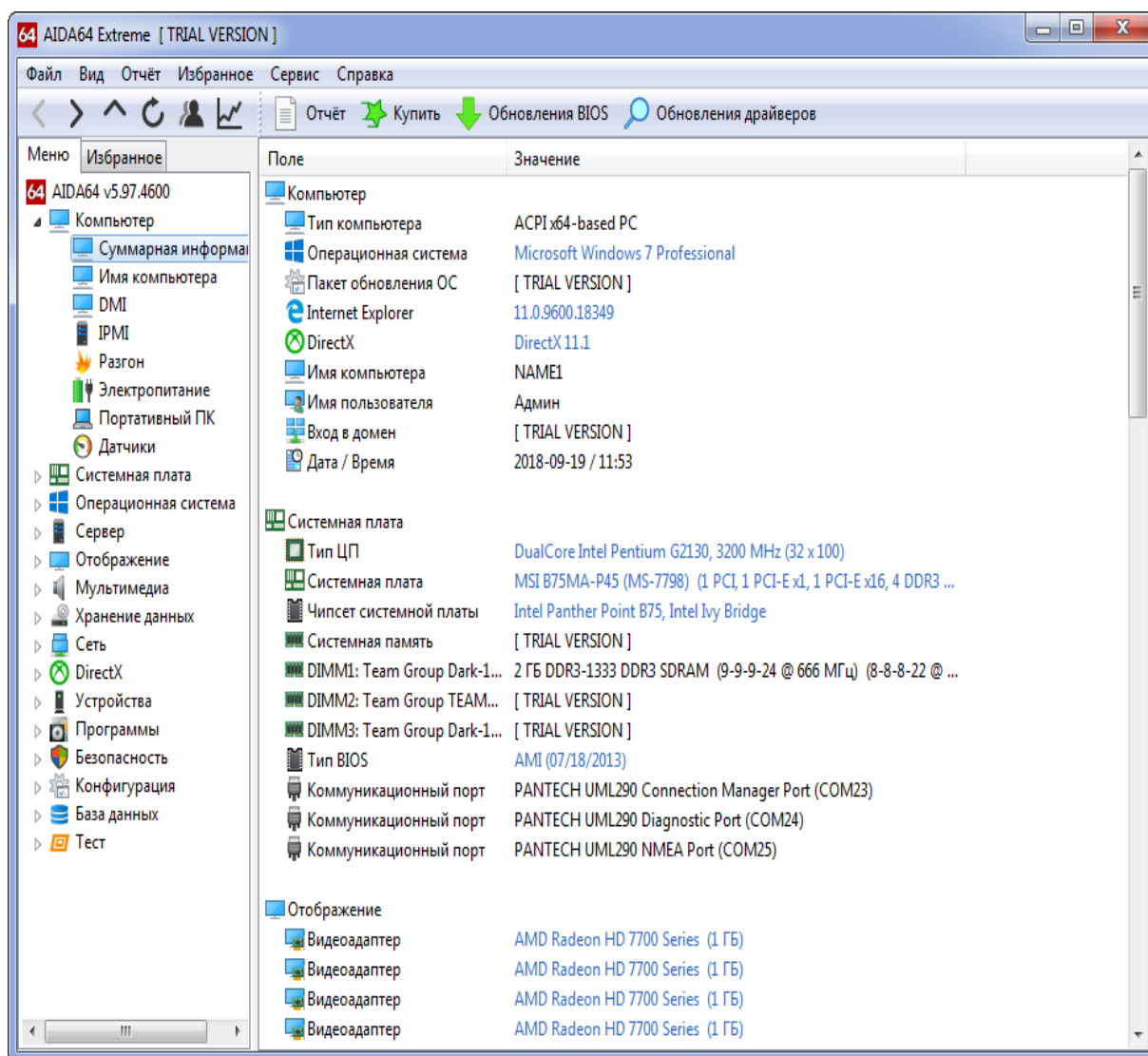


Рисунок 7.5. Суммарная информация

Для большинства случаев этого вполне достаточно, даже если хотите подобрать новый центральный процессор. В следующем разделе уже приводится на порядок больше характеристик про материнскую плату (см. рис. 7.6.1).

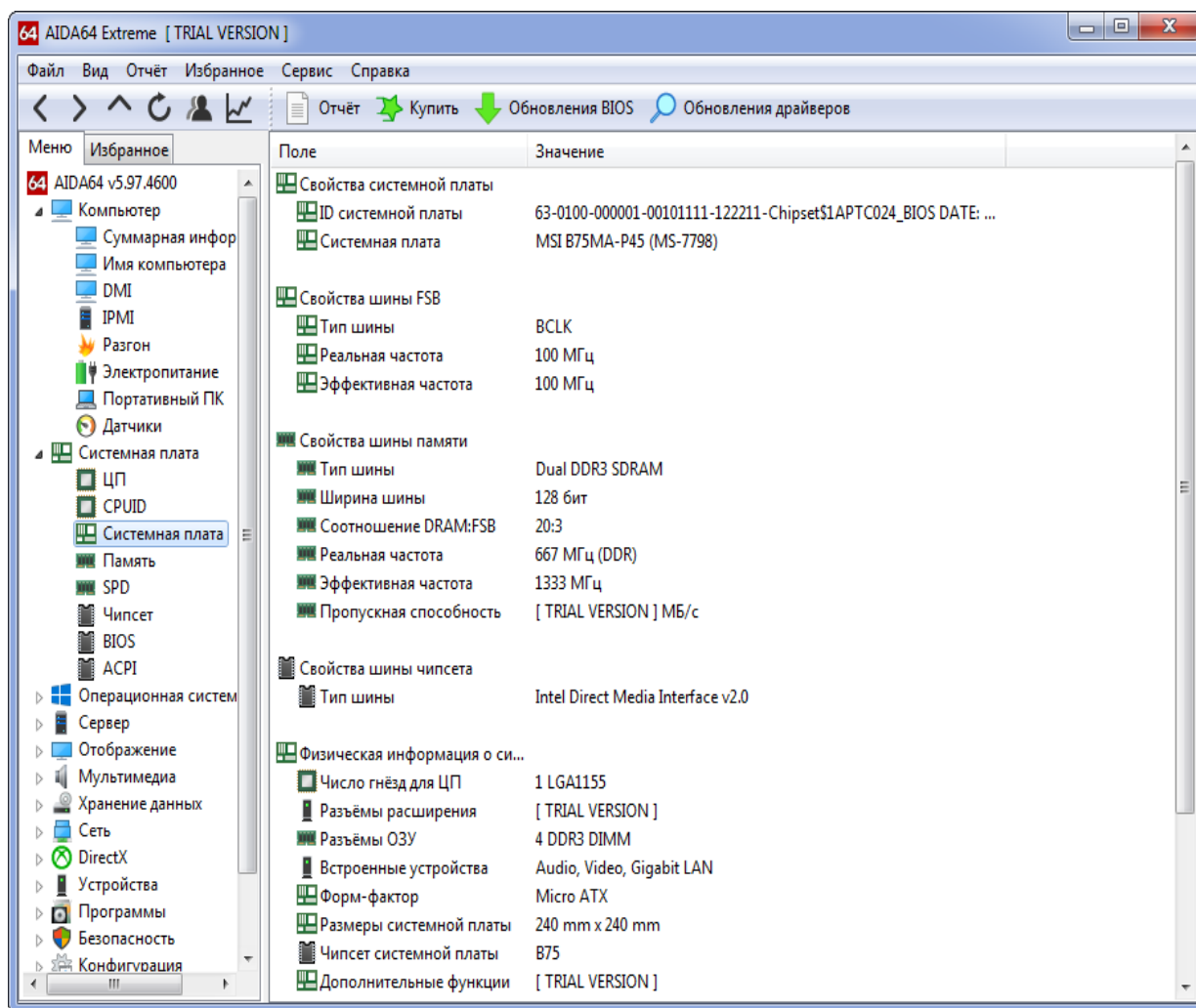


Рисунок 7.6.1. Информация об оборудовании

Видеокарта. Через AIDA64 можно не только модель своей видеокарты узнать, но и увидеть, из какого количества транзисторов она состоит. Заходим в раздел «Отображение». В первой ветке увидим основные данные о видеосистеме, а в разделе «Графический процессор» – уже огромный перечень характеристик (см. рис. 7.6.2).

Оперативная память. Наряду с двумя предыдущими девайсами оперативная память является тем компонентом, о параметрах которого должен знать любой геймер (хотя бы объем и частоту). Все это и намного больше можно отыскать в ветке SPD в разделе «Системная плата» (см. рис. 7.6.3).

Температура. AIDA 64 позволяет узнать температуру центрального процессора, видеокарты и иных составляющих ЭОМ. При подозрении на перегрев какого-либо компонента или его разгон эти сведения важны. Они находятся в ветке «Датчики» в первом разделе программы (см. рис. 7.6.4).

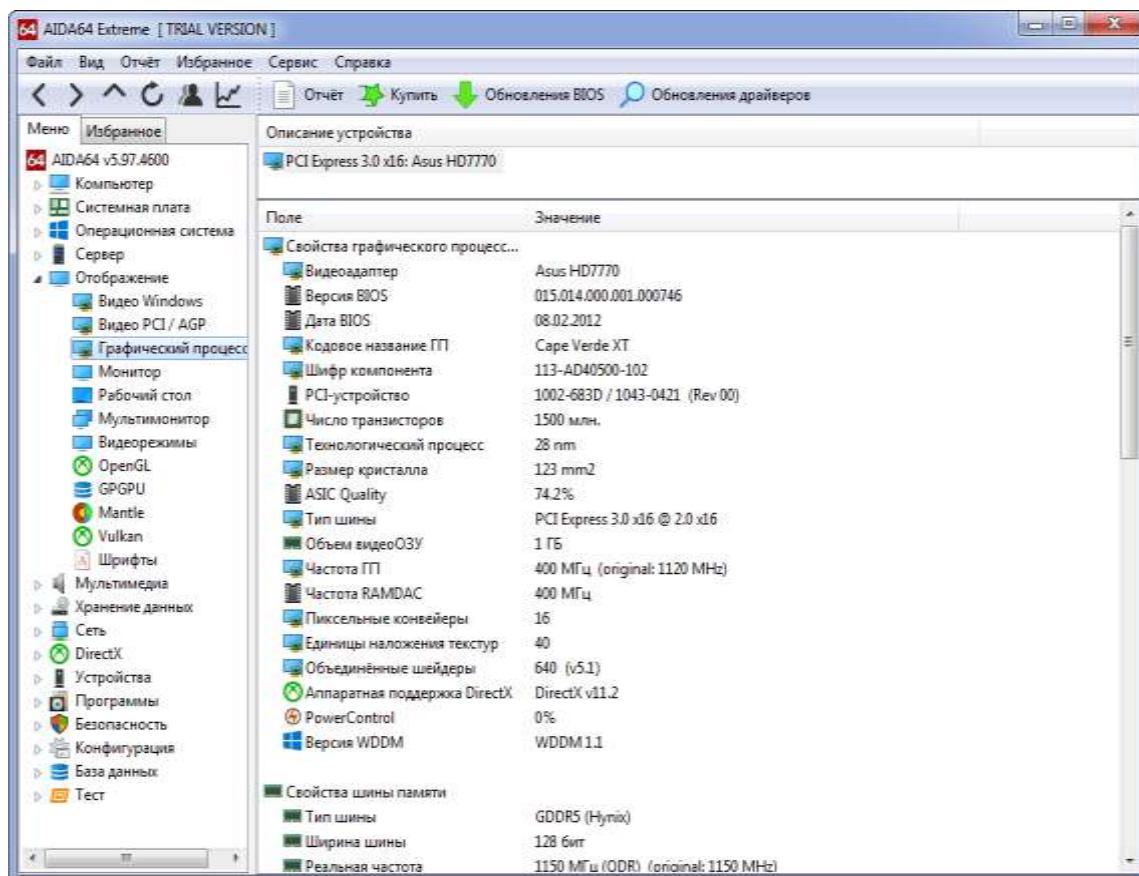


Рисунок 7.6.2. Информация об оборудовании

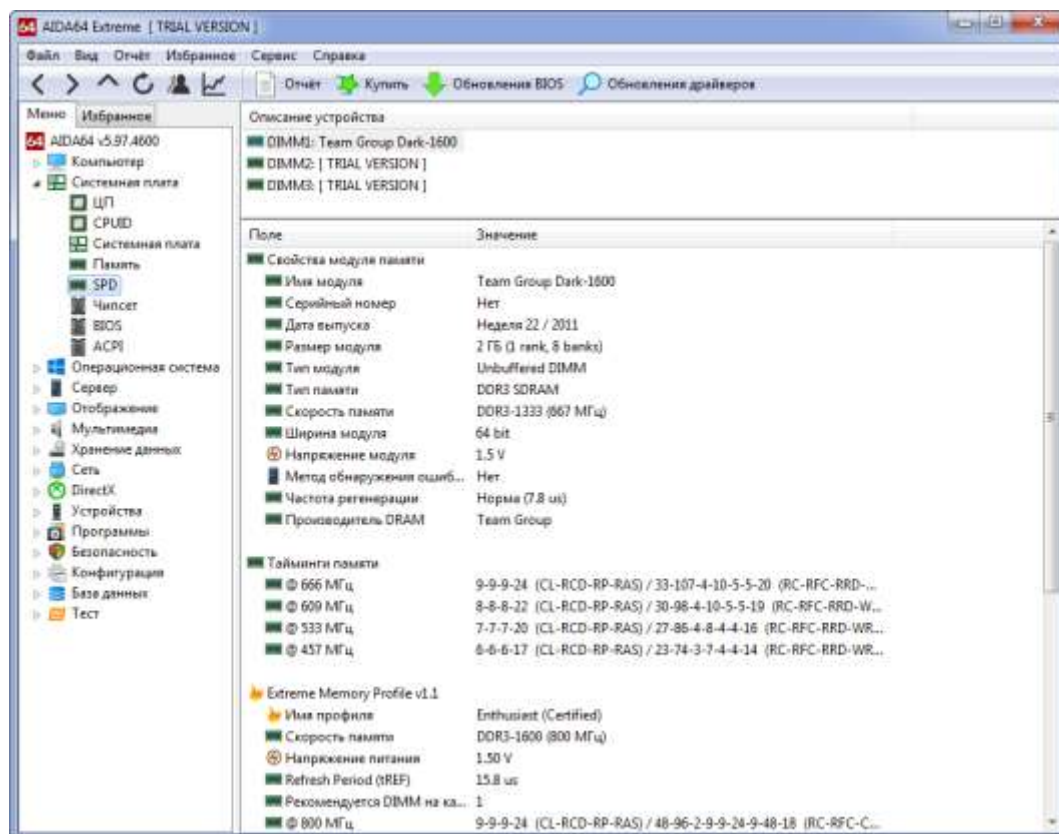


Рисунок 7.6.3. Информация об оборудовании

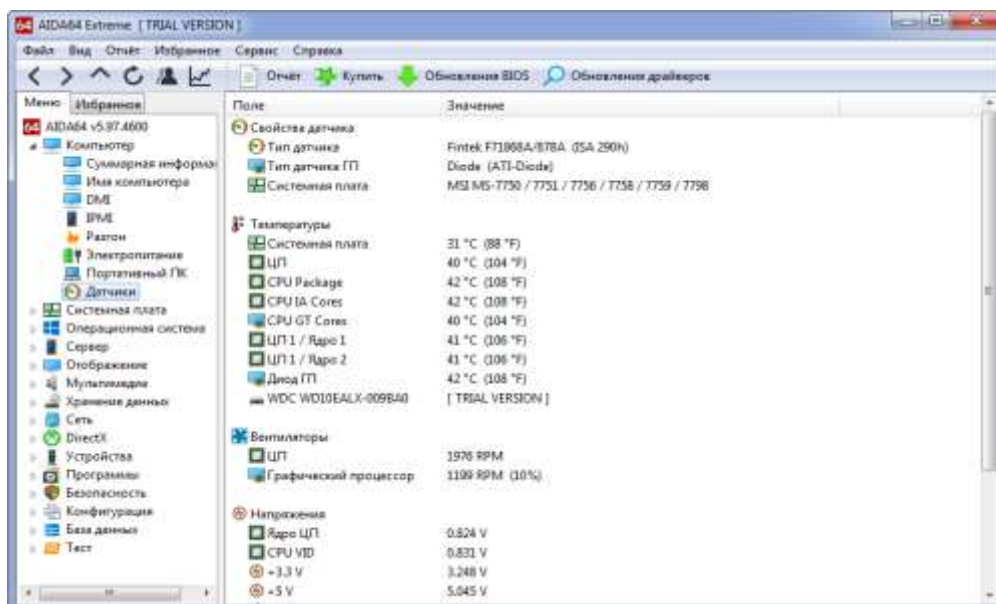


Рисунок 7.6.4. Информация об оборудовании

Драйверы. Приложение показывает используемые драйверы для всех установленных аппаратных компонентов и дает ссылки на их новые версии на официальный сайт.

После перехода в первую ветку раздела «Устройства» увидим классический диспетчер задач. После клика по оборудованию окно справа разделится горизонтально, в нижней его части приводятся свойства выбранного устройства. Внизу в строке «Производитель» находится ссылка на страницу с драйвером на официальном ресурсе (см. рис. 7.6.5).

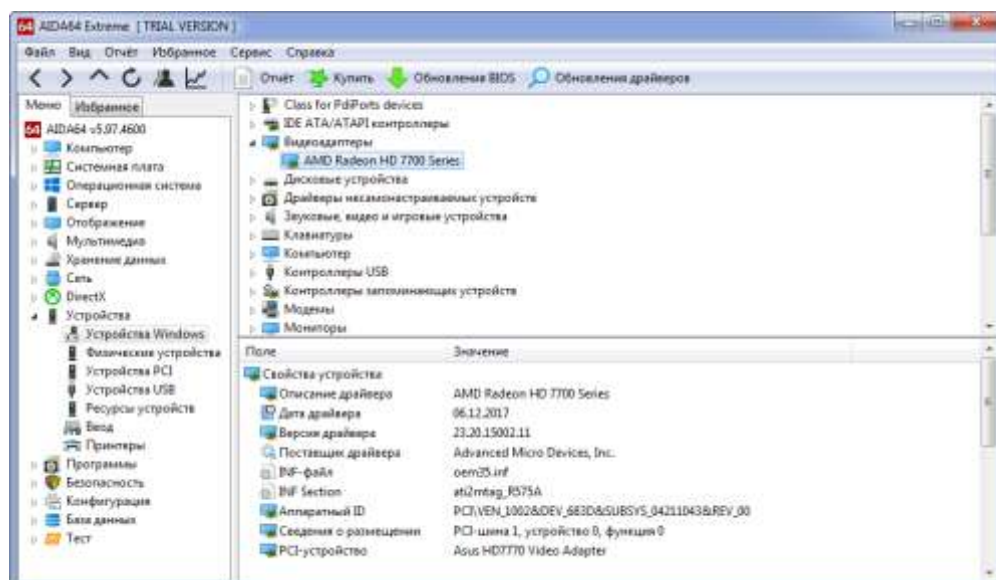


Рисунок 7.6.5. Информация об оборудовании

Безопасность – все, что касается защиты системы: антивирус, файрвол, наличие новых заплаток. *Конфигурация* – все настройки Windows в одном месте, а также содержимое основных конфигурационных файлов Windows.

Отчеты (см. рис. 7.7). Через главное меню или панель инструментов вызывается «Мастер отчетов». Благодаря профилям для их создания можно получить текстовый документ с любой информацией, которую отображает AIDA64. Пользователю доступен ряд шаблонов и функция ручного выбора интересных ему разделов, сведения из веток которых необходимо экспортировать в файл.

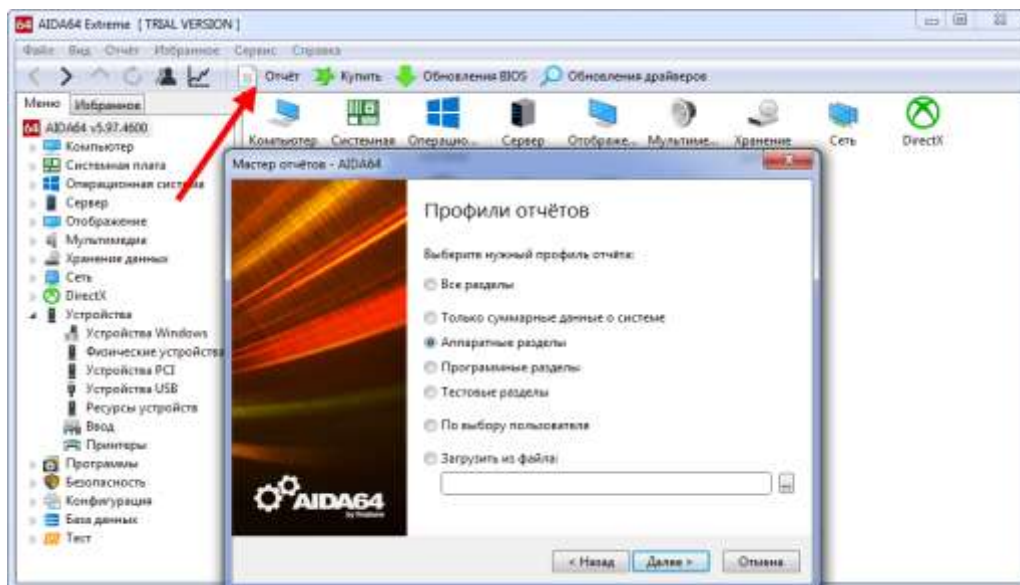


Рисунок 7.7. Отчеты

Тест – здесь собраны различные алгоритмы проверки стабильности и оценки производительности компонентов компьютера (ЦП, видеокарта, оперативная память), а также сравнение полученных результатов с итогами тестирования других составляющих.

Выполните практические задания по анализу аппаратной части автоматизированного рабочего места. Полученную информацию занесите в таблицу.

Задание 5. Проанализируйте составляющие предоставленного рабочего места.

Задание 6. Проанализируйте суммарную информацию об основных сведениях и конфигурации предоставленного рабочего места.

Задание 7. Получите информацию о графической составляющей (сведения о мониторе, графическом ускорителе и его компонентах (память, процессор)).

Задание 8. Получите информацию о звуковой подсистеме компьютера (используемые аудиоустройства).

Задание 9. Получите информацию о материнской плате, ее спецификации, чипсете, оперативной памяти и центральном процессоре, а также BIOS.

Задание 10. Получите перечень характеристик и текущего состояния устройств для долговременного хранения цифровой информации: физические, ло-

гические, съемные, оптические, сетевые, а также SMART-данные. Информацию предоставьте отдельно по каждому носителю.

Задание 11. Получите информацию о сети: общие, группы, в которых состоит учетная запись, и все о созданных аккаунтах. Получите информацию о сетевой карте, используемых сетях и ресурсах, Интернете, портах.

Задание 12. Получите информацию о периферийных устройствах: их виде, типе и производителе, в том числе клавиатуре и мыши. Информацию предоставьте отдельно по каждому устройству.

Задание 13. Получите информацию об используемой ОС, в том числе о статистике ее работы (когда установлена, сколько проработала).

Характеристики автоматизированного рабочего места

Составляющая	Вид сведений	Полученные сведения
1. Видео. Монитор (экран)	Модель	
	Диагональ	
	Тип подключения	
	Разрешение экрана	
2. Видео. Видеокарта	Модель	
	Тип	
	Видеопамять	
	Особенности	
3. Звук	Модель	
	Тип адаптера	
	Производитель	
	Драйвер	
4. Центральный процессор	Тип ЦП	
	Производитель	
	Тактовая частота	
	Количество ядер	
5. Материнская плата	Модель	
	Свойства шины FSB	
	Свойства шины памяти	
	Частоты	
6. Оперативная память	Модель	
	Объем памяти	
	Частота	
7. BIOS	Тип	
	Производитель	
8. Хранение данных	Тип диска	
	Объем диска	
9. Сеть	Тип	
	Адрес	
10. Периферийные устройства	Вид	
	Тип	
	Производитель	

11. Операционная система	Наименование	
	Дата установки	
	Версия	
	Имя компьютера	

Задание 14. Создайте отчет по работе системы при помощи «Мастер отчетов».

Основные понятия и термины

Криминалистически значимая информация (КЗИ) – извлеченные и интерпретированные цифровые следы, имеющие доказательственное значение по делу (переписка, логины, файлы, история действий, финансовые транзакции и т.д.).

Цифровые (компьютерные) следы – данные в цифровой форме, имеющие отношение к расследуемому событию, которые были созданы, изменены, удалены или использованы в процессе совершения преступления и могут быть получены с цифровых носителей.

Источник цифровых следов – любое устройство или система, способная хранить, обрабатывать или передавать цифровую информацию (компьютеры, смартфоны, планшеты, серверы, маршрутизаторы, облачные хранилища, IoT-устройства, банкоматы, автомобильные системы и т.д.).

Эфемерные (временные) следы – данные, существующие только в оперативной памяти (RAM) или в течение активного сеанса, которые могут быть утрачены после выключения устройства.

Вопросы и задания для оценки теоретических знаний

1. Дайте определение цифрового следа. Чем он принципиально отличается от традиционного материального следа?
2. Перечислите не менее пяти видов источников цифровых следов, помимо персонального компьютера.
3. Что такое метаданные? Приведите примеры трех различных типов метаданных и объясните их криминалистическое значение.
4. В чем заключается основная проблема установления атрибуции при работе с цифровыми следами?
5. Опишите путь, по которому может распространиться цифровой след от одного отправленного фотографического изображения. На каких устройствах и в каких формах он может сохраниться?
6. Что такое эфемерные следы? Почему их извлечение является первоочередной задачей при работе с включенным устройством?
7. Как использование облачных технологий меняет процесс обнаружения и изъятия цифровых следов? Какие правовые сложности возникают?
8. Каким образом технологии шифрования (дискового, файлового, сетевого) влияют на доступность цифровых следов для следователя?
9. Какие артефакты могут остаться в системе после использования злоумышленником средств анонимизации (TOR, VPN)?

8. ОСОБЕННОСТИ ФИКСАЦИИ СЛЕДОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Вопросы для самостоятельного изучения:

8.1. Порядок поиска информации на электронных носителях, компьютерных и мобильных устройствах, а также интернет-сайтах.

8.2. Порядок работы с цифровыми файлами, поиск метаданных в цифровых фотографиях.

Методические рекомендации по вопросам, изучаемым в ходе самостоятельной работы

При рассмотрении **первого вопроса** необходимо уяснить порядок поиска информации на электронных носителях, компьютерных и мобильных устройствах, а также интернет-сайтах.

Задание 1. Определите, какие действия должен выполнить специалист перед началом поиска цифровых следов на электронных носителях информации.

Операционная система выполняет массу процедур, чтобы работать быстрее. К примеру, она записывает данные в реестр, временные папки и др. За счет этого временные данные, связанные с файлом, отследить вручную довольно сложно. В Windows есть файл подкачки `pagefile.sys` и своп памяти `hiberfil.sys`, который используется в режиме гибернации. Они находятся в корневом каталоге диска с операционной системой. Важно, что в `pagefile.sys` и `hiberfil.sys` есть не только файлы, которые открывали с момента последней загрузки Windows. Данные могут храниться несколько недель или даже месяцев.

Задание 2. Определите особенности наиболее популярных систем для анализа электронных носителей.

Задание 3. Определите методы поиска следов сохраненных изображений в операционной системе.

Задание 4. Укажите, какой инструментарий применяется для поиска и аналитики информации в сети Интернет и социальных сетях.

Задание 5. Определите, какие действия необходимо выполнить при обнаружении и фиксации электронной информации.

Компания «Элкомсофт» предоставляет государственным и правоохранительным органам полный спектр решений для проведения криминалистического анализа, сбора доказательной базы и восстановления доступа к зашифрованной информации. Программные решения предлагают полную прозрачность, подробные отчеты, скорость и простоту в использовании. Данные, полученные с помощью программных продуктов «Элкомсофт», могут использоваться в качестве доказательной базы во время следствия и в суде.

Advanced Office Password Recovery разблокирует защищенные паролем документы Microsoft Word и электронные таблицы Excel в течение гарантированного периода вместо взлома и восстановления сложных паролей. Инструмент поддерживает документы и электронные таблицы, созданные с помощью устаревших версий Microsoft Office или сохраненные в режиме совместимости в современных версиях.

Задание 6. Разблокируйте пароль для зашифрованных файлов .doc с использованием программы Advanced Office Password Recovery компании «Элкомсофт».

Порядок выполнения задания.

6.1. Откройте программу Advanced Office Password Recovery. Изучите интерфейс (см. рис. 8.1.1).

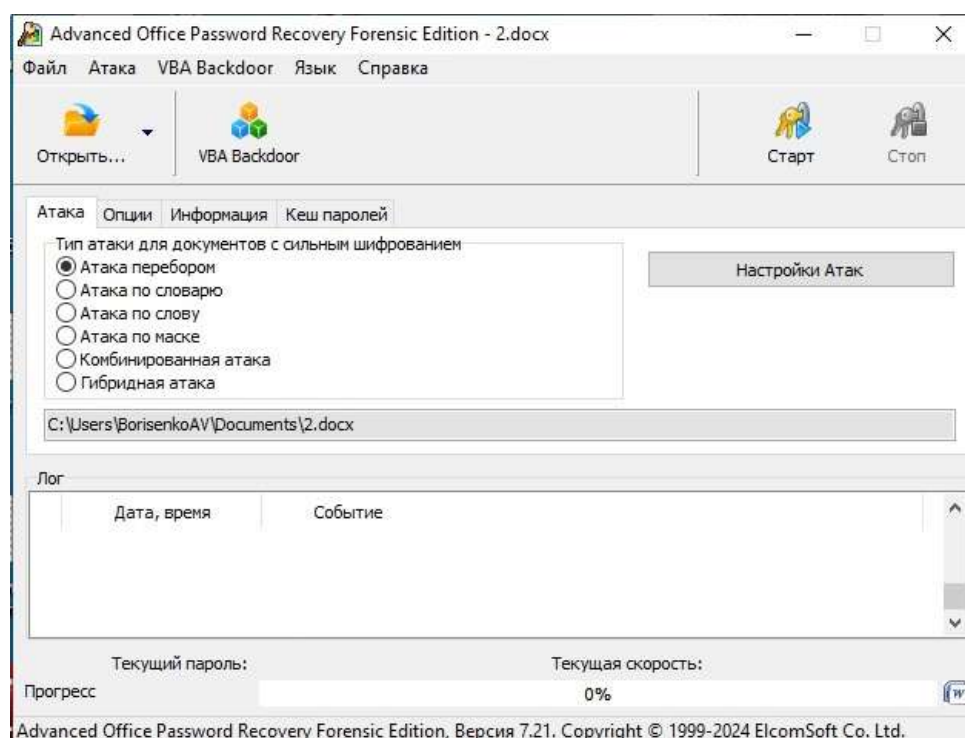


Рисунок 8.1.1. Интерфейс программы Advanced Office Password Recovery

6.2. Отключите проведение мгновенной атаки (см. рис. 8.1.2).

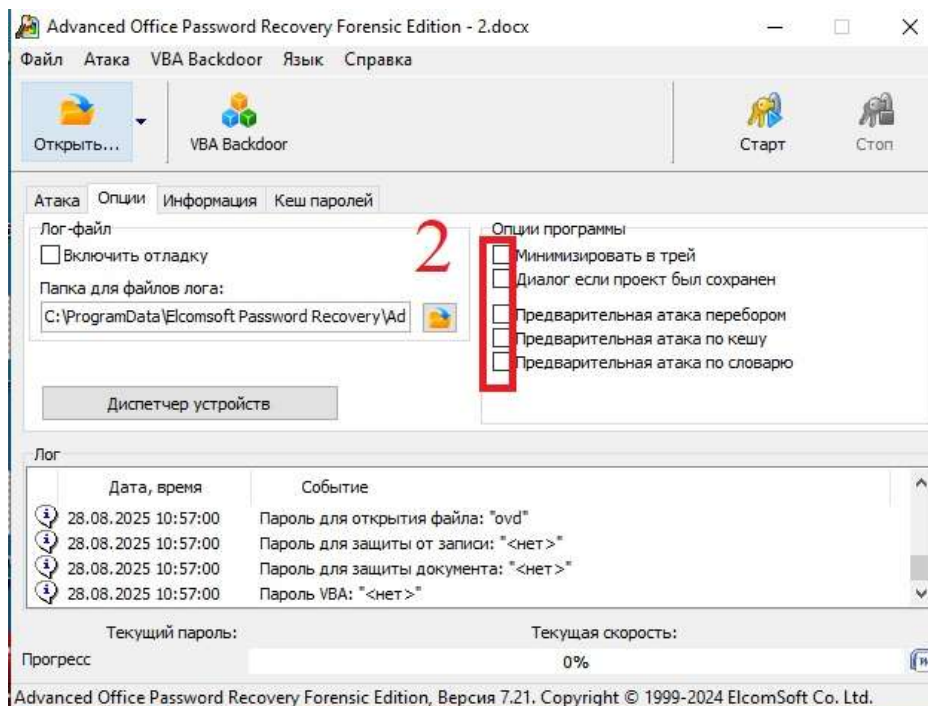


Рисунок 8.1.2. Интерфейс программы Advanced Office Password Recovery

6.3. Выберите необходимый тип атаки на пароль и установите настройки атаки (см. рис. 8.1.3).

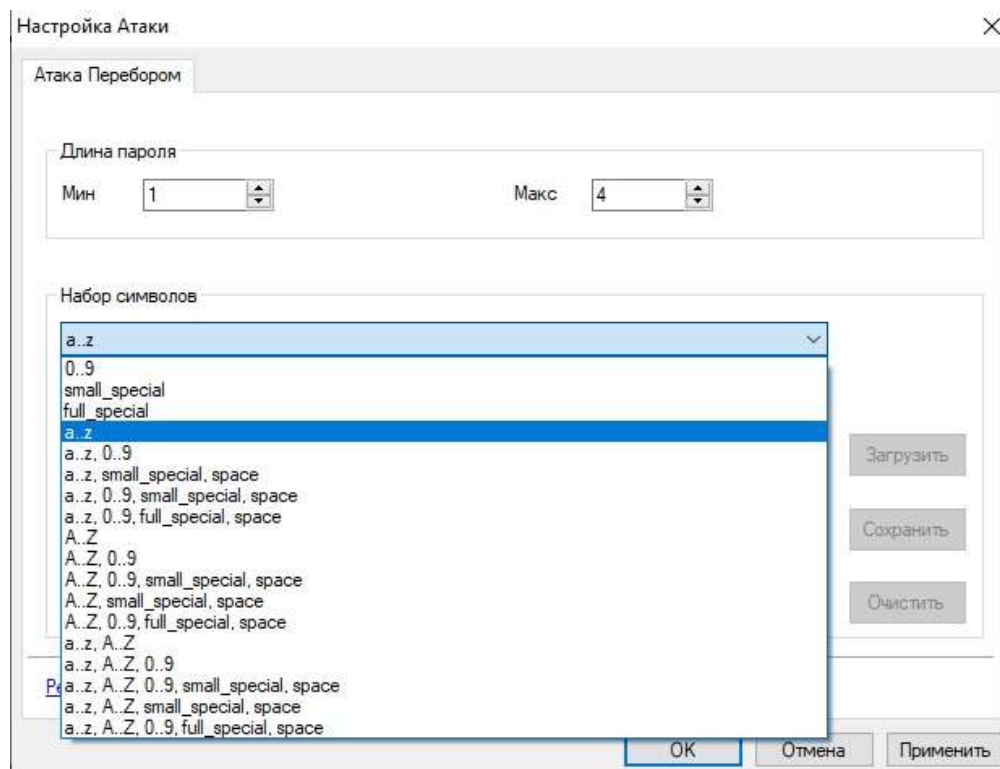


Рисунок 8.1.3. Интерфейс программы Advanced Office Password Recovery

6.4. Откройте необходимый защищенный файл .doc и разблокируйте пароль (см. рис. 8.1.4).

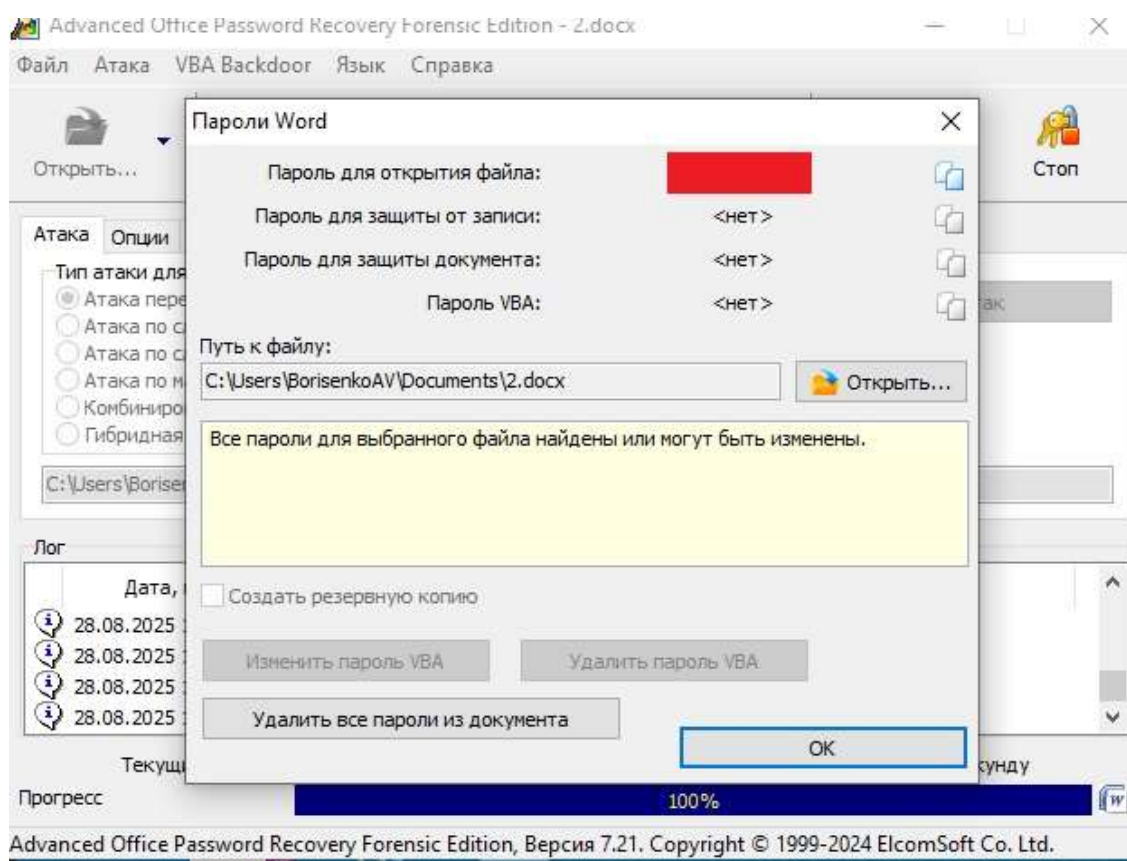


Рисунок 8.1.4. Интерфейс программы Advanced Office Password Recovery

Во **втором вопросе** важно довести обучающимся порядок работы с цифровыми файлами, поиск метаданных в цифровых фотографиях. Для использования электронной информации в суде прежде ее нужно правильно собрать и закрепить. Тут не обойтись без помощи специалиста, обладающего подходящей квалификацией. Ведь основное условие, которое необходимо будет соблюсти, – это неизменность исходной информации. То есть она должна быть сохранена в первоначальном виде. Изменения могут исказить картину событий и не позволят установить истину. Именно для соблюдения условия неизменности информации лучше обратиться к профессионалам. Чаще ими являются судебные эксперты в области компьютерно-технических экспертиз и другие специалисты, обладающие знаниями и навыками в нужной сфере.

Анализируя фотографии, можно обнаружить интересующие объекты, вещи, особенности расположения мест на работе, документы на столе и прочие нюансы. По элементам в кадре можно будет определить:

- место работы или отдыха;
- различного вида взаимоотношения с иными лицами;
- невербальные сигналы на фотографиях;
- идентификацию места съемки;
- круг знакомств;

- статусы в мессенджерах и социальных сетях
- комментарии к медиаконтенту.

Содержание тегов с метаданными в современной цифровой фотографии связано с принятием в свое время стандартов IPTC и EXIF.

EXIF (англ. *ExchangeableImageFileFormat*) – стандарт, в котором звуковые файлы и изображения дополняются комментирующей информацией, такой как авторство, способы его получения, условия и др.

IPTC – стандарт метаданных, применяющийся для цифровых изображений, более узкой направленности, касающейся авторства.

Данные стандарты широко реализованы в современной цифровой технике. Во время съемки фотоаппараты добавляют в файлы изображений метаданные. Добавляется специфическая информация данной конкретной камеры, использованной при съемке, могут быть добавлены GPS-координаты с приемника. Совокупность такой дополнительной информации может быть очень полезна при проведении мероприятий по сбору информации при поиске людей. Если фотоаппарат добавлял GPS-координаты с приемника, то извлечь подобную информацию из цифровой фотографии можно либо с использованием прикладного программного обеспечения, либо посредством сервисов сети Интернет, где, как правило, представляется возможность просмотреть место привязки на карте мира.

Задание 7. Выполните поиск метаданных в цифровых фотографиях.

Порядок выполнения задания.

7.1. Метаданные в фото (данные EXIF) – это информация о графическом объекте, содержащая ряд сведений о владельце фотографии и самом снимке.

Для поиска метаданных в цифровых фотографиях существует множество способов и специальных утилит.

7.2. Метаданные на смартфонах. Чтобы посмотреть информацию на iOS, надо зайти в приложение «Фото», выбрать нужную фотографию и нажать на значок с символом **i**.

На Android в разных оболочках функция может называться по-разному: в стандартной версии ОС значок и символ будут аналогичные – **i**. В сторонних вариантах это может быть «Показать информацию» или «Подробнее».

Обычно смартфоны показывают не очень много информации: **дату, параметры камеры**, на которую сделан снимок, и **геолокацию**, если функция включена. Местоположение также можно добавить вручную.

7.3. Метаданные на компьютере. В Windows надо нажать правой кнопкой мыши по файлу → «Свойства» → «Подробно». Во вкладке будут все основные данные: разрешение, размер, глубина цвета, авторство и геолокация.

На macOS посмотреть метаданные можно сразу в Finder. Делается это так: Finder → выбор папки → выбор файла → «Вид» → «Показать параметры просмотра». Далее в открывшемся окошке надо отметить те метаданные, которые вы хотите увидеть. Информация будет отображаться в правой части окна Finder, под превью изображения.

Чтобы посмотреть метаданные фото в Linux, можно использовать утилиту identify из ImageMagick. Позволяет получить подробную информацию о файле изображения. Для получения наиболее полной информации об изображении можно выполнить команду identify с параметром -verbose.

7.4. Метаданные на компьютере в сети Интернет. В сети Интернет существуют различные сервисы просмотра информации о месте съемки, техническом устройстве, которым производилась съемка, и прочих свойствах. К примеру, подобную информацию предоставляет сервис pic2map, расположенный по адресу: <https://www.pic2map.com>. Одновременно реализована возможность просмотра места съемки на карте, однако только в том случае, если фотоаппарат добавлял GPS-координаты с приемника. Отображение таких сведений на странице сервиса производится уже после передачи фотографии через форму загрузки на стартовой странице, здесь же будет отмечено и место проведения фотосъемки (см. рис. 8.2).

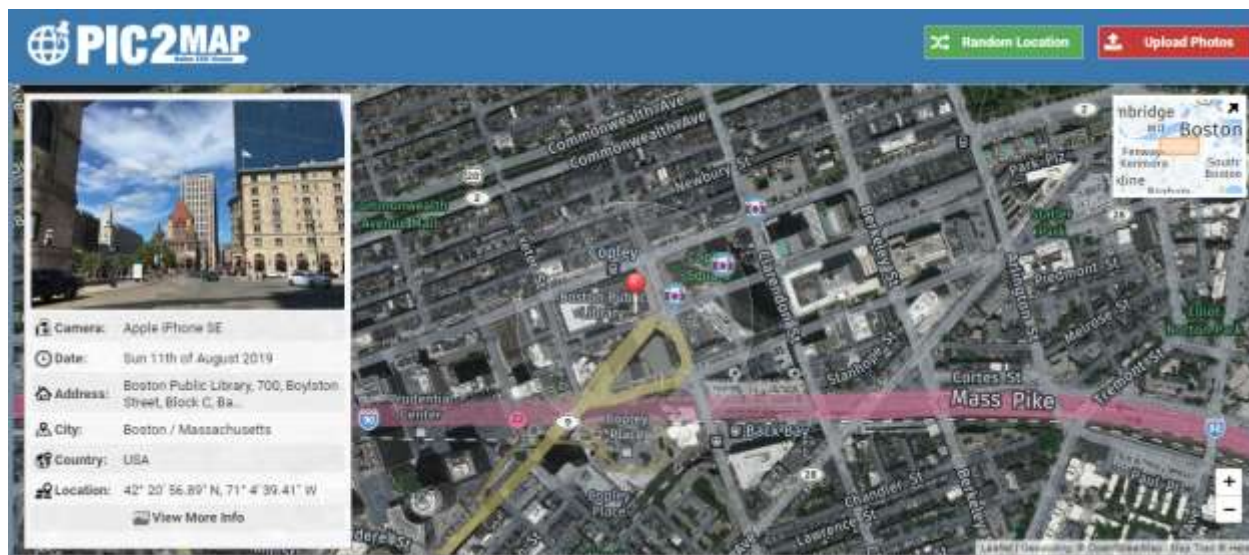


Рисунок 8.2. Карта места съемки в pic2map

На странице сервиса ниже карты места съемки представлены свойства фотографии (см. рис. 8.3), сгруппированные в разделы:

1. *Раздел CAMERA INFORMATION содержит информацию об устройстве, производившем фотосъемку.* В этом разделе может быть представлена информация о бренде (Brand), модели устройства (Model), линзе фотоаппарата (Lens Info), выдержке затвора фотоаппарата (Shutte), размере апертуры по отношению к фокусному расстоянию объектива (F Number), чувствительности датчика изображения к количеству присутствующего света (ISO Speed), состоянии вспышки (Flash), фокусном расстоянии (Focal Length), цветовой модели (Color Space), что может быть полезным при идентификации устройства разыскиваемого лица.

2. *Раздел FILE INFORMATION содержит информацию о файле.* В этом разделе может быть представлена информация об имени файла (File Name), о размере фотоизображения в пикселях (Image Size), количестве пикселей

(Resolution), уникальном идентификаторе изображения (Unique ID), типе файла изображения (MIME Type), глубине цвета (Dots/Inch). Раздел DATE&TIME («Дата и время») содержит временные характеристики изображения. В этом разделе может быть представлена информация о дате съемки (Date), времени съемки (Time), временной зоне (Time Zone). Данные параметры зависят от настроек фотоаппарата или устройства съемки. Эта информация может быть полезна при сопоставлении соответствий подобных файлов в сети.

3. Раздел *GPS INFORMATION* содержит информацию о географических данных фотографии. Если фотоаппарат добавлял GPS-координаты с приемника, в данном разделе будут представлены сведения о широте места съемки (Latitude), долготе места съемки (Longitude), координатах (Coordinates), высоте GPS (Altitude), направлениях изображения при его захвате во время съемки (Direction Ref и Direction), направлении камеры, а также информация о том, когда была сделана фотография (Pointing).

4. Раздел *LOCATION INFORMATION* содержит информацию о месте съемки. В этом разделе может быть представлена информация о городе (City), регионе (State), стране (Country), об адресе (Address). Эти сведения формируются на основе вышеуказанных данных GPS-метки.

CAMERA INFORMATION		
Brand: Apple	Model: iPhone SE	Lens Info: iPhone SE back camera 4.15mm...
Shutter: 1/2079 (0.0005 seconds)	F Number: f/2.2	ISO Speed: ISO 25
Flash: Not Used	Focal Length: 4.2 mm	Color Space: sRGB
FILE INFORMATION		
File Name: IMG_3187-photo.JPG	Image Size: 4032 x 3024 pixels	Resolution: 12.2 megapixels
Unique ID:	MIME Type: image/jpeg	Dots/Inch: 72 DPI
DATE & TIME		
Date: 2019-08-11	Time: 16:01:51 (GMT-05:00)	Time Zone: America / New York
GPS INFORMATION		
Latitude: 42.349136	Longitude: -71.077614	Lat Ref: North
Long Ref: West	Coordinates: 42° 20' 56.89" N, 71° 4' 39.41" W	Altitude: 6m (Above Sea Level)
Direction Ref: Magnetic North	Direction: 87.62 Degrees	Pointing: East
LOCATION INFORMATION		
City: Boston	State: Massachusetts	Country: USA
Address: Boston Public Library, 700, Boylston Street, Block C, Back Bay, Boston, Suffolk County, Massachusetts, 02116, USA (Location was guessed from coordinates and may not be accurate.)		

Рисунок 8.3. Свойства фотографии в pic2map

Файл цифровой фотографии содержит не только метаданные, но и само изображение. На изображении, помимо людей, могут быть запечатлены общественные места, интерьер помещений интересующего лица. Если отсутствуют геоданные у фотографии, то место можно попытаться определить через серви-

сы сети Интернет, которые, подобно распознаванию текста, пытаются распознать места, основываясь на панорамных изображениях картографических систем. Примером такого ресурса является сервис «Картинки» поисковой системы «Google», расположенный по адресу: <https://www.google.ru/imghp>. В данной поисковой системе в строке поиска имеется значок в виде фотоаппарата (см. рис. 8.4), предоставляющий переход к сервису поиска по картинке.

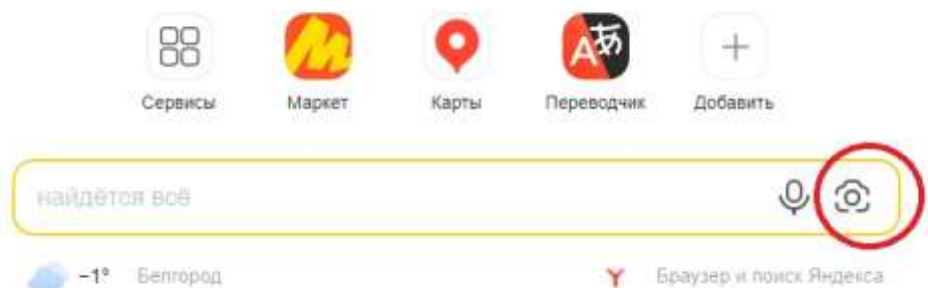


Рисунок 8.4. Сервис поиска по картинке поисковой системы «Яндекс»

После нажатия на пиктограмме «Поиск по картинке» открывается окно с вкладкой «Загрузить файл» для возможности передачи сервису интересующего изображения (см. рис. 8.5).

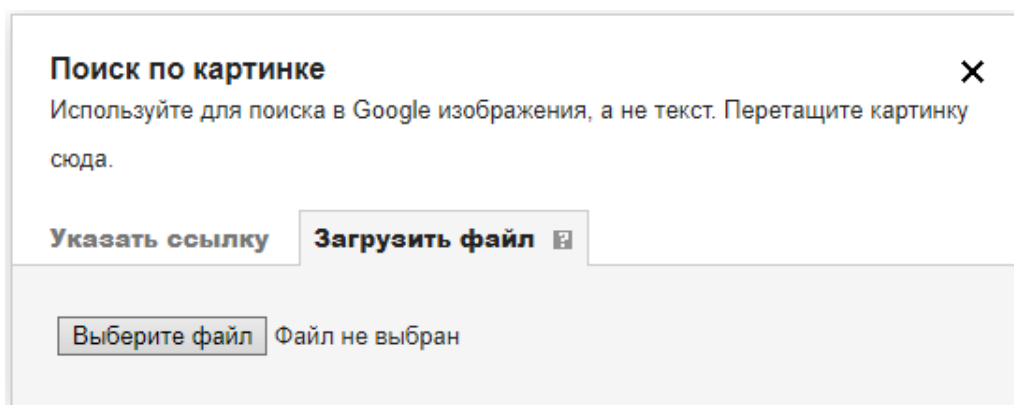
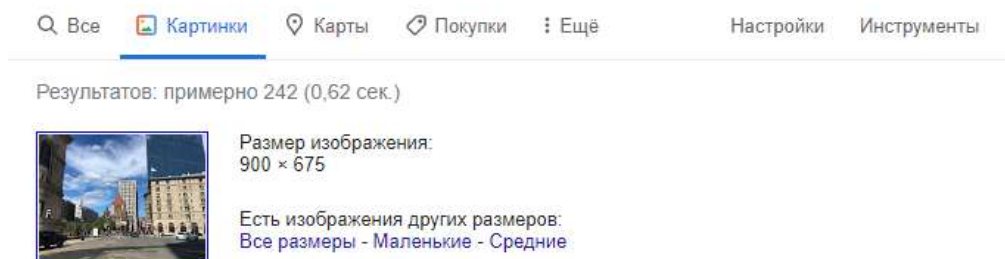


Рисунок 8.5. Загрузка файла в поиске по картинке

Поисковая система предоставит результаты, где аналогичный файл или похожее на изображении место могли встречаться (см. рис. 8.6).

В окне результата поиска при переходе на вкладку «Карты» будет указано место соответствия поисковой фотографии на карте (см. рис. 8.7).



Запрос, который может быть связан с изображением: **copley square**

en.wikipedia.org › wiki › Cop... ▾ Перевести эту страницу

Copley Square - Wikipedia

Copley Square /ˈkɒpli/, named for painter John Singleton Copley, is a public square in Boston's Back Bay neighborhood, bounded by Boylston Street, ...

www.tripadvisor.ru › ... › Бостон › Отели Бостона

COPLEY SQUARE HOTEL 4* (Бостон) - отзывы, фото и ...

Copley Square Hotel 4*, Бостон: Читайте объективные отзывы и просматривайте фотографии реальных путешественников. Проверьте ...

Похожие изображения



Рисунок 8.6. Результаты поиска по картинке

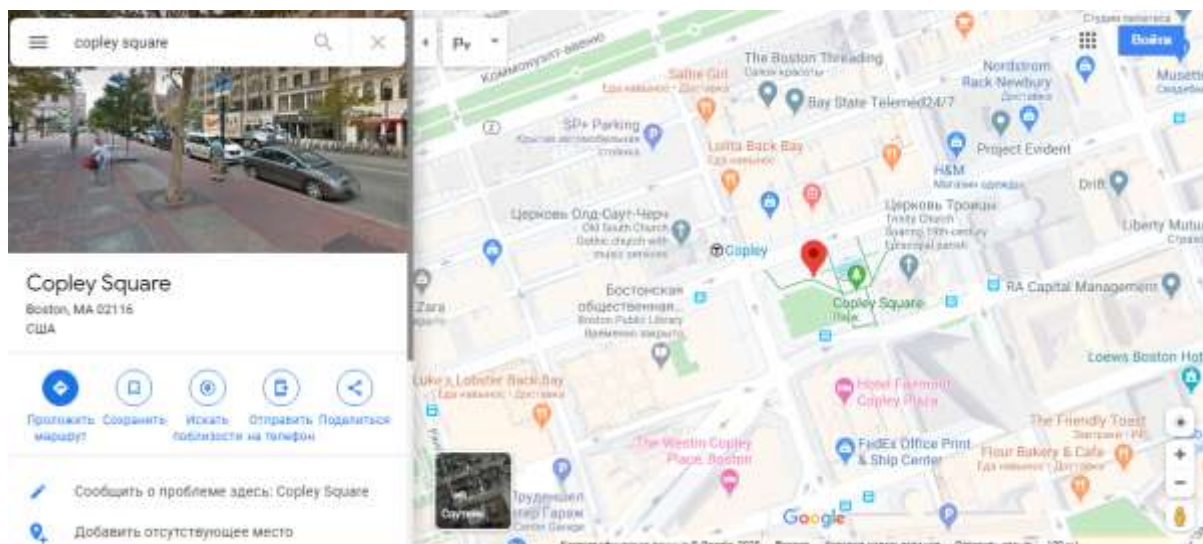


Рисунок 8.7. Результаты поиска по картинке на карте

В таблице 8.1 приведены сервисы, которые позволяют осуществлять поиск по картинкам, фотографиям, в том числе в социальных сетях. Также приведены материалы для поиска провайдеров, проверки адресов электронной почты на идентичность, телефонные справочники и другие поисковики.

Таблица 8.1. Сервисы для определения электронной почты, поиска по фотографии, получения информации о домене, телефонные справочники

Сервис	Предназначение
Поисковики	
https://www.tineye.com/	Поиск по картинке
https://www.pic2map.com	Поиск места по фотографии
https://findclone.ru/	Поиск пользователей по фото в соцсети «ВКонтакте» (через регистрацию)
https://duckduckgo.com/	Поисковик
https://www.mmnt.ru/	Поисковик по FTP
https://www.wolframalpha.com/	База знаний и набор вычислительных алгоритмов. Английский язык
IP-адреса, провайдеры, домены	
https://www.wservice.info/	Сетевые утилиты. Определение провайдера, принадлежность IP, используется ли почтовый сервер и у кого он размещен
https://2ip.ru/	Информация об IP-адресе или домене
http://whoishistory.ru/	Домены и IP с историей изменений
https://mailtester.com/testmail.php	Проверка e-mail на действительность
http://eais.rkn.gov.ru/	Единый реестр сайтов, запрещенных Роскомнадзором
Разное	
https://pkk5.rosreestr.ru/	Публичная кадастровая карта
http://wikimapia.org	Wikimapia – интерактивная карта мира
http://exif.regex.info/exif.cgi	Сведения о графических файлах (указываем ссылку или загружаем фото)
Сотовые операторы, телефонные справочники	
https://smspilot.ru/test.php?type=hlr	Определение оператора сотовой связи, определение в сети абонент или нет. Количество запросов в сутки ограничено
https://smc.ru/testhlr/?SE=c6a65a8a	Определение оператора сотовой связи, определение в сети абонент или нет. Количество запросов в сутки ограничено
https://zniis.ru/bdpn/check	Определение сотового оператора
https://money.yandex.ru/phone?args&_openstat=yandex;_mphonekoldun;_header	Определение сотового оператора
https://spravnik.com/	Телефонные справочники городских номеров СНГ
http://nomerorg.website/	Телефонные справочники городских номеров России
https://xinit.ru/bs/	Карта местонахождения базовых станций
https://www.kody.su/city/	Телефонные коды городов России

Основные понятия и термины

Возможны следующие инциденты кибербезопасности:

- взлом сетевого принтера или ИП телефона;
- обнаружение вредоносной программы типа «троян»;
- выявление постороннего устройства (например, рабочей станции);
- выявление заражения сетевым червем;
- при включении компьютера синий экран;
- воздействие вредоносной программы типа «шифровальщик».

Мониторинг информационной безопасности – это сбор и исследование сведений для обнаружения возможных атак. Его также называют мониторингом событий безопасности.

Вопросы для оценки теоретических знаний

1. Какой из примеров цифровых следов является активным?
2. На какие свойства информации влияют угрозы информационной безопасности?
3. В чем опасность цифровых следов?
4. Какой регулятор осуществляет контроль в области защиты информации техническими средствами?
5. На сайте какого регулятора в свободном доступе размещен банк данных угроз информационной безопасности?
6. Каковы рекомендации по минимизации цифрового следа?
7. Как подразделяются следы совершения компьютерного преступления?
8. Через какой сервис сети Интернет можно установить провайдера?
9. Как проявляется неправомерный доступ к компьютерной информации в работе ЭВМ?
10. Какой регулятор осуществляет контроль в области защиты персональных данных?
11. Каковы рекомендации по минимизации цифрового следа?
12. Как называются потенциальные злоумышленники?
13. Какой из примеров цифровых следов является пассивным?
14. Перечислите виды компьютерной экспертизы.
15. Что исследуется при осмотре съемных носителей информации?

ЗАКЛЮЧЕНИЕ

На современном этапе развития российского общества актуализируется проблема осуществления правоохранительными органами своих функций на требуемом уровне их компетентности для обеспечения защиты граждан страны от многочисленных преступлений в глобальной сети Интернет и формируемом информационном пространстве.

В связи с действующей мировой геополитической ситуацией, как никогда, важно иметь надежные правоохранительные структуры, которые будут успешно справляться со своими обязанностями по охране прав и свобод общества и каждого человека по отдельности. Ввиду этого в условиях современной модернизации общества и современного научно-технологического прогресса правоохранительным органам зачастую помогают различные информационные системы, которые на постоянной основе используются в качестве базовых средств в деятельности, направленной на борьбу с преступностью и защиту общества и государства.

Внедрение учебного модуля «Основы информационных технологий и кибербезопасности в деятельности органов внутренних дел Российской Федерации» позволит ускорить формирование информационно-технологической компетентности у действующих сотрудников правоохранительных органов как составной части профессиональной компетентности, что обеспечит высокую эффективность их служебной деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом изменений, одобренных в ходе общероссийского голосования 01.07.2020) [Электронный ресурс] // СПС «КонсультантПлюс».
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // СПС «КонсультантПлюс».
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // СПС «КонсультантПлюс».
4. Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» [Электронный ресурс] // СПС «КонсультантПлюс».
5. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] // СПС «КонсультантПлюс».
6. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // СПС «КонсультантПлюс».
7. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [Электронный ресурс] // СПС «КонсультантПлюс».
8. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [Электронный ресурс] // СПС «Гарант».
9. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] // СПС «КонсультантПлюс».
10. Постановление Правительства Российской Федерации от 08.02.2018 № 127 (ред. от 20.12.2022) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [Электронный ресурс] // СПС «КонсультантПлюс».
11. Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» [Электронный ресурс] // СПС «КонсультантПлюс».
12. Национальный стандарт Российской Федерации ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения» [Электронный ресурс] // Электронный фонд правовых и

нормативно-технических документов. – URL: <https://docs.cntd.ru/document/> (дата обращения: 18.03.2025).

13. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (в редакции приказа ФСТЭК России от 15.02.2017 № 27, от 28.05.2019 № 106) [Электронный ресурс] // СПС «КонсультантПлюс».

14. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (ред. от 20.02.2020) [Электронный ресурс] // СПС «КонсультантПлюс».

15. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (ред. от 28.05.2019) [Электронный ресурс] // СПС «КонсультантПлюс».

16. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (ред. от 15.03.2021) [Электронный ресурс] // СПС «КонсультантПлюс».

17. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [Электронный ресурс] // СПС «КонсультантПлюс».

18. Приказ ФСБ России от 24.10.2022 № 524 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» [Электронный ресурс] // СПС «КонсультантПлюс».

19. Приказ Минцифры России от 10.09.2021 № 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» // СПС «КонсультантПлюс».

20. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021) [Электронный ресурс] // СПС «КонсультантПлюс».

21. Деятельность органов внутренних дел по пресечению угроз кибербезопасности: учебно-методическое пособие / А.Н. Александров, Е.Г. Ковалева, В.Л. Акапьев [и др.]. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2024. – 104 с.
22. Симаков А.А., Кургузов А.В. Защита информации в компьютерных системах: учеб. пособие. – Омск: Омская академия МВД России, 2022. – 108 с.
23. Информатика и информационные технологии в профессиональной деятельности: учебник / И.Ф. Амельчаков [и др.]. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2018. – 369 с.
24. Информатика и информационные технологии в профессиональной деятельности: курс лекций / Н.В. Коробов [и др.]; под общ. ред. Н.В. Коробова. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2022. – 144 с.
25. Информационно-телекоммуникационные технологии в профессиональной служебной деятельности: учебно-методическое пособие / В.Л. Акапьев, А.А. Дрога, А.Э. Федосеев [и др.]. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2023. Ч. I. – 116 с.
26. Информационные технологии управления и организация защиты информации: курс лекций / В.А. Апульцин, Ш.Х. Гонов, В.Н. Лебедев [и др.]. – Москва: Академия управления МВД России, 2021. – 72 с.
27. Бажукова Ю.В., Равнюшкин А.В., Черепанова Ю.Е. Информационное право: учебное пособие. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2020. – 208 с.
28. Информатика и информационные технологии в профессиональной деятельности: учебное пособие / А.Г. Карпика, С.В. Лемайкина, В.Б. Гунько [и др.]. – Ростов-на-Дону: РЮИ МВД России, 2022. Ч. 2. – 48 с.
29. Дрога А.А., Савотченко С.Е., Акапьев В.Л. Использование особенностей системного программного обеспечения для противодействия преступности в сфере информационно-телекоммуникационных технологий: учебное пособие. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2023. – 76 с.
30. Организационная защита информации. Часть 1: Методологические основы организационной защиты информации: учебное пособие. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2019. – 156 с.
31. Основы информатики и информационных технологий в органах внутренних дел: учебное пособие / А.Н. Прокопенко [и др.]. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2016. – 144 с.
32. Основы кибербезопасности в деятельности сотрудников правоохранительных органов: учебное пособие / А.Н. Прокопенко [и др.]. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2023. – 153 с.
33. Основы цифровой грамотности: учебное пособие / В.В. Гончар [и др.]. – Москва: Московский университет МВД России имени В.Я. Кикотя, 2024. – 141 с.
34. Особенности использования информационных технологий в органах внутренних дел на транспорте: учебное пособие / И.Ф. Амельчаков [и др.]. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2016. – 118 с.

35. Ушаков А.Ю., Саакян А.Г., Поздышев Р.С. Практика расследования преступлений, совершенных с использованием криптовалюты: учебное пособие. – Москва: ДГСК МВД России, 2021. – 64 с.

36. ФСТЭК России официально подтвердила статус безопасности процессоров разработчика Astra Linux [Электронный ресурс]. – URL: <https://astralinux.ru/>.

37. Astra Linux 1.8 [Электронный ресурс]. – URL: <https://astra.ru/proxima/>

38. Russian IT Solutions [Электронный ресурс]. – URL: <https://astra.ru/upload/iblock/a85/r8kemtduq3hwhyx092s905fspj8zkntw.pdf>.

39. What is Endpoint Device Security? [Электронный ресурс]. – URL: <https://www.sentinelone.com/cybersecurity-101/endpoint-security/endpoint-device-security/>.

40. What Is Endpoint Security? How Does It Work? [Электронный ресурс]. – URL: <https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security>.

УЧЕБНОЕ ИЗДАНИЕ

Акапьев Виктор Львович,

кандидат педагогических наук;

Ковалева Екатерина Геннадьевна,

кандидат технических наук;

Борисенко Александр Васильевич,

кандидат физико-математических наук;

Федосеев Андрей Эдуардович,

кандидат физико-математических наук;

Панарин Валентин Валентинович

**Основы информационных технологий и кибербезопасности
в деятельности органов внутренних дел Российской Федерации**

Учебно-методическое пособие

Редактор

Е.А. Олейникова

Комп. верстка

И.Ю. Чернышева, Е.А. Прокопова

Подписано в печать 2026. Формат 60х90/16

Усл. печ. л. 5 Тираж 54 экз. Заказ 3

Отпечатано в отделении полиграфической и оперативной печати
Белгородского юридического института МВД России имени И.Д. Путилина
г. Белгород, ул. Горького, 71

ISBN 978-5-91776-669-0

