Отчет по лабораторным работам по дисциплине

**Основы информационной безопасности**

**Вариант 24**

Студент 2 курса 1 группы

Факультета ФИТ

Угоренко Виолетта Романовна

Оглавление

[**Лабораторная работа №1** 3](#_Toc195750792)

[**Лабораторная работа №2** 6](#_Toc195750793)

[**Лабораторная работа №3** 8](#_Toc195750794)

[**Лабораторная работа №4** 14](#_Toc195750795)

[**Лабораторная работа №5** 25](#_Toc195750796)

[**Лабораторная работа №6** 29](#_Toc195750797)

[**Лабораторная работа №7** 34](#_Toc195750798)

[**Лабораторная работа №8** 35](#_Toc195750799)

[**Лабораторная работа №9** 37](#_Toc195750800)

[**Лабораторная работа №10** 42](#_Toc195750801)

[**Лабораторная работа №11** 47](#_Toc195750802)

[**Лабораторная работа №12 51**](#_Toc195750803)

[**Лабораторная работа №13 55**](#_Toc195750804)

# **Лабораторная работа №1**

*Контрольные вопросы*

Что такое информационная безопасность?

Информационная безопасность - состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере;

Перечислите основные национальные интересы в информационной сфере.

Реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации.

Формирование и поступательное развитие информационного общества.

Равноправное участие Республики Беларусь в мировых информационных отношениях.

Преобразование информационной индустрии в экспортно-ориентированный сектор экономики.

Эффективное информационное обеспечение государственной политики.

* Обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

Какие основные угрозы национальной безопасности, связанные с ИТ-сферой, вы знаете?

Деструктивное информационное воздействие на личность, общество и государственные институты.

Нарушение функционирования критически важных объектов информатизации.

Рост преступности с использованием информационно-коммуникационных технологий.

Недостаточная эффективность информационного обеспечения государственной политики.

Несовершенство системы обеспечения безопасности критически важных объектов информатизации.

Назовите основные внутренние и внешние источники угроз национальной безопасности в информационной сфере.

**Внутренние:**

Распространение недостоверной или умышленно искаженной информации.

Зависимость от импорта информационных технологий и средств информатизации.

Несоответствие качества национального контента мировому уровню.

Недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий.

Рост преступности с использованием информационно-коммуникационных технологий.

**Внешние**:

Открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия.

Доминирование ведущих зарубежных государств в мировом информационном пространстве.

Информационная деятельность зарубежных государств, международных и иных организаций, наносящая ущерб национальным интересам.

Развитие технологий манипулирования информацией.

Препятствование распространению национального контента за рубежом.

Попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь.

Перечислите основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере.

В информационной сфере Республики Беларусь осуществляется комплекс мероприятий, направленных на нейтрализацию внутренних угроз национальной безопасности. Основные направления государственной политики включают:

*Совершенствование прав граждан*: Разработка механизмов реализации прав на получение, хранение и использование информации, что включает доступ к государственным информационным ресурсам и услугам.

*Стратегия информатизации*: Внедрение стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы административных процедур для граждан и бизнеса.

*Развитие технологий*: Ускоренное развитие индустрии информационных и телекоммуникационных технологий с акцентом на повышение качества и конкурентоспособности национального контента.

*Нормативная база*: Совершенствование законодательства в области информационной безопасности, что включает создание комплексной государственной системы защиты информации и оптимизацию государственного регулирования.

*Методы защиты информации*: Разработка и внедрение современных методов защиты информации в критически важных инфраструктурах, что предотвращает негативное воздействие на национальную безопасность16.

*Международное сотрудничество*: Участие в международных договорах по информационному обмену и сохранение роли регулятора при внедрении иностранных технологий.

*Приоритетными являются:*

Завершение формирования комплексной государственной системы обеспечения информационной безопасности в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере.

Совершенствование нормативной правовой базы обеспечения информационной безопасности.

Эти меры направлены на создание безопасной информационной среды, защиту персональных данных граждан и обеспечение их прав на информацию, что является ключевым аспектом государственной политики в данной сфере.

# **Лабораторная работа №2**

*Условие задания*

Решить задачу разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа в соответствии с вариантом.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E*0 | *E* | *K* | *C* |
| 24 | 26000 | 23000 | 6 | 1000 |

*Исполнительная часть*

*1)*

*2)* 0,9

*3)*

*4)*

*5)*

![](data:application/x-msmetafile;base64,)

0,94

**Вывод:** Я научилась решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа и выяснила, что с данными значениями моего варианта защита эффективна. Эффективно.

*Контрольные вопросы*

1. Что такое технический канал утечки информации?

Технический канал утечки информации – это несанкционированный способ передачи данных за пределы защищённой системы с использованием физических или электронных средств, например, электромагнитных излучений, акустических волн или побочных сигналов оборудования.

2. Чем отличаются пассивные и активные методы защиты информации от утечки по техническим каналам?

**Пассивные методы защиты** направлены на предотвращение утечек без воздействия на потенциального злоумышленника. Они включают экранирование, использование специальных строительных материалов, защиту от электромагнитных излучений и контроль доступа.

**Активные методы защиты** включают применение средств обнаружения и противодействия утечкам, таких как генерация помех, системы обнаружения утечек и подавление несанкционированных каналов передачи информации.

3.Приведите примеры пассивных методов защиты информации.

Экранирование помещений и оборудования.

Использование звукопоглощающих материалов.

Контроль электромагнитных излучений.

Установка физических барьеров (например, сейфов, защищённых шкафов).

4. Перечислите примеры активных методов защиты информации.

Генерация маскирующих шумов.

Использование систем подавления радиосигналов.

Мониторинг электромагнитных излучений с последующим их подавлением.

Активное выявление и блокировка каналов утечки.

5. По характеру проводимых действий как разделяются все методы защиты информации?

Законодательные (правовые) – установление норм и правил защиты данных.

Организационные – контроль доступа, обучение персонала, аудит безопасности.

Технические – использование защитных устройств и технологий.

Комплексные – сочетание нескольких методов для повышения эффективности защиты.

**Лабораторная работа №3**

**РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕС-КОМПАНИИ**

**Вариант 24**

Цель: разработать проект политики информационной безопасности бизнес-компании.

Контрольные вопросы

**1. Что такое политика безопасности?**

Набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию.

**2. Что означают метки безопасности?**

Метки безопасности используются для реализации принудительного управления доступом к субъектам и объектам. Метка субъекта описывает его благонадежность, метка объекта – степень «закрытости» содержащейся в нем информации.

**3. Какие работы производятся по обеспечению режима информационной безопасности?**

– определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания;

– оценка рисков;

– выбор контрмер, обеспечивающих режим информационной безопасности;

– управление рисками;

– аудит системы управления информационной безопасностью;

– выработка политики безопасности.

**4. Какие практические шаги осуществляются для определения политики информационной безопасности?**

Этап 1. Выбор национальных и международных руководящих документов и стандартов в области информационной безопасности и формулирование на их базе основных требований и положений политики информационной безопасности компании, включая:

– управление доступом к средствам вычислительной техники (СВТ), программам и данным, а также антивирусную защиту;

– вопросы резервного копирования;

– проведение ремонтных и восстановительных работ;

– информирование об инцидентах в области информационной безопасности и пр.

Этап 2. Выработка подходов к управлению информационными рисками и принятие решения о выборе уровня защищенности компьютерных информационных систем (КИС). Уровень защищенности в соответствии с зарубежными стандартами может быть минимальным (базовым) либо повышенным. Этим уровням защищенности соответствует минимальный (базовый) или полный вариант анализа информационных рисков.

Этап 3. Структуризация контрмер по защите информации по следующим основным уровням: административному, процедур ному, программно-техническому.

Этап 4. Установление порядка сертификации и аккредитации КИС на соответствие стандартам в сфере информационной безопасности. Назначение периодичности проведения совещаний по тематике информационной безопасности на уровне руководства, в том числе периодического пересмотра положений политики информационной безопасности, а также порядка обучения всех категорий пользователей информационной системы в области информационной безопасности.

Этап 5. Определение сферы (границ) системы управления ин формационной безопасностью и конкретизация целей ее создания. На этом этапе определяются границы системы, для которой должен быть обеспечен режим информационной безопасности.

**5. Что является основой программно-технического уровня для обеспечения безопасности?**

− идентификация и аутентификация пользователей;

− управление доступом;

− протоколирование и аудит;

− криптография;

− экранирование;

− обеспечение высокой доступности и т. д.

Задание для выполнения



**1. Введение**

Политика информационной безопасности (ИБ) компании ЖЭС разрабатывается с целью защиты ценных данных, минимизации рисков, связанных с различными угрозами, и создания эффективной системы управления безопасностью информации. Информационные ресурсы компании являются ключевым активом, а их защита требует системного подхода, охватывающего технические, организационные и процедурные меры.

Современные угрозы информационной безопасности становятся все более изощренными, а их последствия могут привести к серьезным финансовым потерям, репутационному ущербу и юридическим последствиям. В связи с этим необходим комплексный подход к разработке и внедрению политики защиты, учитывающий как внешние, так и внутренние угрозы, а также их влияние на бизнес-процессы компании.

**2. Основные цели политики безопасности**

Главной задачей политики является обеспечение конфиденциальности, целостности и доступности информации. Конфиденциальность подразумевает защиту данных от несанкционированного доступа, целостность — предотвращение их изменения или уничтожения, а доступность — обеспечение бесперебойной работы информационной системы.

Защита информационных активов компании необходима для предотвращения утечек данных, несанкционированного доступа, а также обеспечения бесперебойной работы всей системы. Помимо этого, политика направлена на соответствие требованиям действующих нормативных документов и стандартов в сфере информационной безопасности. Руководство компании определяет стратегию обеспечения ИБ, расставляя приоритеты в развитии механизмов защиты и распределении ресурсов.

**3. Границы системы информационной безопасности**

Политика распространяется на все информационные системы компании, охватывая программное обеспечение, вычислительную технику, базы данных, сетевые инфраструктуры, а также организационные и кадровые процессы, связанные с обработкой информации. В организации предусмотрена строгая иерархия доступа к данным и контроль за использованием вычислительных мощностей.

Описание структуры компании и автоматизированных систем обработки информации, используемых в ЖЭС, позволяет определить уровень защиты, необходимый для конкретных ресурсов. К ним относятся серверное оборудование, рабочие станции сотрудников, средства связи и системы хранения данных. Данные ресурсы должны быть защищены в зависимости от их значимости, а политика безопасности должна предусматривать механизмы их классификации и контроля.

**4. Оценка рисков и возможные угрозы**

Процесс оценки рисков основывается на анализе вероятных угроз и их воздействия на работу компании. Одной из серьезных проблем являются несанкционированные попытки доступа к системам, которые могут быть вызваны как внешними, так и внутренними нарушителями. Особую опасность представляют вредоносное программное обеспечение, кибератаки, утечка данных вследствие ошибок сотрудников и социальная инженерия.

**Конкретные угрозы и их решения**

1. **Фишинговые атаки** – мошеннические письма, направленные на получение конфиденциальных данных сотрудников.
   * **Решение**: Внедрение спам-фильтров, регулярное обучение персонала, многофакторная аутентификация.
2. **Вирусы и вредоносное ПО** – могут привести к краже данных, нарушению работы систем.
   * **Решение**: Использование корпоративного антивирусного ПО, регулярное обновление системы, ограничение установки сторонних программ.
3. **DDoS-атаки** – перегрузка серверов искусственным трафиком, что приводит к недоступности сервисов.
   * **Решение**: Использование систем обнаружения атак, балансировщиков нагрузки, резервных серверов.
4. **Несанкционированный доступ к конфиденциальной информации** – попытки сотрудников или злоумышленников получить доступ к закрытым данным.
   * **Решение**: Разграничение прав доступа, шифрование информации, мониторинг активности пользователей.
5. **Физическое проникновение и кража оборудования** – потеря серверов, компьютеров, носителей информации.
   * **Решение**: Охранные системы, видеонаблюдение, биометрическая идентификация для доступа в помещения.
6. **Сбой оборудования и потеря данных** – выход из строя серверов, повреждение жестких дисков, стихийные бедствия.
   * **Решение**: Резервное копирование, дублирование серверов, хранение копий в разных локациях.
7. **Социальная инженерия** – манипуляции, заставляющие сотрудников раскрывать конфиденциальные данные.
   * **Решение**: Обучение персонала, ограничение распространения критической информации, строгие процедуры верификации запросов.

**5. Уровни защиты информации**

Политика информационной безопасности предполагает многослойную защиту, включающую административные, процедурные и программно-технические меры.

**Административный уровень** включает разработку политики безопасности, контроль за соблюдением регламентов и проведение обучения персонала. В рамках этого уровня проводятся регулярные аудиты безопасности, проверка соответствия сотрудников требованиям безопасности и разъяснительная работа.

**Процедурные меры** охватывают управление доступом к оборудованию, мониторинг действий сотрудников, а также планирование мероприятий по восстановлению данных и реагированию на инциденты. В рамках процедурных мер реализуются алгоритмы быстрого реагирования на инциденты, а также разрабатываются планы резервного копирования и восстановления.

**Программно-технические меры** реализуются через механизмы идентификации пользователей, аудит действий в системе, использование криптографической защиты, фильтрацию сетевого трафика и защиту периметра сети. Особое внимание уделяется технологиям шифрования данных, контролю за использованием информационных ресурсов и защите от атак извне.

**6. Реализация и контроль за выполнением политики**

Для успешного внедрения политики информационной безопасности компания реализует поэтапный процесс, включающий выбор стандартов и нормативных документов, оценку рисков, структуризацию контрмер и проведение сертификации информационных систем. Важной частью процесса является организация постоянного мониторинга уровня безопасности, регулярные проверки соответствия требованиям и пересмотр действующих регламентов с учетом новых угроз.

Для обеспечения высокого уровня осведомленности сотрудников проводятся тренинги, инструктажи и разъяснительные мероприятия. Работники компании должны понимать важность соблюдения норм ИБ и осознавать потенциальные риски, связанные с нарушением политики безопасности.

**7. Заключение**

Политика информационной безопасности компании ЖЭС является фундаментальным документом, регулирующим стратегию защиты данных и управления рисками. Реализация данного комплекса мер позволит минимизировать угрозы, повысить устойчивость системы к кибератакам и обеспечить надежную защиту всей информационной структуры организации.

Политика должна регулярно пересматриваться и дополняться в соответствии с актуальными угрозами, новыми технологиями и изменениями в законодательстве.

# **Лабораторная работа №4**

Цель: овладеть навыками настройки и использования брандмауэра Windows.

**Контрольные вопросы**

**1. Дайте определение понятию «брандмауэр».**

Брандмауэр (межсетевой экран) – это аппаратный или программный комплекс, позволяющий проверять (фильтровать) входные и выходные потоки данных, проходящие через интернет или сеть.

**2. Каково основное назначение брандмауэра?**

В случаи нарушения политики безопасности компьютера брандмауэр блокирует эти данные.

**3. Как создаются правила по ограничению доступа программ к сети?**

Для создания правила по ограничению доступа программ к сети необходимо открыть панель управления в меню «Пуск». В зависимости от версии операционной системы Windows может отображаться классический вид панели управления или с разделениями по категориям. На первом этапе необходимо включить брандмауэр, в случае если он был ранее выключен. Нужно выбрать в левой панели управления вкладку «Включение и отключение брандмауэра Windows». В появившемся окне переключаем параметры на значение «Включение брандмауэра Windows». Вторым этапом является настройка правил для входящих и исходящих подключений. Для этого выбираем вкладку «Дополнительные параметры». В открывшемся окне щелкаем мышью в левой панели по строке «Правила для входящих подключений», затем во вкладке меню «Действие» выбираем «Создать правило», либо нажимаем «Создать правило» в правой панели. В открывшемся мастере создания правила выбираем «Для программы», в случае если необходимо перекрыть доступ к сети конкретной программе, либо «Для порта» (например, если есть необходимость отключить часть возможностей программы). При ограничении работы программы далее необходимо указать ее путь обязательно через папку, в которой она установлена, а не через ярлыки. Далее указывается, какое именно действие вы хотите применить. В данном случае необходимо блокировать подключение. В следующем окне указываем имя правила. В общем списке появляется созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели. При двойном нажатии на правило отображаются его свойства. Аналогично создаются и правила для исходящих подключений.

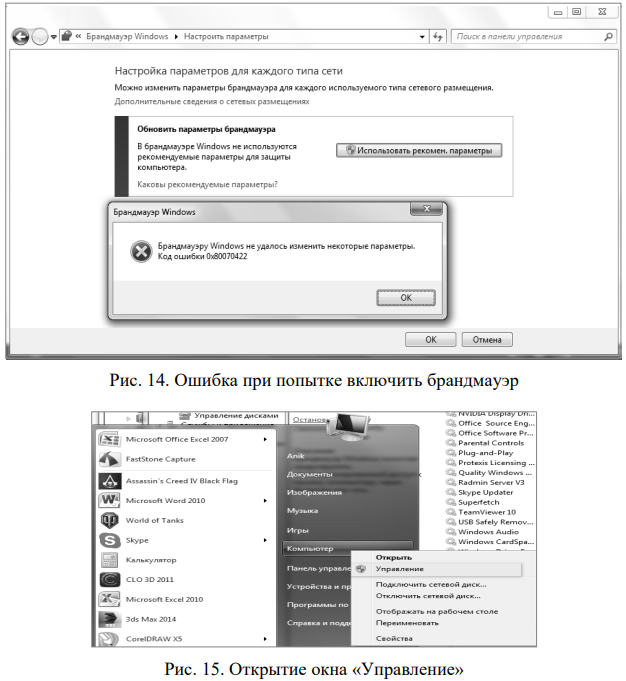
**4. Как можно вызвать командную строку?**

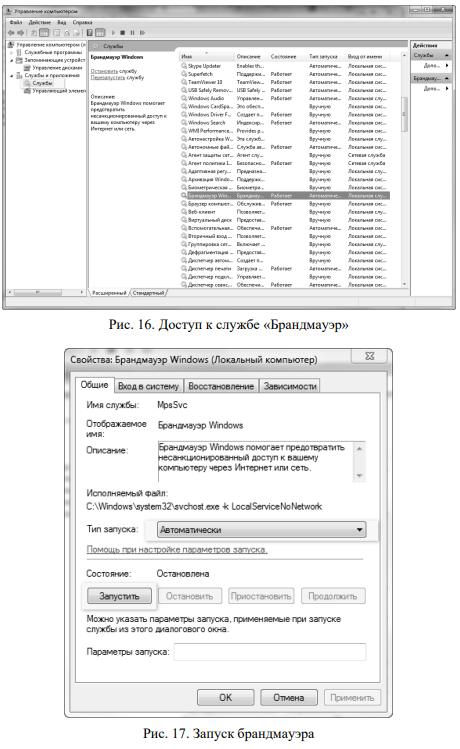
Чтобы вызвать командную строку в операционной системе Windows, выполните следующие шаги:

1. С помощью меню "Пуск":
   * Нажмите на кнопку "Пуск" (значок Windows) в левом нижнем углу экрана.
   * Введите в строке поиска "cmd" или "командная строка".
   * В результатах поиска выберите "Командная строка" или "Command Prompt".
2. С помощью сочетания клавиш:
   * Нажмите сочетание клавиш Windows + R, чтобы открыть окно "Выполнить".
   * Введите "cmd" и нажмите "Enter" или "ОК".
3. Запуск с правами администратора:
   * Откройте меню "Пуск" и введите "cmd" или "командная строка" в строке поиска.
   * В результатах поиска кликните правой кнопкой мыши на "Командная строка" и выберите "Запуск от имени администратора".

**5. Перечислите способы устранения возможных ошибок системы при включении брандмауэра**

При возникновении ошибок при попытке включить брандмауэр, например как на рис. 14, необходимо включить брандмауэр в соответствующих службах Windows s (рис. 15–17).



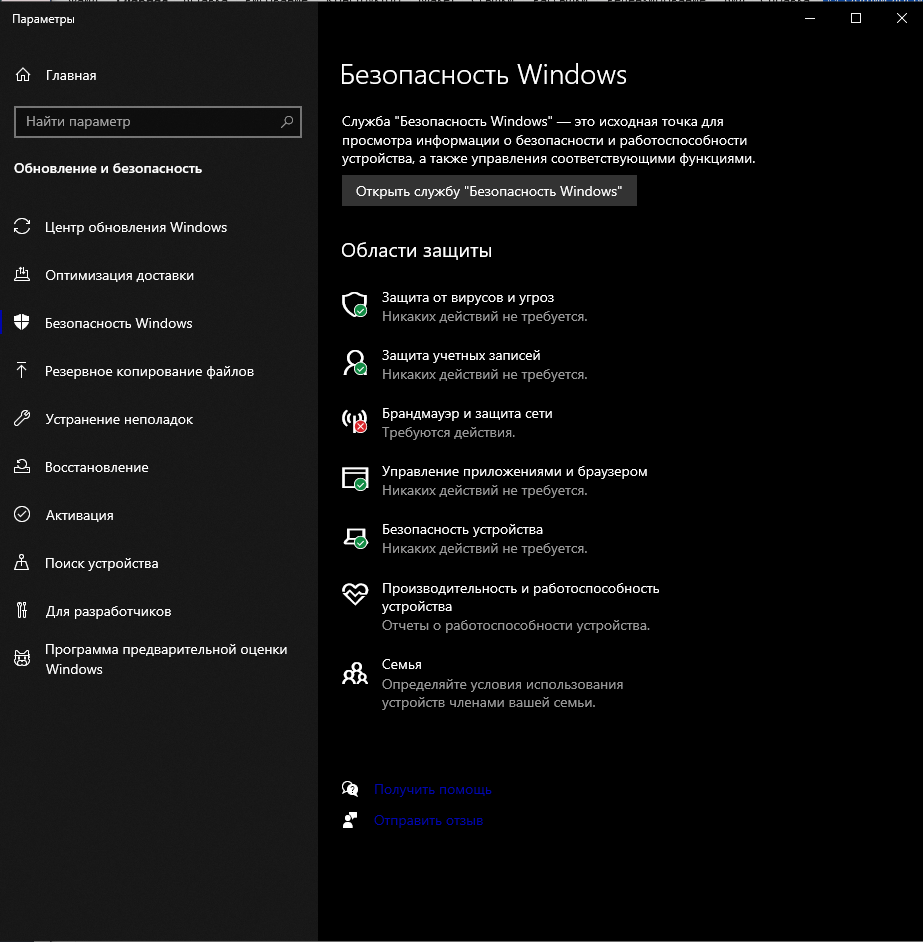


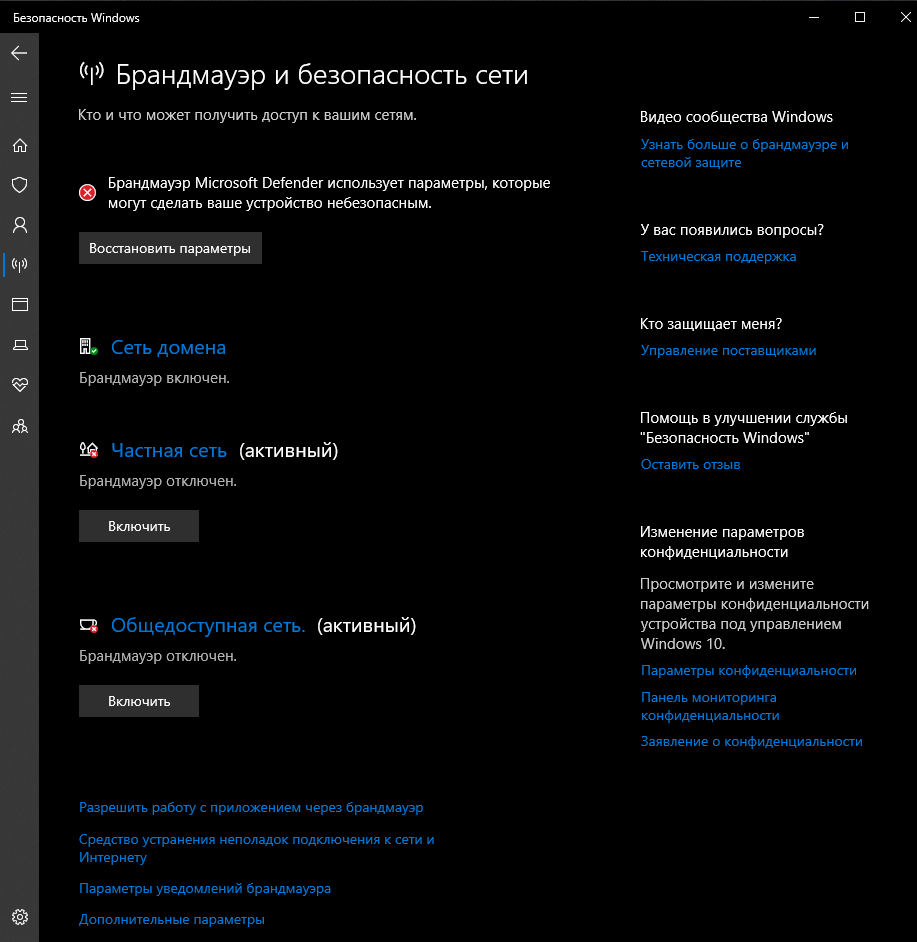
**Задание для выполнения**

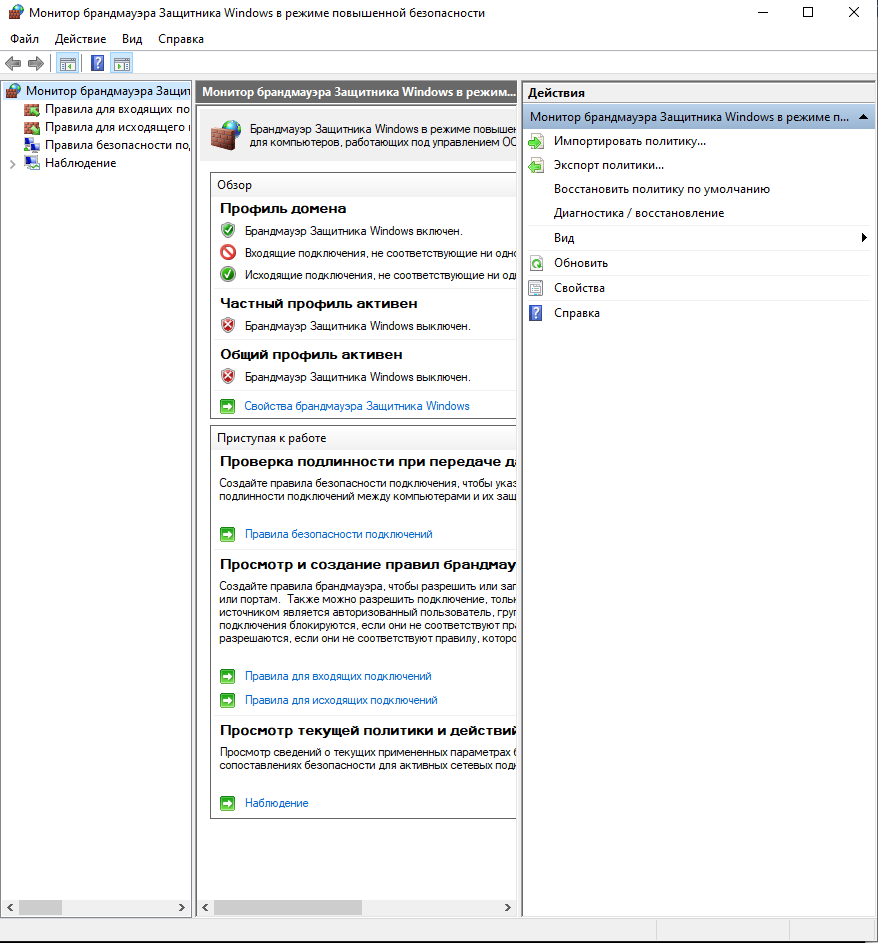
**1. Создание правил для входящих подключений**

a) Блокировка подключения для одной программы

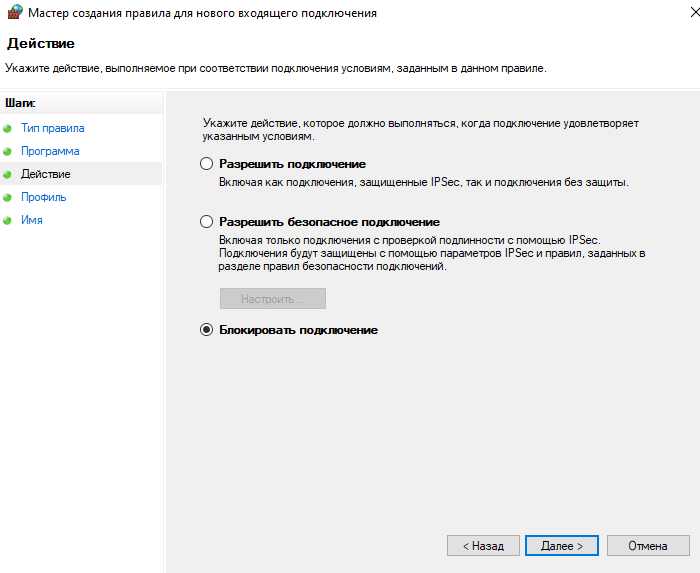
1. Откройте Панель управления и перейдите в раздел Система и безопасность.
2. В разделе "Система и безопасность" выберите Брандмауэр Windows Defender.
3. В левом меню выберите Дополнительные параметры.
4. В окне "Дополнительные параметры" выберите Правила для входящих подключений и нажмите Создать правило в правом меню.
5. Выберите Программа и нажмите Далее.
6. Укажите путь к исполняемому файлу программы, для которой хотите заблокировать подключение, и нажмите Далее.
7. Выберите Блокировать подключение и нажмите Далее.
8. Укажите профиль(и), к которым будет применено правило (доменный, частный, общественный) и нажмите Далее.
9. Назовите правило и нажмите Готово.

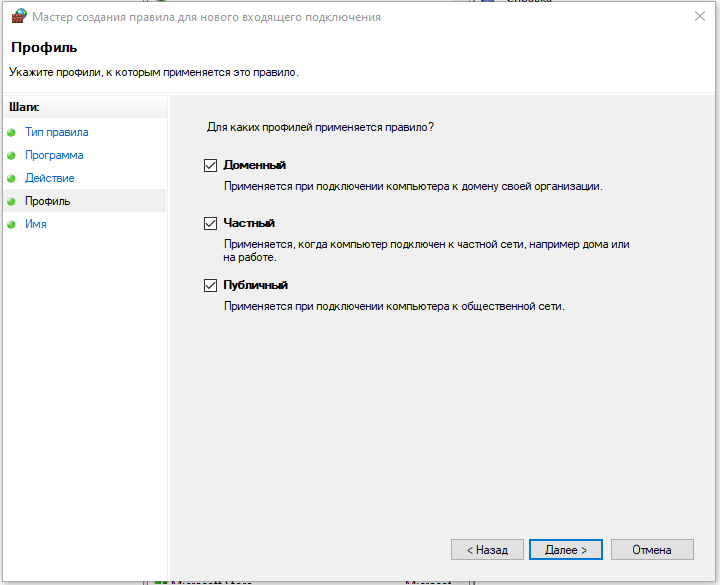






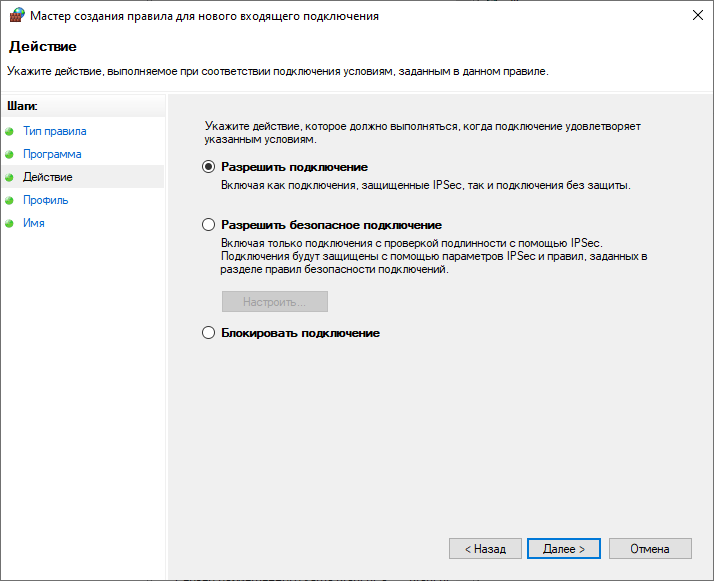


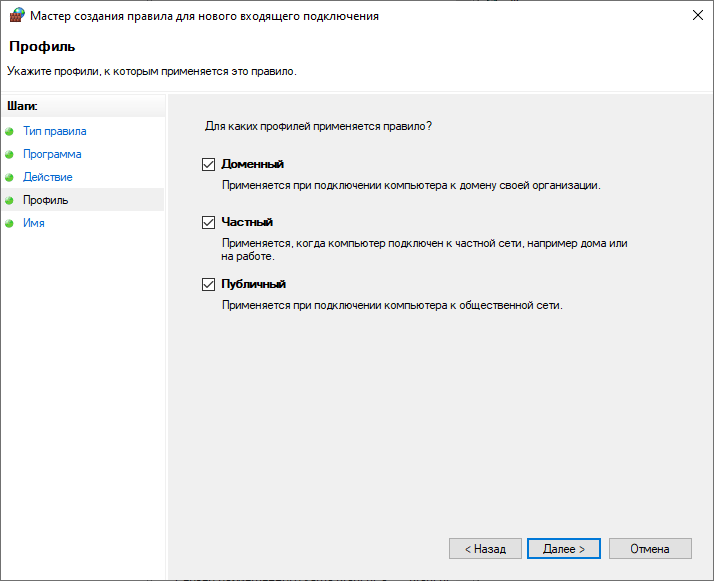




б) Разрешение подключения для одной программы

1. Повторите шаги 1-4 из предыдущего раздела.
2. Выберите Программа и нажмите Далее.
3. Укажите путь к исполняемому файлу программы, для которой хотите разрешить подключение, и нажмите Далее.
4. Выберите Разрешить подключение и нажмите Далее.
5. Укажите профиль(и), к которым будет применено правило (доменный, частный, общественный) и нажмите Далее.
6. Назовите правило и нажмите Готово.

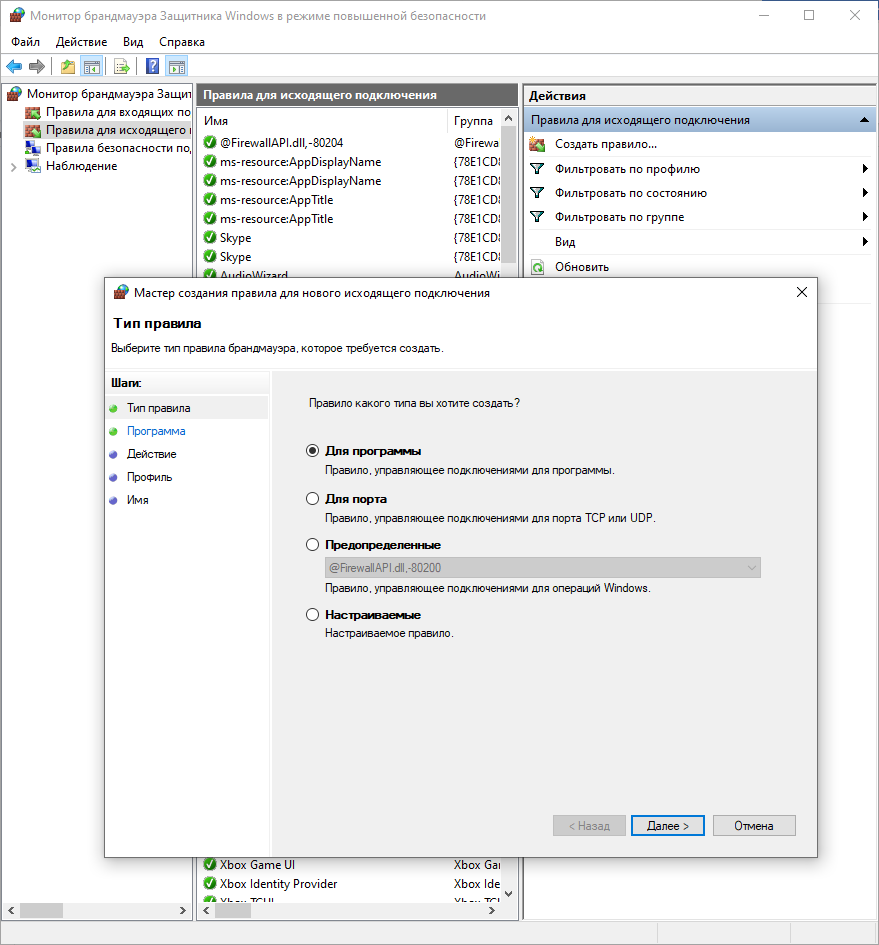


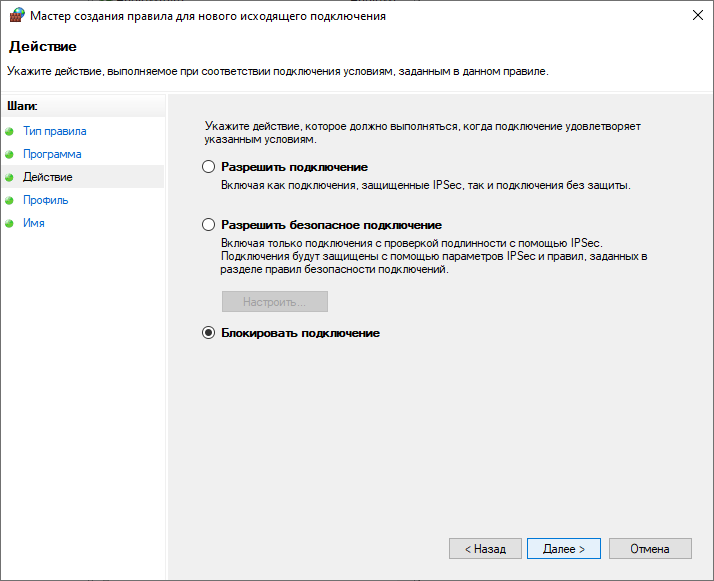


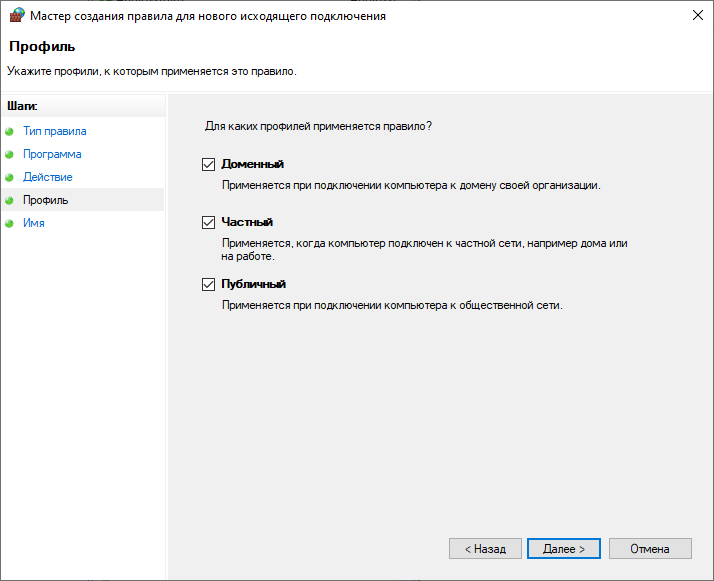
**2. Создание правил для исходящих подключений**

а) Блокировка подключения для одной программы

1. В окне "Дополнительные параметры" выберите Правила для исходящих подключений и нажмите Создать правило в правом меню.
2. Выберите Программа и нажмите Далее.
3. Укажите путь к исполняемому файлу программы, для которой хотите заблокировать подключение, и нажмите Далее.
4. Выберите Блокировать подключение и нажмите Далее.
5. Укажите профиль(и), к которым будет применено правило (доменный, частный, общественный) и нажмите Далее.
6. Назовите правило и нажмите Готово.

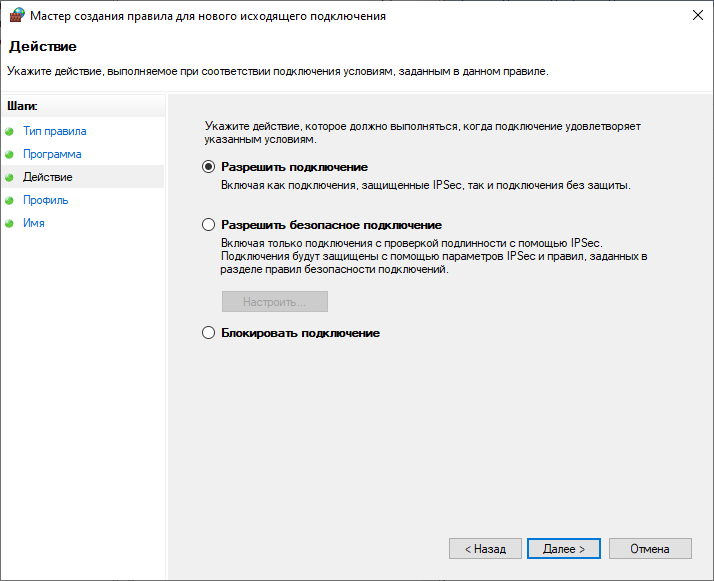


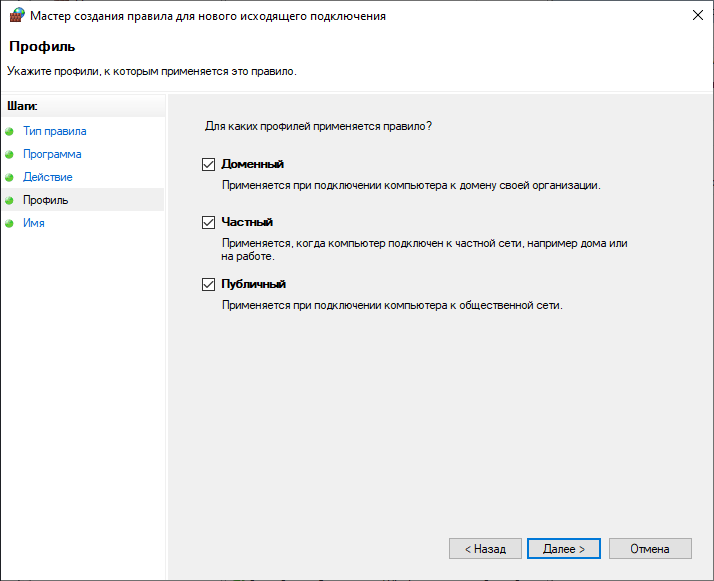




б) Разрешение подключения для одной программы

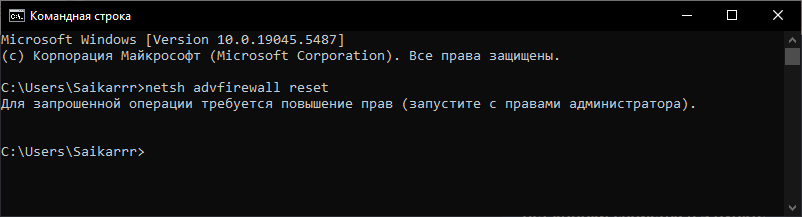
1. Повторите шаги 1-4 из предыдущего раздела.
2. Выберите Программа и нажмите Далее.
3. Укажите путь к исполняемому файлу программы, для которой хотите разрешить подключение, и нажмите Далее.
4. Выберите Разрешить подключение и нажмите Далее.
5. Укажите профиль(и), к которым будет применено правило (доменный, частный, общественный) и нажмите Далее.
6. Назовите правило и нажмите Готово.





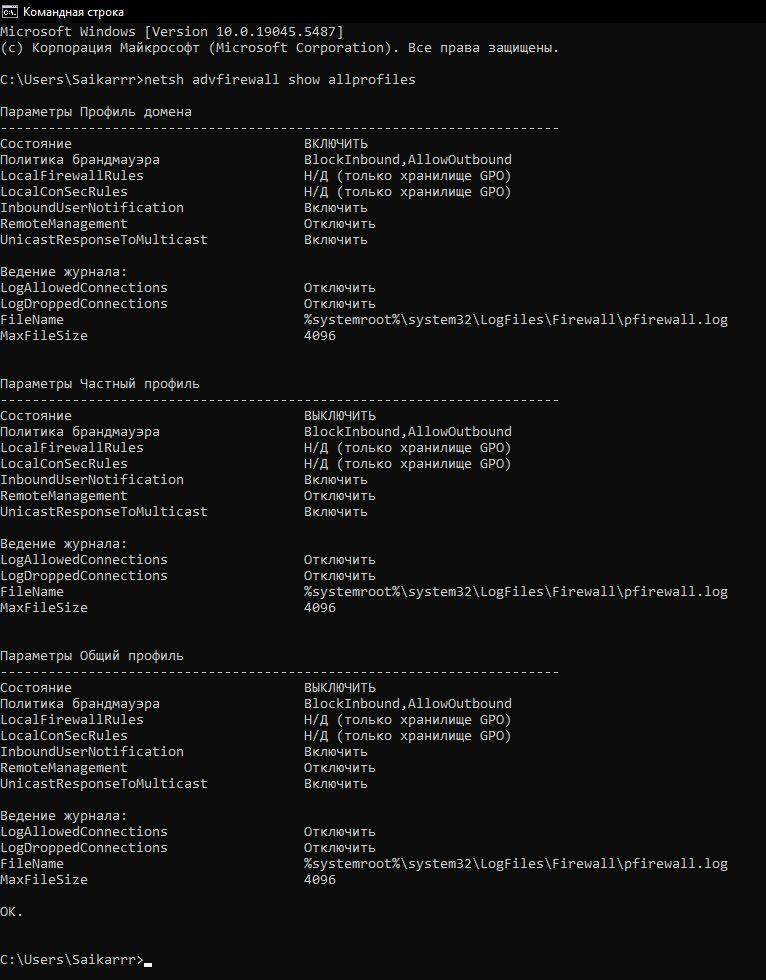
**3. Восстановление настроек брандмауэра в исходное состояние**

1. В окне "Дополнительные параметры" выберите Свойства в правом меню.
2. Во вкладке Общие выберите Восстановить значение по умолчанию и нажмите ОК.

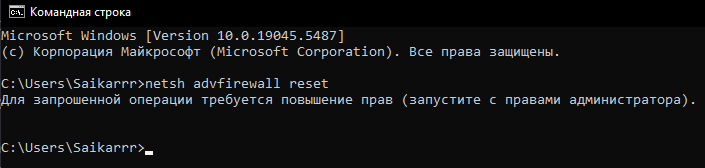


**4. Опробование действия нескольких команд**

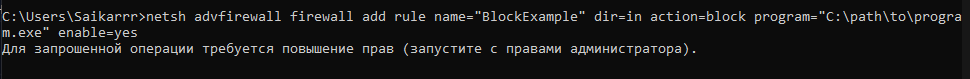
* Команда netsh advfirewall show allprofiles - отображает текущие настройки всех профилей брандмауэра.



* **Команда** netsh advfirewall reset - восстанавливает настройки брандмауэра по умолчанию.



* + **Команда** netsh advfirewall firewall add rule name="BlockExample" dir=in action=block program="C:\path\to\program.exe" enable=yes - добавляет правило для блокировки входящего подключения для указанной программы.



* + - Команда netsh advfirewall firewall add rule name="AllowExample" dir=in action=allow program="C:\path\to\program.exe" enable=yes - добавляет правило для разрешения входящего подключения для указанной программы.



# **Лабораторная работа №5**

Цель: Овладеть основными криптографическими алгоритмами симметричного шифрования.

**Контрольные вопросы**

**1. Что такое криптография?**

Криптография – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства) информации.

**2. В чем особенность симметричных криптосистем?**

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

Обмен информацией осуществляется в три этапа:

− отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);

− отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;

− получатель получает сообщение и расшифровывает его.

Если для каждого дня и для каждого сеанса связи будет использоваться уникальный ключ, это повысит защищенность системы.

**3. Что можно использовать в качестве ключа в симметричных криптосистемах?**

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

**4. Как происходит расшифровка сообщений в системе Виженера?**

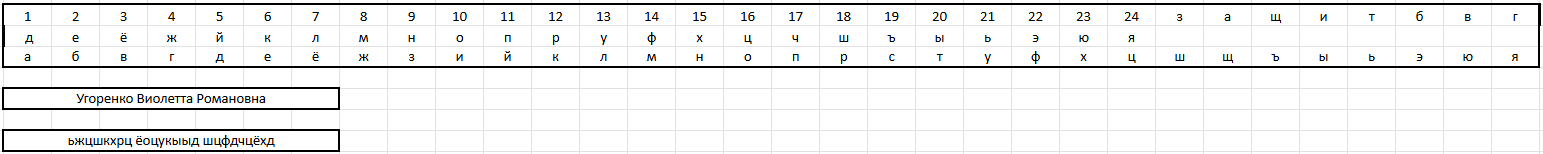
* Подготовка ключа: Ключевое слово повторяется столько раз, сколько необходимо, чтобы его длина совпала с длиной зашифрованного сообщения. Это позволяет каждой букве сообщения соответствовать своя буква ключа.
* Определение сдвига: Каждая буква ключа определяет, на сколько позиций назад по алфавиту нужно сдвинуть соответствующую букву зашифрованного текста. Например, если ключевая буква — «B», то сдвиг будет равен 1, если «C» — 2 и так далее (A соответствует 0).
* Обратный сдвиг: Каждая буква зашифрованного сообщения смещается по алфавиту в обратную сторону на указанное число позиций, определяемое буквой ключа. Это возвращает исходные буквы текста.
* Составление расшифрованного текста: После обратного сдвига всех букв получается оригинальное сообщение.

**5. Расскажите об алгоритме шифрования «двойной квадрат» Уитстона.**

* Подготовка двух квадратов: Создаются два 5x5 (или 6x6 в случае использования расширенного алфавита) квадрата, заполненные буквами алфавита. В классическом варианте буква «J» обычно объединяется с «I», чтобы вместить 26 букв в 5x5 квадрат. Ключевые слова или фразы используются для заполнения квадратов: сначала записывают уникальные буквы ключа, затем заполняют оставшиеся буквы алфавита.
* Разделение текста: Шифруемый текст разбивается на пары букв (диграммы). Если в паре встречаются одинаковые буквы, между ними вставляется «фиктивная» буква, например «X» (пример: «MEET» становится «ME XT»).
* Шифрование с использованием квадратов: Для каждой пары букв выполняются следующие операции: Найдите обе буквы в своих соответствующих квадратах. Если буквы находятся в одной строке, каждая из них заменяется на букву справа (циклический переход, если в конце строки). Если буквы находятся в одном столбце, замените их на буквы, находящиеся ниже (циклический переход вверх, если внизу). Если буквы формируют прямоугольник, каждая заменяется на букву в противоположном углу прямоугольника в той же строке.
* Результат: Все пары букв после применения вышеописанных правил формируют зашифрованное сообщение.

**Задание для выполнения**

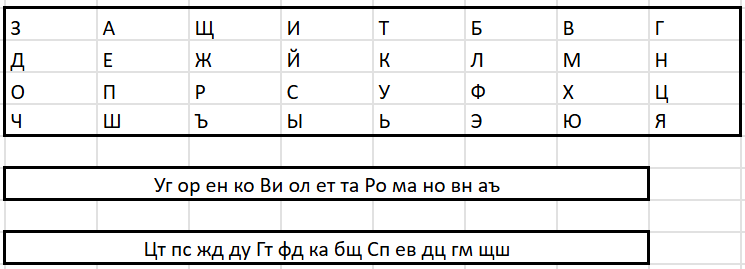
1) Шифр Цезаря(ключ 24)



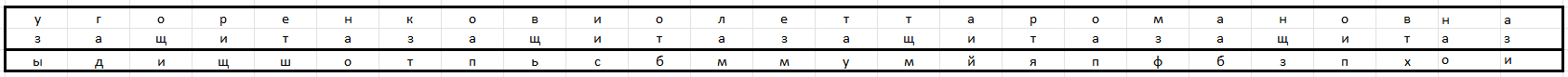
2)Шифр Трисемуса (защита)

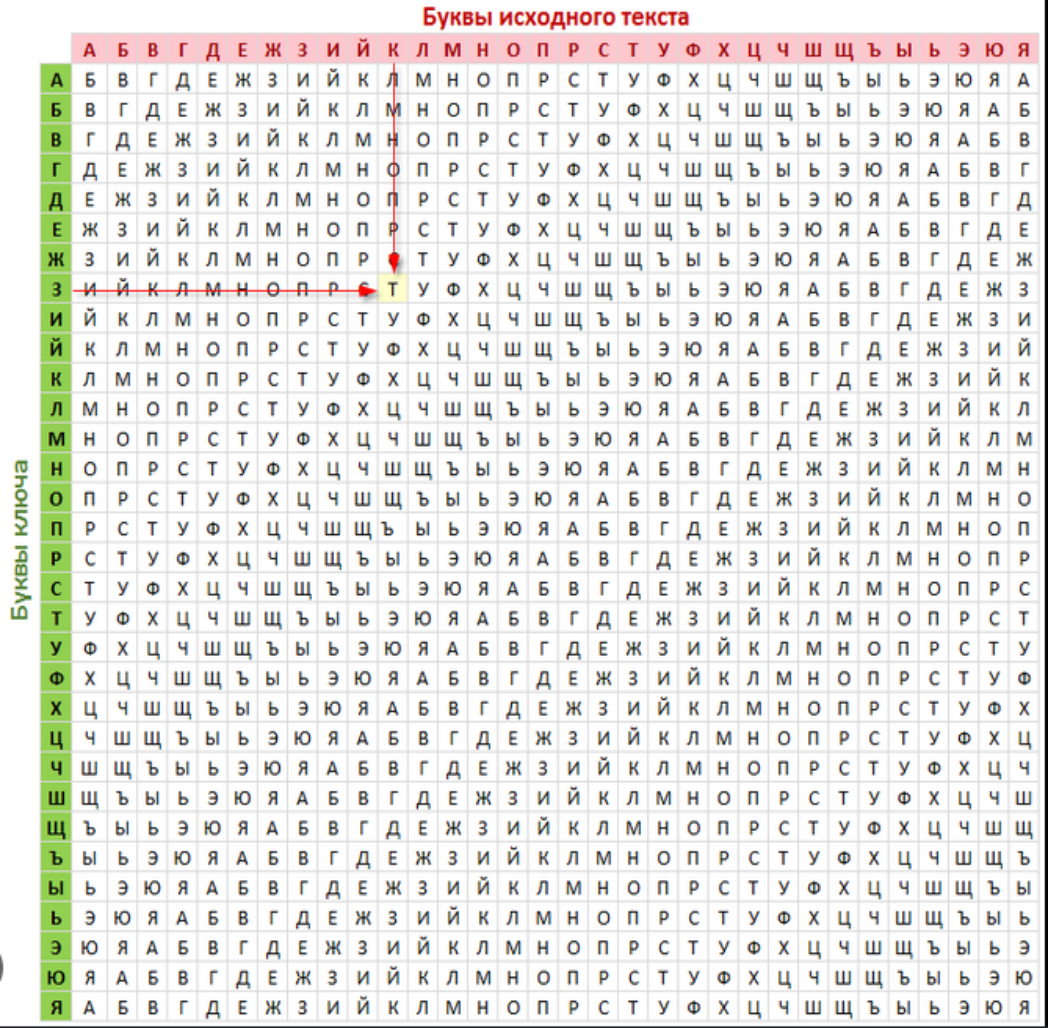


3)Шифр Плейфейра (защита)

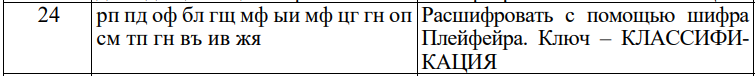


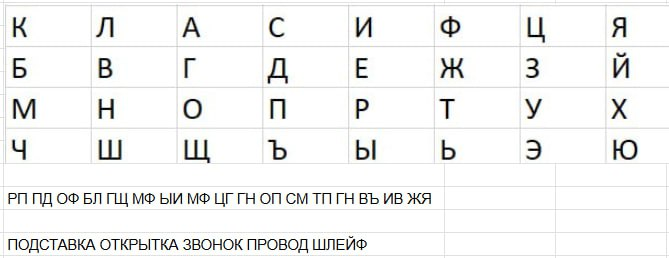
4)Шифр Виженера (защита)





**Задание 3 (Вариант 24)**





# **Лабораторная работа №6**

Цель: Овладеть основными криптографическими алгоритмами асимметричного шифрования.

**Контрольные вопросы**

**1. В чем особенность асимметричных криптосистем?**

Ассиметричная система шифрования ассиметрична, потому что не требует использования идентичных ключей отправителем и получателем шифрованного сообщения. Она является системой с открытым ключом, так как один из ключей не содержится в секрете.

**2. С помощью какого ключа происходит шифрование сообщения?**

Ассиметричная система шифрования использует открытый ключ, который передается по открытому каналу и предназначен для шифрования сообщения.

Шифрование на открытом ключе базируется на двух различных ключах, составляющих пару, но не идентичных. В шифровании с асимметричным ключом каждый ключ является уникальным. Пара ключей «открытый/секретный» работает сообща: один ключ предназначен для шифрования данных, а другой – для расшифровки, и наоборот. Секретный ключ должен содержаться в секретности в целях безопасности, а открытый ключ может передаваться по небезопасному соединению без угрозы для системы. Следовательно, система шифрования на открытом ключе решает одну из главных проблем старых систем шифрования, заключающуюся в безопасном способе передачи ключа шифрования другой стороне.

**3. В чем особенность алгоритма Диффи – Хеллмана?**

Реализация элементов схемы шифрования Диффи – Хеллмана. В 1976 г. после публичной критики алгоритма DES и указания на сложность обработки секретных ключей Уитфилд Диффи (Whitfield Diffie) и Мартин Хеллман (Martin Hellman) опубликовали свой алгоритм обмена ключами. Это была первая публикация на тему криптографии с открытым ключом и, воз- можно, самый большой шаг вперед в области криптографии, сделанный когда-либо.

Из-за невысокого быстродействия, свойственного асимметричным алгоритмам, алгоритм Диффи – Хеллмана не предназначен для шифрования данных. Он был ориентирован на передачу секретных ключей DES, ARS или других подобных алгоритмов через небезопасную среду. В большинстве случаев алгоритм Диффи – Хеллмана не используется для шифрования сообщений, потому что он, в зависимости от реализации, от 10 до 1000 раз медленнее алгоритма DES.

**4. Какие недостатки можно выделить в асимметричных криптосистемах?**

1. Скорость работы

Асимметричные алгоритмы, как правило, медленнее, чем симметричные. Шифрование и дешифрование больших объемов данных может занимать значительное время.

1. Больший размер ключей

Для достижения того же уровня безопасности, что и в симметричных системах, асимметричные алгоритмы требуют гораздо больших ключей. Это увеличивает объем хранимой информации и время обработки.

1. Уязвимость к определенным атакам

Некоторые асимметричные алгоритмы могут быть уязвимы к атакам, основанным на математических свойствах, таких как атаки на основе квантовых вычислений.

1. Сложность реализации

Асимметричные криптосистемы сложнее в реализации и требуют более тщательного управления ключами. Это может приводить к ошибкам в конфигурации и использованию.

1. Проблемы с распределением ключей

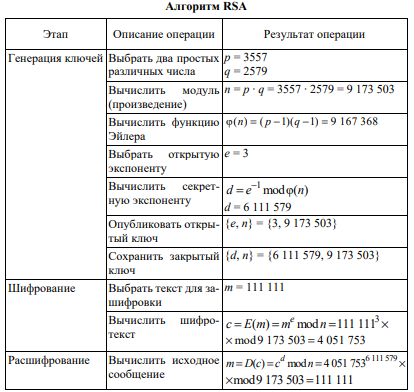
Хотя асимметричные системы упрощают распределение публичных ключей, существует риск подмены (атаки «человек посередине»), если не используется надежный механизм проверки подлинности ключей.

**Задание для выполнения**

**1. Объясните процесс работы алгоритма RSA.**

**Генерация ключей:**

* Выбираются два простых различных числа p и q.
* Вычисляется модуль n=p⋅q.
* Вычисляется функция Эйлера ϕ(n)=(p−1)(q−1).
* Выбирается открытая экспонента e, которая является взаимно простым числом с ϕ(n).
* Вычисляется секретная экспонента d как d=e−1mod  ϕ(n).
* Открытый ключ — это пара (e,n), а закрытый ключ — пара (d,n).



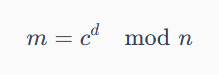
**Шифрование:**

Сообщение m шифруется с использованием открытого ключа:



**Расшифрование:**

Шифротекст c расшифровывается с использованием закрытого ключа:



**Особенности алгоритма RSA:**

*Безопасность***:** Основана на сложности задачи факторизации больших целых чисел.

*Использование***:** Применяется как для шифрования, так и для цифровых подписей.

*Эффективность*: Медленнее симметричных алгоритмов, поэтому часто используется для передачи ключей.

*Длина ключа:* Требует более длинные ключи для обеспечения аналогичной криптостойкости по сравнению с симметричными алгоритмами.

**2. Объясните процесс работы алгоритма Диффи – Хеллмана.**

**Генерация ключей:**

* Два участника согласовывают два числа: большое простое число pp и примитивный корень g.
* Каждый участник генерирует свой секретный ключ a или b.
* Вычисляются открытые ключи: A=g^a mod  p и B=g^b mod  p

**Обмен ключами:**

* Участники обмениваются открытыми ключами A и B.
* Каждый участник вычисляет общий секретный ключ: s=B^a mod p или s=A^b mod p.

**Особенности алгоритма Диффи – Хеллмана:**

*Обмен ключами*: Используется для безопасного обмена ключами, а не для шифрования данных.

*Безопасность*: Основана на сложности вычисления дискретных логарифмов.

*Эффективность*: Медленнее симметричных алгоритмов, но обеспечивает высокий уровень безопасности.

*Применение*: Часто используется для установления сеансовых ключей в протоколах безопасности.

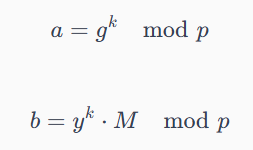
**3. Объясните процесс работы алгоритма Эль-Гамал.**

**Генерация ключей:**

* Выбирается случайное простое число p длиной n бит.
* Выбирается случайный примитивный элемент g.
* Выбирается случайное целое число x такое, что 1<x<p−1.
* Вычисляется y=g^x mod p.
* Открытым ключом является тройка (p,g,y), а закрытым ключом — число x.

**Шифрование:**

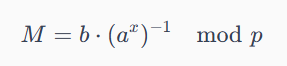
* Выбирается сессионный ключ — случайное целое число k такое, что 1<k<p−1.
* Вычисляются числа a и b по формулам:



* Пара чисел (a,b) является шифротекстом.

**Расшифрование:**

* Исходное сообщение M вычисляется из шифротекста (a,b) по формуле:



**Особенности алгоритма Эль-Гамаля:**

* *Длина шифротекста*: Шифротекст в два раза длиннее исходного сообщения.
* *Безопасность*: Основана на сложности вычисления дискретных логарифмов.
* *Применение*: Часто используется для цифровых подписей и обмена ключами.
* *Гибкость*: Может быть использован как для шифрования, так и для цифровых подписей.

# **Лабораторная работа №7**

Цель: Изучить и закрепить умение реализации электронноцифровой подписи на примере RSA.

**Контрольные вопросы**

*Лабораторная работа №7*

***1. Объясните последовательность выполнения процедур генерации и проверки ЭЦП.***

**Генерация ЭЦП:**

1. Отправитель вычисляет хеш сообщения.
2. Шифрует этот хеш своим закрытым ключом – это и есть подпись.
3. Отправляет сообщение и подпись получателю.

**Проверка ЭЦП:**

1. Получатель вычисляет хеш от полученного сообщения.
2. Расшифровывает подпись открытым ключом отправителя.
3. Если оба хеша совпадают – подпись подлинная, сообщение не изменялось.

***2. Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.***

**1. Генерация ключей.** Отправитель и получатель генерируют свои открытые и закрытые ключи.

**2. Подписание сообщения.** Отправитель хеширует сообщение, шифрует хеш закрытым ключом и отправляет сообщение с подписью.

**3. Проверка подписи.** Получатель вычисляет хеш сообщения, расшифровывает подпись открытым ключом отправителя и сравнивает хеши. Если совпадают – подпись действительна.

***3. Опишите схему протокола ЭЦП на основе алгоритма RSA.***

**1. Генерация ключей.**

Пользователи создают пару ключей (открытый и закрытый).

**2. Формирование подписи.**

Отправитель шифрует хеш сообщения своим закрытым ключом, а затем открытым ключом получателя.

**3. Расшифровка сообщения.**

Получатель сначала расшифровывает сообщение своим закрытым ключом, затем открытым ключом отправителя. Если результат совпадает с ожидаемым, подпись верна.

# **Лабораторная работа №8**

Цель: Получить основные сведения из курса теории чисел.

**Контрольные вопросы**

**1. Сформулируйте алгоритм Евклида нахождения наибольшего общего делителя целых чисел.**

**Алгоритм Евклида** – это алгоритм нахождения наибольшего общего делителя (НОД) пары целых чисел.

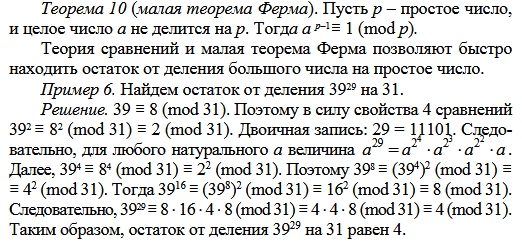
**2. Что значит расширенный алгоритм Евклида?**

Расширенный алгоритм Евклида — это расширение [алгоритма Евклида](https://ru.ruwiki.ru/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%95%D0%B2%D0%BA%D0%BB%D0%B8%D0%B4%D0%B0), которое вычисляет, кроме [наибольшего общего делителя](https://ru.ruwiki.ru/wiki/%D0%9D%D0%B0%D0%B8%D0%B1%D0%BE%D0%BB%D1%8C%D1%88%D0%B8%D0%B9_%D0%BE%D0%B1%D1%89%D0%B8%D0%B9_%D0%B4%D0%B5%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C) (НОД) целых чисел a a и bb , ещё и коэффициенты [соотношения Безу](https://ru.ruwiki.ru/wiki/%D0%A1%D0%BE%D0%BE%D1%82%D0%BD%D0%BE%D1%88%D0%B5%D0%BD%D0%B8%D0%B5_%D0%91%D0%B5%D0%B7%D1%83), то есть целые x x и yy , такие что ax + by = НОД(a,b)

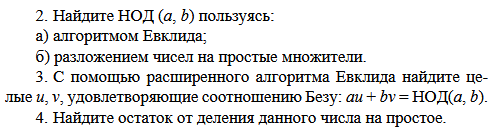
**3. Какие числа называются взаимно простыми?**

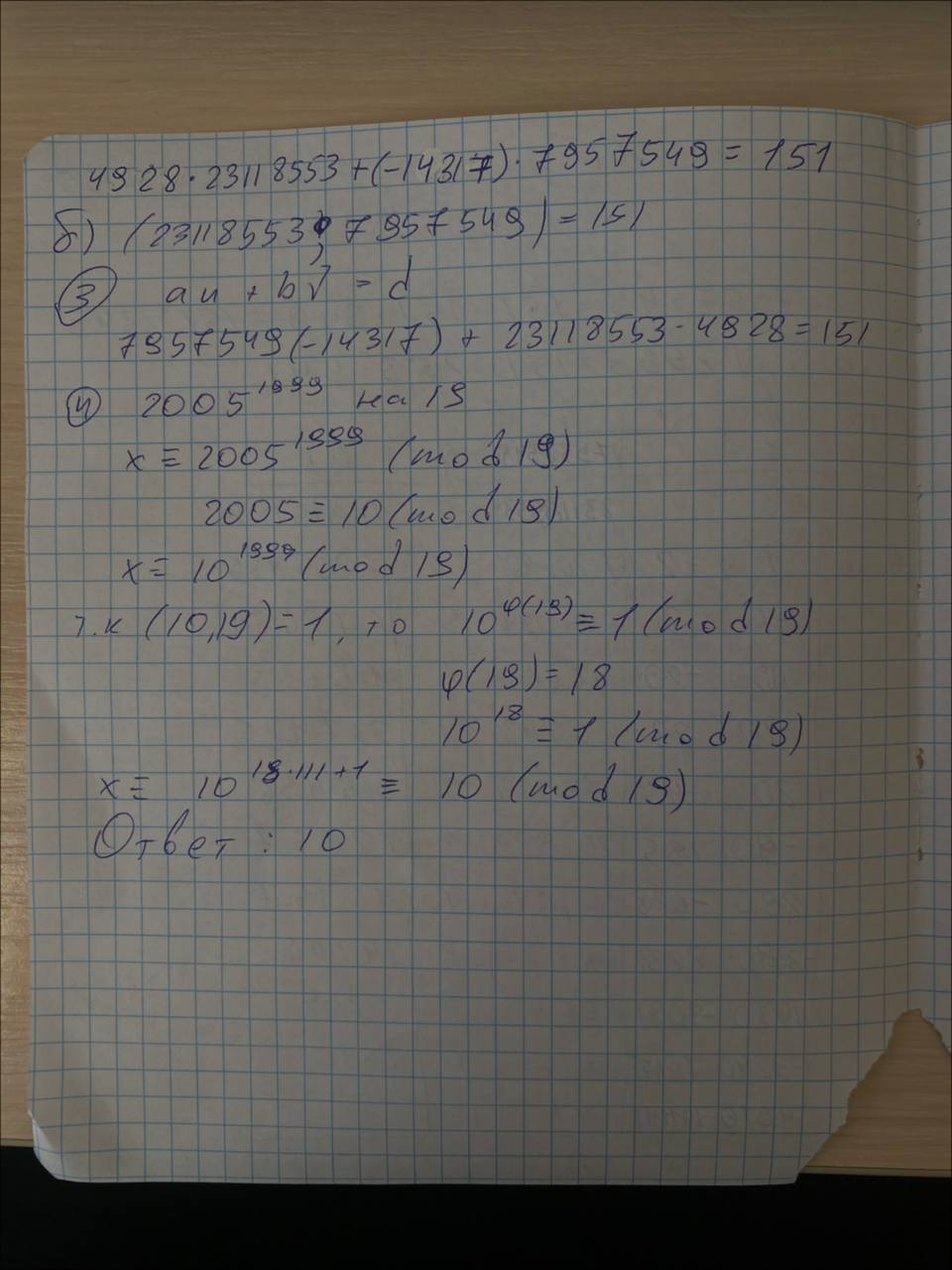
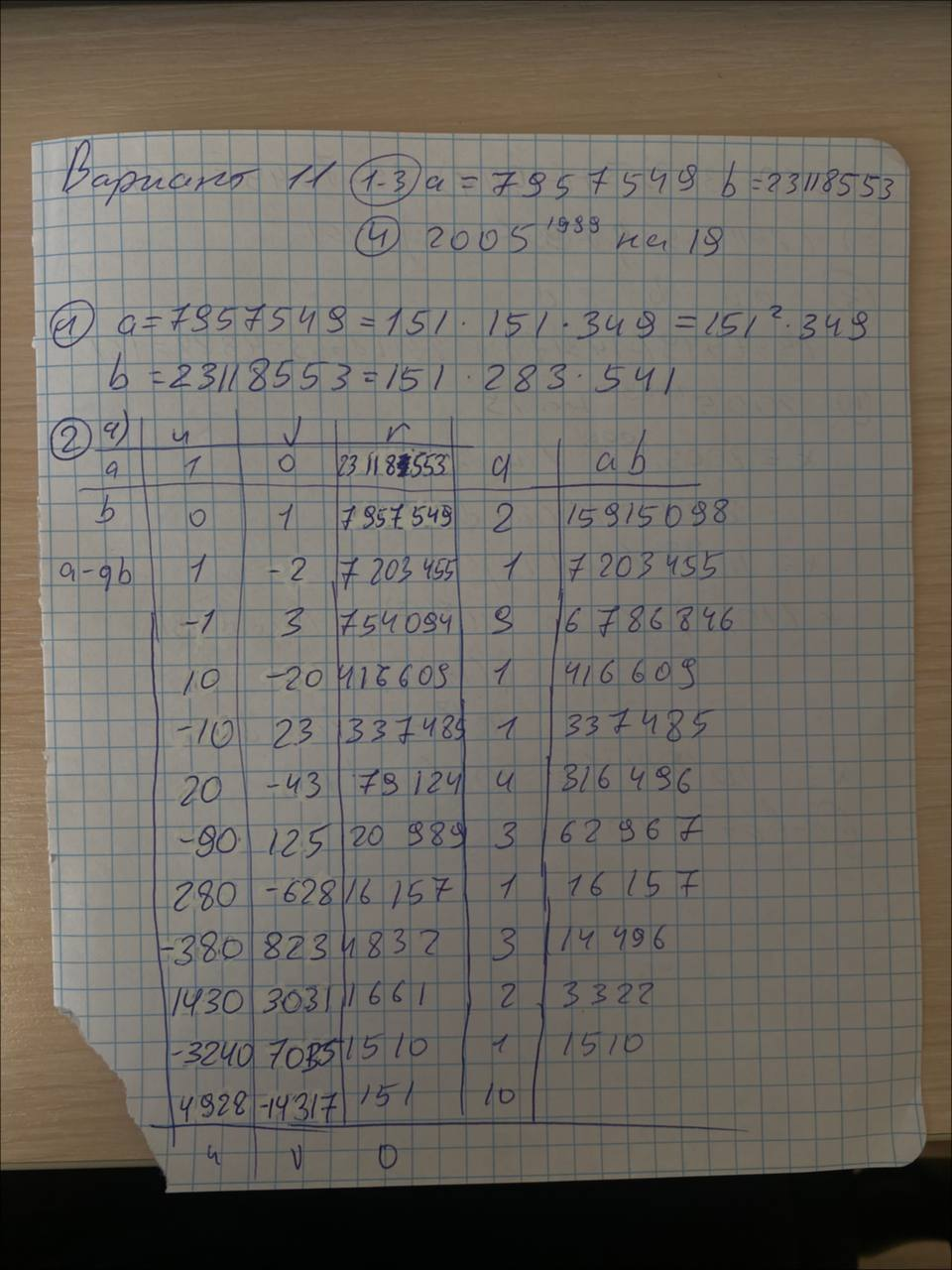
Целые числа a и b называются взаимно простыми, если НОД (a, b) = 1

**4. Объясните малую теорему Ферма.**



**Задание для выполнения**





# **Лабораторная работа №9**

Цель: Изучить основные положения авторского права и смежных прав.

**Контрольные вопросы**

1. **На какие объекты распространяется авторское право?**

Авторское право распространяется как на обнародованные, так и на необнародованные произведения, существующие в какой-либо объективной форме:

− письменной (рукопись, машинопись, нотная запись и др.);

− устной (публичное произнесение, публичное исполнение и др.);

− звуко- или видеозаписи (механическая, магнитная, цифровая, оптическая и др.);

− изображения (рисунок, эскиз, картина, карта, план, чертеж, кино-, теле-, видео-, фотокадр и др.);

− объемно-пространственной (скульптура, модель, макет, сооружение и др.);

− электронной, в том числе цифровой.

**Объекты авторского права:**

− литературные произведения;

− драматические и музыкально-драматические произведения, произведения хореографии и пантомимы и другие сценарные произведения;

− музыкальные произведения с текстом и без текста;

− аудиовизуальные произведения;

− произведения изобразительного искусства;

− произведения прикладного искусства и дизайна;

− произведения архитектуры, градостроительства и садово-паркового искусства;

− фотографические произведения, в том числе произведения, полученные способами, аналогичными фотографии;

− карты, планы, эскизы, иллюстрации и пластические произведения, относящиеся к географии, картографии и другим наукам;

– компьютерные программы (прикладные программы и операционные системы на любом языке и в любой форме, включая исходный текст и объектный код; базы данных или компиляции иных материалов в любой форме, представляющие собой по подбору и расположению материалов результат интеллектуального творчества);

− произведения науки;

− производные произведения (переводы, обработки, инсценировки, музыкальные аранжировки, обзор, аннотации, рефераты; сборники произведений: энциклопедии, антологии, атласы и другие составные произведения как результат творческого труда);

− составные произведения – сборники.

**Не являются** объектами авторского права:

– официальные документы (правовые акты, судебные постановления, иные документы административного и судебного характера, учредительные документы организаций), а также их официальные переводы;

− государственные символы и знаки (флаг, герб, гимн, государственные награды, денежные и иные знаки, почтовые марки);

− произведения народного творчества, авторы которых не известны.

Авторское право не распространяется на собственно идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты, даже если они выражены, отображены, объяснены или воплощены в произведении.

1. **Что относится к личным неимущественным правам?**

Авторские права делятся на личные неимущественные (моральные права – droit moral) и имущественные (экономические) права (рис. 21).

Личные неимущественные права:

− признаваться автором произведения (право авторства);

− использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом либо без обозначения имени, т. е. анонимно (право на имя);

− обнародовать или разрешать обнародовать произведение в любой форме (право на обнародование), включая право на отзыв;

− право на защиту произведения, включая его название, от всякого рода искажений или любого иного посягательства, способных нанести ущерб чести и достоинству автора (право на защиту репутации автора).

Личное неимущественное право принадлежат автору независимо от его имущественных прав и сохраняется за ним даже после уступки исключительных прав на использование произведения.

1. **Что относится к личным имущественным правам?**

Имущественные права – исключительное право осуществлять или разрешать осуществлять следующие действия:

− воспроизведение произведения;

− распространение оригинала или экземпляров произведения посредством продажи или иной передачи права собственности;

− прокат оригиналов или экземпляров компьютерных про-

грамм, баз данных, аудиовизуальных произведений, нотных текстов музыкальных произведений и произведений, воплощенных в фонограммах;

− импорт экземпляров произведения;

− публичный показ оригинала или экземпляра произведения;

− публичное исполнение произведения;

− передачу произведения в эфир;

− иное сообщение произведения для всеобщего сведения;

− перевод произведения на другой язык;

− переделку или иную переработку произведения.

**Авторские**

**права**

**Личные**

**неимущественные**

**права**

право

авторства

право

на

имя

право

на

неприкосновенность

произведения

право

на

обнародование

право

на

отзыв

воспроизведение

распространение

прокат

импорт

публичный

показ

публичное

исполнение

передача

в

эфир

передача

по

кабелю

иное

сообщение

для

всеобщего

сведения

перевод

переработка

иные

возможные

способы

использования

произведения

иные

имущественные

права

:

–

право

следования

;

–

право

на

получение

вознаграждения

за

воспроизведение

произведений

в

лич

-

ных

целях

**Имущественные**

**права**

**,**

**исключительное**

**право**

1. **Каковы особенности авторского права на составные произведения?**

Авторское право на составные произведения:

− автору сборника и других составных произведений (составителю) принадлежит авторское право на осуществленные им подбор и распоряжение материалов как результат творческого труда (составительство);

− составитель пользуется авторским правом при условии соблюдения им прав авторов каждого из произведений, включенных в составное;

− авторы произведений, включенных в составное произведение, вправе использовать свои произведения независимо от составного произведения, если иное не предусмотрено авторским договором;

− авторское право составителя не препятствует другим лицам осуществлять самостоятельный подбор и расположение тех же материалов для создания своих составных произведений;

− лицу, выпускающему в свет энциклопедии, энциклопедические словари, периодические и продолжающиеся сборники научных трудов, газеты, журналы и другие периодические издания, принадлежат исключительные права на использование таких изданий в целом. Это лицо вправе при любом использовании таких изданий указывать свое наименование или требовать такого указания;

− авторы произведений, включенных в такие издания, сохраняют исключительные права на использование своих произведений независимо от издания в целом, если иное не предусмотрено авторским договором.

1. **Каков срок действия авторского права?**

Неимущественное право (право авторства, право на имя и право на защиту репутации автора) охраняются бессрочно. Имущественные права действуют в течение всей жизни автора (соавторов) и 50 лет после его (последнего соавтора) смерти.

Общественное достояние по истечении срока действия имущественных прав на объекты авторского права или смежных прав означает переход этих объектов в общественное достояние, т. е. они могут свободно использоваться любым физическим или юридическим лицом без выплаты вознаграждения.

Переход авторского права по наследству, кроме прав авторства, на имя и на защиту репутации автора действует без ограничения срока.

Автор вправе указать лицо, на которое он возлагает охрану своих личных неимущественных прав после своей смерти и которое осуществляет свои полномочия пожизненно. При отсутствии указаний охрана осуществляется его наследниками или специально уполномоченным государственным органом Республики Беларусь при отсутствии наследников.

1. **Кто является субъектом авторского права?**

Субъекты авторского права и смежных прав. Субъектом авторского права, как правило, является гражданин, творческим трудом которого создано произведение науки, литературы или искусства. Им может быть и гражданин, не достигший восемнадцатилетнего возраста, и душевнобольной. Так, авторские права детей, представленные на смотры или выставки детской или юношеской самодеятельности и т. д., защищаются авторским правом.

Но недееспособные, став субъектами авторского права, не имеют права самостоятельно совершать какие-либо сделки, связанные с использованием авторского права. Несовершеннолетние в возрасте от 14 до 18 лет могут самостоятельно осуществлять авторские права на свои произведения.

За авторами – гражданами Республики Беларусь и их правопреемниками авторское право признается на все произведения независимо от места их обнародования или нахождения в какой-либо объективной форме.

Если произведение обнародовано либо не обнародовано, но существует на территории Республики Беларусь в какой-либо объективной форме, то авторское право распространяется на такое произведение независимо от гражданства автора.

За гражданами других государств, обнародовавшими свои произведения за пределами Республики Беларусь, авторское право признается в соответствии с международными договорами Республики Беларусь.

# **Лабораторная работа №10**

1. **Что такое патентное исследование?**

Целью патентных исследований является определение уровня техники, который используется для проверки соответствия заявленного изобретения условиям патентоспособности «новизна» и «изобретательский уровень».

Патентное исследование проводится на основании формулы изобретения с учетом описания и чертежей, если они имеются, а также с учетом изменений формулы изобретения, принятых во внимание при рассмотрении заявки.

При определении уровня техники общедоступными считаются сведения, содержащиеся в источниках информации, с которыми любое лицо может ознакомиться само либо о содержании которых ему может быть законным путем сообщено.

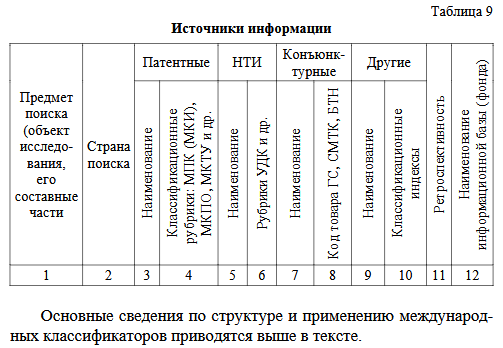
1. **Что такое патентная чистота?**

Патентная чистота — это юридическое свойство объекта. Если объект обладает патентной чистотой, значит, его можно свободно использовать в стране, по которой проводилась проверка, без риска нарушить действующие на ее территории [патенты](https://onlinepatent.ru/uslugi/patent-na-izobretenie/) третьих лиц.

Когда разработчик (сам изобретатель или компания) выводит продукт на новый рынок, ему важно снизить финансовые риски — нужно заранее узнать, есть ли на этом рынке действующие патенты на такой продукт или его составные части — чтобы это узнать, проводят проверку патентной чистоты.

Если найдутся мешающие патенты, производитель может исключить использование чужих патентов и так снизить вероятность получения претензий от правообладателей и возникновения убытков.

1. **В чем заключается этап разработки регламента поиска?**

Разработка регламента поиска. Регламент поиска включает выбор источников информации страны, в которой будет вестись поиск, его ретроспективу и указание источников (этот этап оформляется в виде табл. 9). 

1. **Что включает в себя этап систематизации и анализа отобранной документации?**

Систематизация и анализ отобранной документации. По выявленным в процессе поиска документам, требующим, например, в случае нарушения прав объектов промышленной собственности незамедлительного принятия решений руководством организации, выводы и рекомендации исполнителей патентных исследований оформляются в виде экспертного заключения



1. **Как происходит оформление результатов исследований в виде отчета о патентных исследованиях?**

Оформление результатов исследований в виде отчета о патентных исследованиях. Отчет о патентных исследованиях должен содержать:

− титульный лист;

− список исполнителей;

− содержание;

− перечень сокращений, условных обозначений, символов, единиц, терминов;

− общие данные об объекте исследования;

− основную (аналитическую) часть;

− заключение;

− приложения.

Каждый из разделов аналитической части (ее содержание определяет третий этап) должен включать:

− анализ и обобщение информации в соответствии с поставленными перед патентными исследованиями задачами;

− выводы и рекомендации для достижения конечного результата данной работы;

− оценку соответствия результатов патентных исследований заданию на их проведение, обоснование необходимости проведения дополнительных исследований.

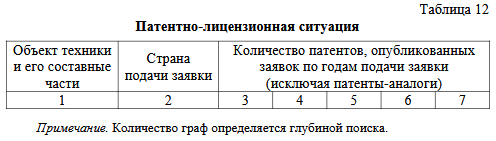
В заключении в общем случае приводят:

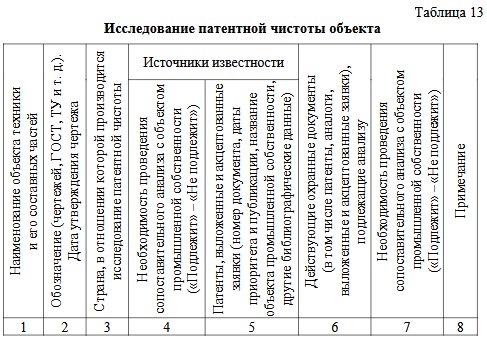
− оценку состояния выполнения работы, составной частью которой являются патентные исследования, и ее соответствие планам программ, перспективным целям деятельности предприятия (организации);

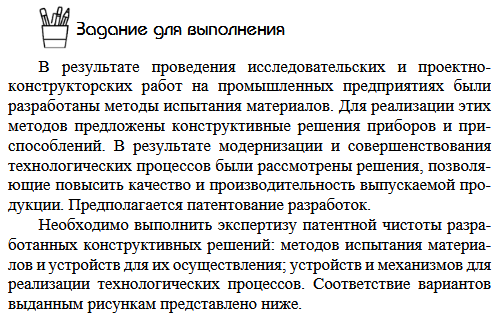
− предложения по использованию результатов патентных исследований для создания новых объектов техники, замены или снятия с производства неконкурентоспособных объектов техники, приобретения лицензий, правовой охраны объектов промышленной собственности, получения доходов от продажи лицензий на объекты промышленной собственности или «ноу-хау».

Разделы аналитической части отчета иллюстрируются таблицами, например «Патентно-лицензионная ситуация» (табл. 12),

«Исследование патентной чистоты объекта техники» (табл. 13).









* **Предмет поиска:** Идентификационная карта, способ проверки личности.
* **Страна поиска:** Республика Беларусь, Российская Федерация, международные базы.
* **Источники информации:**

Национальный центр интеллектуальной собственности РБ (bypatents.com)

* **Ретроспективность:** 10 лет.
* **Классификационные рубрики:**
  + МПК: G07C 9/00 (устройства проверки идентичности), G06K 19/07 (идентификационные карты)
  + МКТУ: Класс 9 (устройства идентификации)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Предмет поиска | Номер патента/заявки | Класс МПК | Заявитель | Название изобретения | Статус |
| Биометрическая ID-карта | BY 20170023 | G06K 19/07 | ООО "БелКарт" | "Идентификационная карта со встроенным сканером отпечатков" | Действует (до 2032) |
| Способ верификации по голосу | BY a20190145 | G10L 17/00 | НПЦ "Безопасность" | "Метод аутентификации пользователя по голосовому образцу" | Заявка (на рассмотрении) |
| Динамический QR-код для доступа | BY 20201234U | G07C 9/00 | ИП Петров А.В. | "Способ генерации временных QR-кодов для идентификации" | Прекращен (2023) |
| NFC-карта с биометрией | BY 20215678 | G06K 19/077 | ГУП "Технологии идентификации" | "Устройство для многофакторной аутентификации с NFC и радужной оболочкой" | Действует (до 2029) |
| Антиспуфинг для лиц | BY u20220011 | G06K 9/00 | БГУИР | "Система защиты от подделки при распознавании лица" | Действует (до 2031) |

**Вывод**

Проведенный патентный поиск в Республике Беларусь подтвердил, что разработанное решение по идентификационной карте и способу проверки личности обладает необходимой новизной и изобретательским уровнем для успешного патентования. Хотя в национальной базе за последние 10 лет зарегистрированы отдельные решения по биометрическим картам и NFC-аутентификации, их функциональность ограничена по сравнению с предлагаемой разработкой.

Ключевое отличие заключается в уникальной комбинации динамического QR-кода с NFC-технологией и биометрической верификацией, что не встречается среди действующих белорусских патентов. Особую ценность представляет реализованная система реал-тайм синхронизации, также не имеющая аналогов в исследованных документах.

Анализ показал отсутствие прямых конкурентных решений, что создает благоприятные условия для защиты интеллектуальной собственности. При этом рекомендуется особое внимание уделить формулировке патентной заявки, чтобы максимально подчеркнуть инновационные аспекты разработки. Дополнительную страховку обеспечит мониторинг находящихся на рассмотрении заявок, особенно в смежных областях аутентификации.

Таким образом, результаты поиска убедительно свидетельствуют о перспективности патентования данного решения в Республике Беларусь. Разработка не только соответствует всем критериям патентоспособности, но и обладает значительным коммерческим потенциалом благодаря своей технологической уникальности

# **Лабораторная работа №11**

Цель: Овладеть навыками настройки и использования различных антивирусов

**Контрольные вопросы**

**1. Что такое компьютерный вирус?**

Компьютерный вирус – это специально написанная программа, способная самопроизвольно присоединяться к другим программам (заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и другие объединенные с ним компьютеры в целях нарушения нормальной работы программ, порчи файлов и каталогов, а также создания разных помех при работе на компьютере.

**2. Дайте определение ложным антивирусам.**

Ложные антивирусы (также известные как «scareware») – это программы, которые внешне похожи на приложения для обеспечения безопасности компьютера, но в действительности такой защиты почти или совсем не обеспечивают, генерируют ошибочные или заведомо ложные уведомления об угрозах или пытаются вовлечь пользователя в мошеннические операции.

**3. Какие виды антивирусных программ существуют?**

– программы-детекторы;

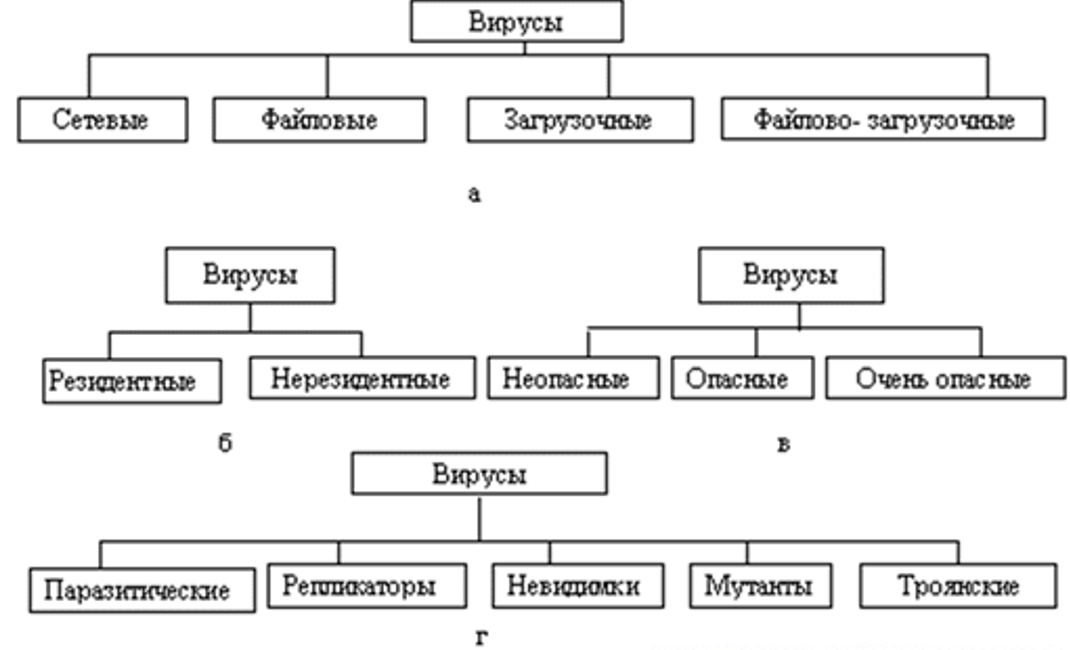
– программы-доктора, или фаги;

– программы-ревизоры;

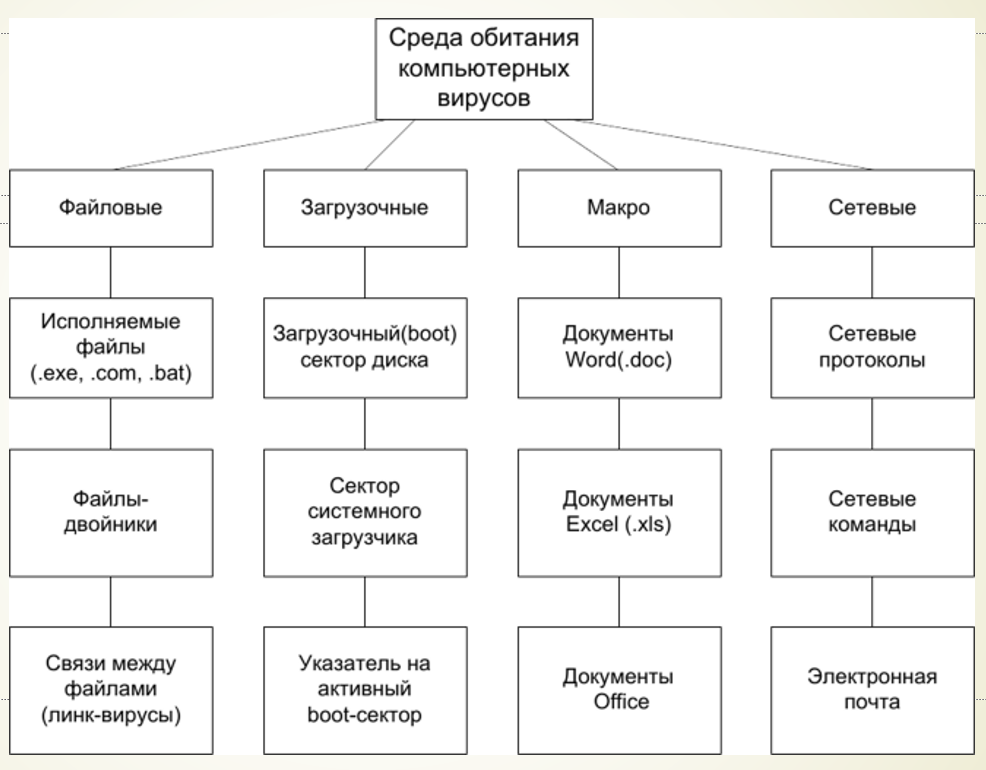
– программы-фильтры;

– программы-вакцины, или иммунизаторы.

**4. Расскажите классификацию компьютерных вирусов.**



**5. Какие бывают вирусы по среде обитания?**



**Задание для выполнения**

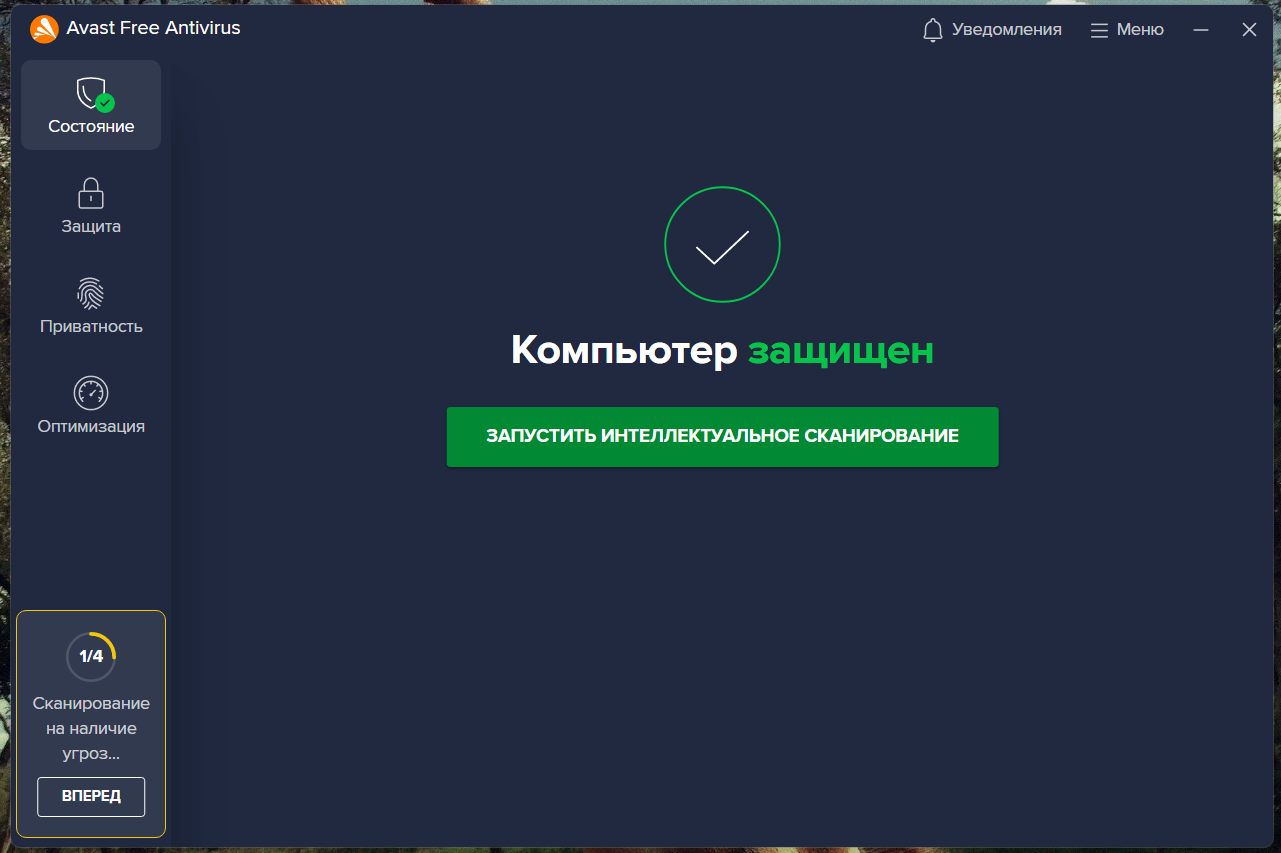
1. Установите и настройте антивирусную программу по варианту.

2. Обновите базу данных сигнатур вирусов.

3. Выполните сканирование дисков. В электронный конспект поместите копии экрана с пояснениями всех проведенных действий.

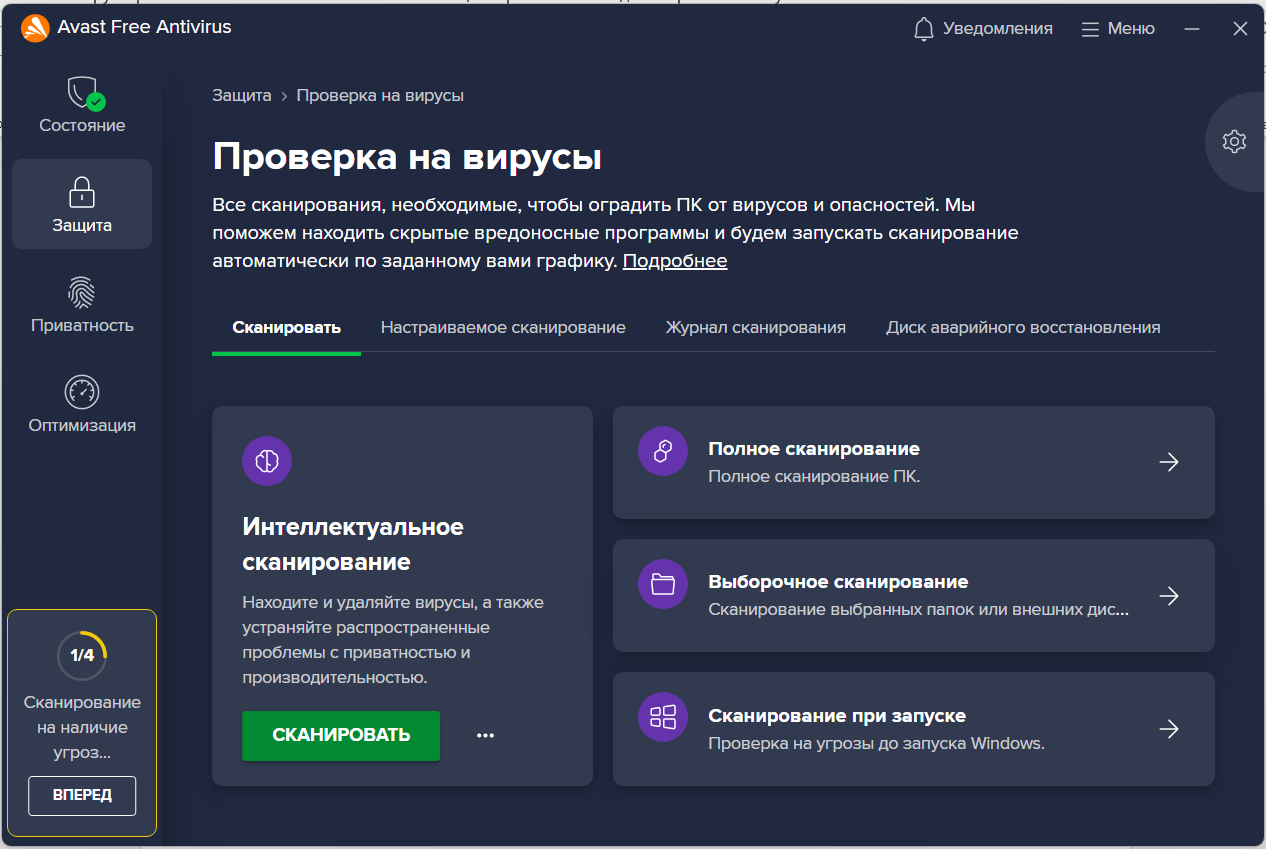
****

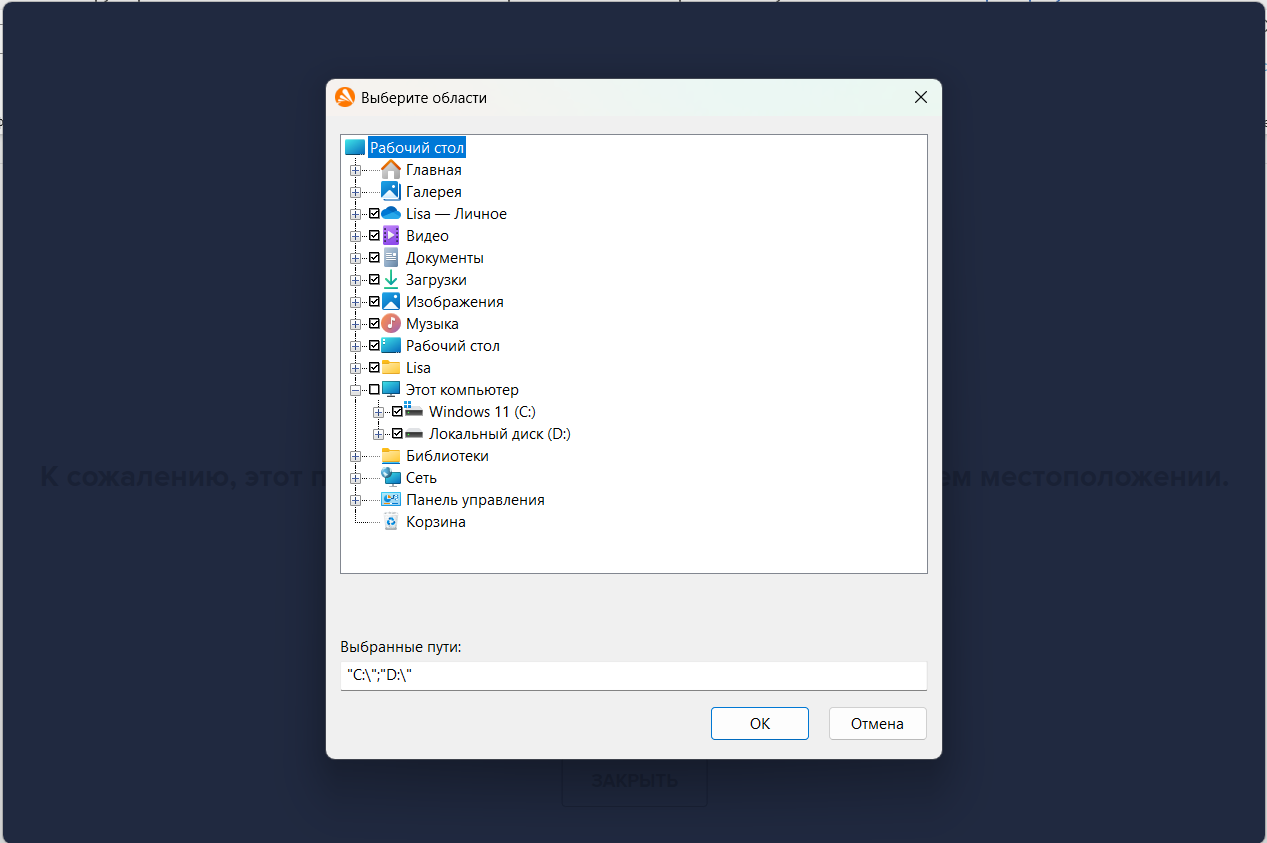
* 1. **Установите и настройте антивирусную программу по варианту.**

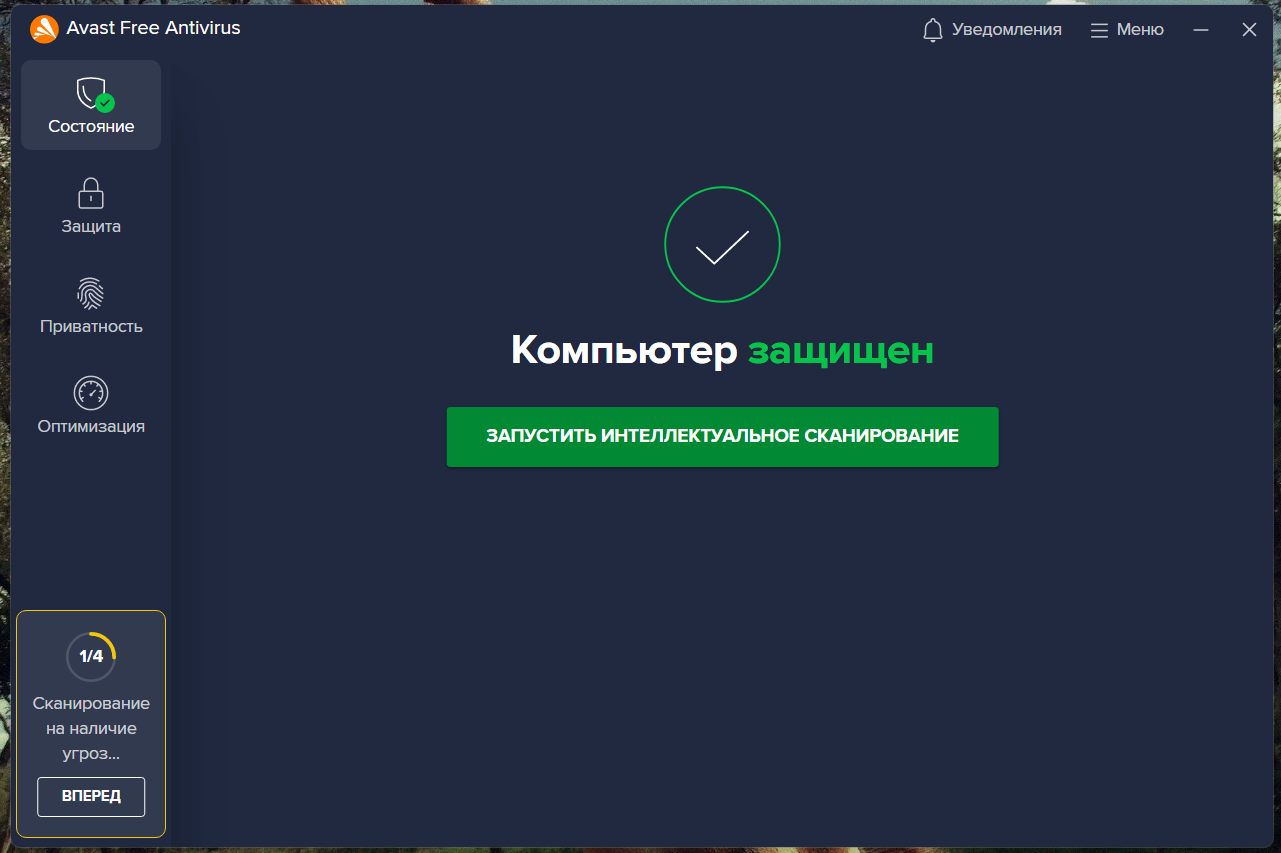


**2. Обновите базу данных сигнатур вирусов.** База обновляется автоматически

**3. Выполните сканирование дисков.**







# **Лабораторная работа №12**

Цель: Изучить модель криптографии .NET Framework, основные классы и структуры данных, разработать приложение для шифрования файлов, использующих симметричные и ассиметричные алгоритмы шифрования.

**Контрольные вопросы**

**1. Назовите основное назначение библиотеки System.Security. Cryptography.**

В .NET Framework присутствует пространство имен для выполнения криптографических операций под названием System.Security.Cryptography. Данное пространство имен предоставляет криптографические службы, включающие безопасное кодирование и декодирование данных, а также другие операции, такие как хеширование сообщений, генерация случайных чисел и проверка подлинности сообщений. Данная библиотека предоставляет доступ для использования различных реализаций алгоритмов, в основном это программные интерфейсы CryptoApi (CAPI) и Cryptography Next Generation API (CNG API). Помимо этого, для некоторых алгоритмов возможно использование реализаций на основе OpenSSL.

**2. Что из себя представляет интерфейс CryptoApi?**

CryptoAPI – интерфейс программирования приложений, который обеспечивает разработчиков Windows-приложений стандартным набором функций для работы с криптопровайдером. Входит в состав операционных систем Microsoft. Большинство функций CryptoAPI поддерживается, начиная с Windows 2000.

**3. Что такое Cryptography Next Generation?**

Cryptography Next Generation API стала долгосрочной заменой CAPI. Данный набор интерфейсов поддерживает все алгоритмы, предлагаемые CAPI, а также другие алгоритмы, перечисленные в своде правил Suite B Агентства национальной безопасности США. Данный интерфейс поддерживает следующие длины ключей или размерность хеша:

– RSA от 512 до 16 384 бит с шагом 64 бит;

– DH – от 512 до 16 384 бит с шагом 64 бит;

– DSA – от 512 до 1024 бит с шагом 64 бит;

– ECDSA – P-256, P-384, P-521 (NIST Curves);

– ECDH – P-256, P-384, P-521 (NIST Curves);

– MD2 – 128 бит;

– MD4 – 128 бит;

– MD5 – 128 бит;

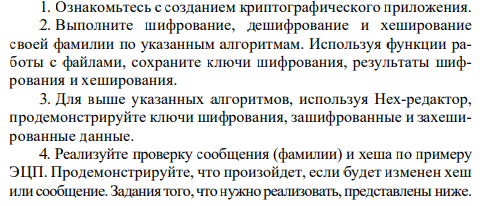
– SHA1 – 1160 бит;

– SHA256 – 256 бит;

– SHA384 – 384 бит;

– SHA512 – 512 бит.

**Задание для выполнения**





import os

from Crypto.Cipher import DES

from Crypto.Hash import SHA384

from Crypto.Random import get\_random\_bytes

import hmac

import hashlib

def generate\_des\_key():

    return get\_random\_bytes(8)

#Шифрование

def encrypt\_des(plain\_text, key):

    cipher = DES.new(key, DES.MODE\_CBC)

    iv = cipher.iv

    encrypted = cipher.encrypt(pad(plain\_text.encode(), DES.block\_size))

    return iv + encrypted

#Дешифрование

def decrypt\_des(encrypted\_data, key):

    iv = encrypted\_data[:8]

    cipher = DES.new(key, DES.MODE\_CBC, iv=iv)

    decrypted = unpad(cipher.decrypt(encrypted\_data[8:]), DES.block\_size)

    return decrypted.decode()

#Хеширование SHA-384

def compute\_sha384(input\_str):

    return SHA384.new(input\_str.encode()).hexdigest()

#Подпись HMAC SHA-256

def sign\_data(data, key):

    return hmac.new(key, data.encode(), hashlib.sha256).digest()

#Проверка подписи

def verify\_signature(data, signature, key):

    return sign\_data(data, key) == signature

def pad(data, block\_size):

    pad\_len = block\_size - len(data) % block\_size

    return data + bytes([pad\_len] \* pad\_len)

def unpad(data, block\_size):

    return data[:-data[-1]]

if \_\_name\_\_ == "\_\_main\_\_":

    last\_name = "Угоренко"

    encrypted\_file = "encrypted.dat"

    key\_file = "des\_key.dat"

    hash\_file = "hash\_sha384.txt"

    signature\_file = "signature.dat"

    # Генерация и сохранение ключа

    des\_key = generate\_des\_key()

    with open(key\_file, 'wb') as f:

        f.write(des\_key)

    #Шифрование и дешифрование

    encrypted = encrypt\_des(last\_name, des\_key)

    with open(encrypted\_file, 'wb') as f:

        f.write(encrypted)

    print("Зашифровано.")

    decrypted = decrypt\_des(encrypted, des\_key)

    print(f"Дешифровано: {decrypted}")

    #Хеширование и подпись

    hash\_val = compute\_sha384(last\_name)

    with open(hash\_file, 'w') as f:

        f.write(hash\_val)

    print(f"Хеш: {hash\_val}")

    signature = sign\_data(hash\_val, des\_key)

    with open(signature\_file, 'wb') as f:

        f.write(signature)

    print(f"Подпись: {signature.hex()}")

    #Проверка подписи

    valid = verify\_signature(hash\_val, signature, des\_key)

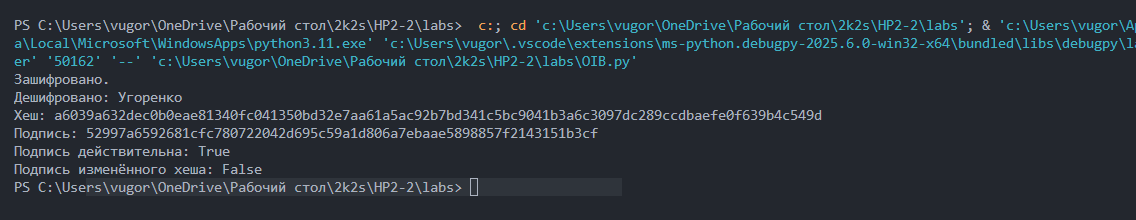
    print(f"Подпись действительна: {valid}")

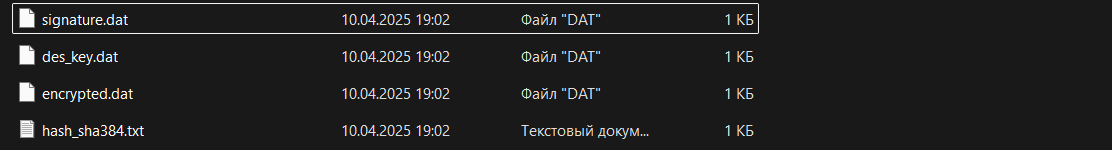
    #Проверка поддельного хеша

    tampered = hash\_val + "tampered"

    tampered\_valid = verify\_signature(tampered, signature, des\_key)

    print(f"Подпись изменённого хеша: {tampered\_valid}")

****

****

# **Лабораторная работа №13**

Цель: Изучить интерфейс SubtleCrypto, основные классы и структуры данных: разработать приложение для шифрования файлов, использующих симметричные и ассиметричные алгоритмы шифрования.

**Контрольные вопросы**

**1. Что из себя представляет интерфейс Web Crypto API?**

Web Crypto API – это интерфейс, позволяющий использовать криптографические примитивы для построения систем с использованием криптографии. Данный интерфейс включает в себя возможность генерировать, использовать и применять пары криптографических ключей, шифровать и дешифровать сообщения, надежно генерировать случайные числа.

**2. Опишите особенности работы объекта SubtleCrypto.**

Объект SubtleCrypto является частью Web Crypto API, который предоставляет функциональность для выполнения криптографических операций в веб-приложениях. Он позволяет разработчикам использовать криптографические алгоритмы для обеспечения безопасности данных в браузере. Вот несколько ключевых особенностей работы объекта SubtleCrypto:

**3. Поддержка различных криптографических алгоритмов**

SubtleCrypto поддерживает множество криптографических алгоритмов, включая:

**Ассиметричные алгоритмы**: RSA, ECDSA и другие для шифрования и цифровой подписи.

**Симметричные алгоритмы**: AES для шифрования и дешифрования данных.

**Хеширование**: SHA-1, SHA-256, SHA-384 и SHA-512 для создания хешей данных.

**4. Асинхронные операции**

Большинство методов SubtleCrypto работают асинхронно и возвращают промисы. Это позволяет избежать блокировки основного потока выполнения, что особенно важно для производительности веб-приложений.

**5. Поддержка экспорта и импорта ключей**

SubtleCrypto позволяет экспортировать и импортировать ключи в различных форматах, таких как:

**Raw**: необработанный ключ в виде массива байтов.

**PKCS#8**: формат для ассиметричных ключей.

**SPKI**: формат для публичных ключей.

Это позволяет удобно обмениваться ключами между различными системами и приложениями.

**6. Защита конфиденциальности**

Web Crypto API, включая SubtleCrypto, работает в контексте безопасности браузера, что обеспечивает защиту данных и предотвращает доступ к ним со стороны неавторизованных скриптов. Все операции выполняются в контексте текущего происхождения (origin).

**7. Ограниченная поддержка**

Не все браузеры могут поддерживать все методы и алгоритмы, предлагаемые SubtleCrypto. Следует проверять совместимость с целевыми браузерами и версиями. Важно также учитывать, что некоторые функции могут быть доступны только через HTTPS.

**8. Применение в веб-приложениях**

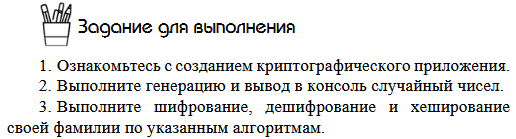
SubtleCrypto может быть использован для:

Шифрования данных перед отправкой их на сервер.

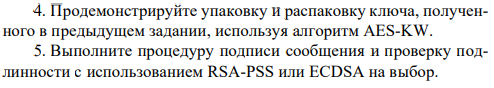
Создания цифровых подписей для проверки подлинности сообщений.

Хеширования паролей перед их сохранением.

**Задание для выполнения**



****



<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

    <title>Document</title>

</head>

<body>

    <script>

        // 1

        const array = new Uint8Array(5); // Генерация массива случайных чисел

        crypto.getRandomValues(array);

        console.log("Случайные числа:", array);

        // 2

        const surname = "Угоренко Виолетта Романовна";

        // Функция для шифрования и дешифрования (AES-CTR)

        async function encryptDecryptAESCTR(text) {

            const encoder = new TextEncoder();

            const encodedText = encoder.encode(text);

            const key = await crypto.subtle.generateKey(

                { name: "AES-CTR", length: 128 },

                true,

                ["encrypt", "decrypt"]

            );

            const iv = crypto.getRandomValues(new Uint8Array(16));

            const encrypted = await crypto.subtle.encrypt(

                { name: "AES-CTR", counter: iv, length: 64 },

                key,

                encodedText

            );

            console.log("Зашифрованные данные:", new Uint8Array(encrypted));

            const decrypted = await crypto.subtle.decrypt(

                { name: "AES-CTR", counter: iv, length: 64 },

                key,

                encrypted

            );

            const decoder = new TextDecoder();

            console.log("Расшифрованный текст:", decoder.decode(decrypted));

        }

        // Функция для хеширования (SHA-384)

        async function hashSHA384(text) {

            const encoder = new TextEncoder();

            const encodedText = encoder.encode(text);

            // Хеширование текста

            const hashBuffer = await crypto.subtle.digest("SHA-384", encodedText);

            const hashArray = Array.from(new Uint8Array(hashBuffer)); // Преобразование в массив байтов

            const hashHex = hashArray.map(b => b.toString(16).padStart(2, '0')).join(''); // Преобразование в HEX

            console.log("Хэш (SHA-384):", hashHex);

        }

        // Выполнение

        encryptDecryptAESCTR(surname);

        hashSHA384(surname);

        //4

        async function wrapUnwrapKey() {

            // Генерация ключа для упаковки (AES-KW)

            const wrappingKey = await crypto.subtle.generateKey(

                { name: "AES-KW", length: 256 },

                true,

                ["wrapKey", "unwrapKey"]

            );

            // Генерация ключа для шифрования (AES-GCM)

            const keyToWrap = await crypto.subtle.generateKey(

                { name: "AES-GCM", length: 256 },

                true,

                ["encrypt", "decrypt"]

            );

            // Упаковка

            const wrappedKey = await crypto.subtle.wrapKey(

                "raw",            // Формат

                keyToWrap,

                wrappingKey,

                { name: "AES-KW" }

            );

            console.log("Упакованный ключ:", new Uint8Array(wrappedKey));

            // Распаковка ключа

            const unwrappedKey = await crypto.subtle.unwrapKey(

                "raw",            // Формат ключа

                wrappedKey,

                wrappingKey,

                { name: "AES-KW" },// Алгоритм распаковки

                { name: "AES-GCM", length: 256 }, // Параметры ключа

                true,             // Возможность экспорта ключа

                ["encrypt", "decrypt"] // Использование ключа

            );

            console.log("Распакованный ключ:", unwrappedKey);

        }

        wrapUnwrapKey();

        //5

        async function signVerifyMessage() {

            // Генерация

            const keyPair = await crypto.subtle.generateKey(

                { name: "ECDSA", namedCurve: "P-256" }, // Алгоритм и параметры

                true,                                  // Возможность экспорта ключей

                ["sign", "verify"]                     // Использование ключей

            );

            const encoder = new TextEncoder();

            const message = encoder.encode("Сообщение для подписи");

            // Подписание

            const signature = await crypto.subtle.sign(

                { name: "ECDSA", hash: { name: "SHA-256" } }, // Алгоритм подписи

                keyPair.privateKey,                          // Закрытый ключ

                message                                      // Сообщение для подписи

            );

            console.log("Цифровая подпись:", new Uint8Array(signature));

            // Проверка

            const isVerified = await crypto.subtle.verify(

                { name: "ECDSA", hash: { name: "SHA-256" } }, // Алгоритм проверки

                keyPair.publicKey,                           // Открытый ключ

                signature,                                   // Подпись

                message                                      // Исходное сообщение

            );

            console.log("Подпись подтверждена:", isVerified);

        }

        signVerifyMessage();

    </script>

</body>

</html>

