**Харченко Евгений Игоревич. ФИТ 2-1-2**

**Лабораторная работа №1**

1. Что такое информационная безопасность?

Информационная безопасность — это состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Это включает защиту информации и информационных систем от несанкционированного доступа, разрушения, модификации или раскрытия.

1. Перечислить 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.

1. Основные угрозы национальной безопасности, связанные с ИТ-сферой?

* 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.

1. Назвать 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.

1. Основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере?

* Совершенствование механизмов реализации прав граждан на получение и использование информации.
* Разработка и реализация стратегии всеобъемлющей информатизации.
* Развитие индустрии информационных и телекоммуникационных технологий.
* Повышение качества, объема и конкурентоспособности национального контента.
* Совершенствование нормативной правовой базы обеспечения информационной безопасности.
* Завершение формирования комплексной государственной системы обеспечения информационной безопасности в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере.
* Разработка и внедрение современных методов и средств защиты информации.
* Участие в международных договорах, регулирующих мировой информационный обмен.
* Сохранение роли регулятора при внедрении иностранных информационных технологий.

**Лабораторная работа №2**

Решите задачу разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа в соответствии с вариантом. Варианты выполнения задания соответствуют номеру студента по журналу группы.

= 22000 — эффективность объекта без защиты.

E = 20000 — текущая эффективность объекта.

K = 6 — коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объекта.

C = 1000 — допустимые расходы на защиту.

Минимизировать ущерб  и максимизировать эффективность ​ и изменение эффективности при заданных допустимых расходах C.

ΔE = ​ − E = 22000 – 20000 = 2000

​ = E / ​= 20000 / 22000 ​≈ 0.909

​ = U / f(C)​  
f(C) = K = 6

​ = U / 6  
​ = ​– ΔE / K​ = 22000 – 2000 / 6 ​≈ 22000 − 333.33 ≈ 21666.67

​ = C = 1000

Итог:

* Изменение эффективности: ≈ 0.909
* Ущерб:  = U / 6
* Эффективность с учетом защиты: ≈ 21666.67
* Допустимые расходы:  = 1000

Выбранные средства защиты удовлетворяют критерию допустимых расходов.

**Лабораторная работа №3**

**Пояснительная записка к проекту политики информационной безопасности паспортного стола**

**Титульный лист**

**Название** **документа**: Политика информационной безопасности паспортного стола

**Разработчик**: Харченко Евгений Игоревич, студент 2-го курса 1-ой группы факультета ИТ.

**Дата**: 27.02.2025

**Введение**

Современное общество характеризуется высоким уровнем цифровизации, что приводит к необходимости защиты персональных данных граждан. В последние десятилетия информационные технологии прочно вошли во все сферы жизни, включая государственные службы. В связи с этим одной из важнейших задач становится обеспечение безопасности информации, особенно той, которая связана с документами, удостоверяющими личность. Паспортный стол — ключевое звено в системе государственной идентификации, обрабатывающее конфиденциальную информацию, включая паспортные данные, регистрационные сведения и биометрическую информацию.

Утечки этих данных могут привести к серьезным последствиям, включая мошенничество, кражу личных данных, незаконное оформление кредитов и другие киберугрозы. В 2017 году произошла одна из крупнейших утечек персональных данных в истории, связанная с атакой на компанию Equifax, в результате чего были скомпрометированы данные 147 миллионов человек. Это подчеркивает необходимость строгого соблюдения норм информационной безопасности.

Кибератаки стали неотъемлемой частью современного мира. В 2021 году атака на американский нефтепровод Colonial Pipeline привела к временному прекращению его работы, что вызвало рост цен на топливо и перебои с поставками. В Беларуси неоднократно фиксировались случаи атак на государственные базы данных, что подчеркивает необходимость строгого контроля и внедрения эффективных мер защиты.

Одной из главных задач любого государственного учреждения, работающего с персональными данными, является обеспечение их конфиденциальности, доступности и целостности. Это требует комплексного подхода, включающего технические, организационные и юридические меры, позволяющие минимизировать риски утечек и атак. Только системный и всесторонний подход может гарантировать защиту данных и предотвращение негативных последствий для граждан и государства.

**Описание структуры бизнес-компании**

Паспортный стол представляет собой государственное учреждение, занимающееся регистрацией и учетом граждан. Основные функциональные подразделения включают:

**- Отдел приема граждан**: Обработка заявлений на выдачу и замену паспортов, регистрация по месту жительства, оформление временной регистрации. Также в компетенцию отдела входит консультирование граждан по вопросам миграции и смены документов. Сотрудники отдела должны быть обучены основам информационной безопасности и строго соблюдать все процедуры, связанные с обработкой данных.

**- Отдел учета и хранения данных**: Ведение баз данных, архивация документов, проверка корректности внесенной информации, организация обмена данными с другими государственными органами. Этот отдел играет ключевую роль в обеспечении целостности и доступности данных. Сотрудники должны регулярно проверять данные на предмет ошибок и несоответствий.

**- Отдел IT-поддержки**: Обеспечение работы технических средств, защита информации, контроль за соблюдением норм информационной безопасности, мониторинг активности пользователей информационных систем. Этот отдел отвечает за техническую поддержку всех информационных систем и регулярное обновление программного обеспечения.

**- Юридический отдел**: Контроль за соблюдением нормативных актов и правовая поддержка сотрудников. Сюда же входит консультирование по вопросам защиты персональных данных и предотвращения юридических рисков. Юридический отдел должен быть в курсе всех изменений в законодательстве, касающихся защиты данных.

**- Отдел внутреннего контроля и аудита**: Регулярные проверки соблюдения норм информационной безопасности, выявление уязвимостей в системе и контроль за выполнением инструкций сотрудниками. Этот отдел проводит регулярные аудиты и проверки, чтобы убедиться, что все процедуры соблюдаются.

**- Отдел кибербезопасности**: Специализированное подразделение, ответственное за мониторинг, реагирование на инциденты и внедрение новых методов защиты информации. Этот отдел должен быть оснащен современными инструментами для обнаружения и предотвращения кибератак.

**- Отдел кадров и обучения**: Занимается подбором персонала, проверкой на благонадежность сотрудников и проведением обучения по информационной безопасности. Обучение должно быть регулярным и охватывать все аспекты информационной безопасности.

**- Финансовый отдел**: Обеспечивает контроль за финансированием мероприятий по защите данных, закупкой программного обеспечения и аппаратных средств. Финансовый отдел должен управлять бюджетом, выделенным на информационную безопасность.

**- Аналитический центр**: Занимается анализом киберугроз, прогнозированием атак и разработкой новых методов защиты. Аналитический центр должен быть в курсе всех современных угроз и тенденций в области кибербезопасности.

**Оценка рисков**

Для обеспечения надежной защиты данных в паспортном столе проводится анализ возможных угроз и уязвимостей. Основные риски можно разделить на несколько категорий:

**По виду:**

**Физическая и логическая целостность**: Уничтожение или искажение информации. Это может произойти из-за сбоев оборудования, ошибок персонала или злонамеренных действий.

Пример: Повреждение сервера может привести к утрате данных о паспортах.

**Конфиденциальность**: Несанкционированное получение данных. Утечка данных может привести к серьезным последствиям, таким как мошенничество или кража личных данных.

Пример: Перехват данных при передаче по незащищенному каналу связи.

**Доступность**: Нарушение работоспособности системы. Это может быть вызвано DDoS-атаками, сбоями оборудования или ошибками персонала.

Пример: DDoS-атака может сделать недоступными онлайн-сервисы паспортного стола.

**Право собственности**: Незаконное использование информационных ресурсов. Это может включать копирование и распространение данных без разрешения.

Пример: Сотрудник может скопировать данные на внешний носитель без разрешения.

**По происхождению:**

**Случайные**: Отказы, сбои, ошибки, стихийные явления. Например, пожары, наводнения или сбои в работе оборудования.

Пример: Пожар в серверной может уничтожить данные.

**Преднамеренные**: Злоумышленные действия людей. Это могут быть атаки хакеров, вредоносное ПО или действия недобросовестных сотрудников.

Пример: Вредоносное ПО может быть установлено через фишинговую атаку.

**По источникам:**

**Люди**: Персонал, посторонние. Человеческий фактор является одной из основных причин утечек данных.

Пример: Сотрудник может случайно отправить конфиденциальную информацию на неправильный адрес электронной почты.

**Технические устройства**: Сбои или неисправности оборудования могут привести к утечкам данных.

Пример: Сбой жесткого диска может привести к потере данных.

**Модели, алгоритмы, программы**: Ошибки в программном обеспечении могут быть использованы для получения несанкционированного доступа.

Пример: Уязвимость в программном обеспечении может быть использована для выполнения вредоносного кода.

**Внешняя среда**: Побочные шумы, сигналы и наводки могут повлиять на работу системы.

Пример: Электромагнитные помехи могут нарушить работу сети.

**Информационные угрозы могут быть обусловлены:**

**Естественными факторами**: Пожары, наводнения и другие стихийные бедствия.

Пример: Наводнение может повредить серверное оборудование.

**Человеческими факторами**: Ошибки персонала, недостаточная квалификация сотрудников, злоумышленные действия.

**Человеческий фактор:**

**Случайные угрозы**: Ошибки в процессе подготовки, обработки и передачи информации. Это может включать неправильное хранение паролей или передачу данных через незащищенные каналы.

Пример: Сотрудник может оставить пароль на заметке у рабочего места.

**Умышленные угрозы**: Несанкционированный доступ к ресурсам АИС. Это могут быть действия сотрудников или внешних злоумышленников.

Пример: Сотрудник может намеренно передать данные третьей стороне.

**Умышленные угрозы**:

**Пассивные угрозы**: Несанкционированное использование информационных ресурсов без влияния на их функционирование. Например, прослушивание.

Пример: Злоумышленник может подключиться к сети и перехватывать данные.

**Активные угрозы**: Нарушение нормального процесса функционирования системы. Это может включать атаки вирусов, DDoS-атаки или действия злоумышленников.

Пример: Вирус может зашифровать данные и потребовать выкуп за их расшифровку.

**Внутренние угрозы**:

**Утечки информации**: Несанкционированный доступ к данным со стороны сотрудников.

Пример: Сотрудник может скопировать данные на флеш-накопитель.

**Неавторизованный доступ**: Доступ к ресурсам без соответствующих прав.

Пример: Сотрудник может использовать чужие учетные данные для доступа к системе.

**Внешние угрозы:**

**Вредоносные программы**: Вирусы, троянцы, черви и другие вредоносные программы.

Пример: Троян может быть установлен через поддельное письмо.

**Атаки хакеров**: Взломы, DDoS-атаки, таргетированные атаки.

Пример: Хакер может использовать уязвимость в программном обеспечении для получения доступа к системе.

**Спам и фишинг**: Рассылка вредоносных писем и попытки обмана пользователей.

Пример: Фишинговое письмо может побудить сотрудника ввести свои учетные данные на поддельном сайте.

**Промышленные угрозы**: Использование сложных вредоносных программ, таких как Stuxnet, Flame, Duqu.

Пример: Stuxnet может быть использован для атаки на промышленные системы.

**Шпионское ПО**: Программы, собирающие данные без ведома пользователя.

Пример: Шпионское ПО может собирать данные о действиях пользователя.

**Ботнеты**: Сети зараженных компьютеров, используемые для распространения вредоносного ПО.

Пример: Ботнет может быть использован для проведения DDoS-атак.

**Случайные угрозы:**

**Недостаточная надежность аппаратуры и программных продуктов**: Сбои и ошибки, приводящие к утечкам данных.

Пример: Сбой сервера может привести к потере данных.

**Ошибки персонала**: Неправильные действия сотрудников, приводящие к нарушению безопасности.

Пример: Сотрудник может случайно удалить важные данные.

**Преднамеренные угрозы:**

**Действия людей**: Работники спецслужб, хакеры, недобросовестные сотрудники. Эти действия могут быть направлены на получение несанкционированного доступа к данным.

Пример: Хакер может использовать социальную инженерию для получения доступа к системе.

**Разработка мер защиты**

**1. Технические меры:**

**Шифрование данных:**

Использование современных алгоритмов шифрования для защиты данных как при хранении, так и при передаче. Это предотвращает несанкционированный доступ к информации даже в случае ее перехвата.

Пример: Внедрение AES-256 для шифрования баз данных.

Пример: Использование VPN для защищенной передачи данных.

Пример: Шифрование резервных копий данных.

**Многофакторная аутентификация:**

Внедрение системы, требующей нескольких факторов для подтверждения личности пользователя. Это может включать пароли, биометрические данные и одноразовые коды.

Пример: Использование SMS-кодов для подтверждения входа в систему.

Пример: Внедрение биометрической аутентификации для доступа к критически важным данным.

Пример: Использование аппаратных токенов для аутентификации.

**Защита сетевой инфраструктуры:**

Использование межсетевых экранов, систем обнаружения и предотвращения вторжений для защиты сети от несанкционированного доступа.

Пример: Установка системы IDS/IPS для мониторинга сетевого трафика.

Пример: Регулярное обновление правил межсетевого экрана для защиты от новых угроз.

Пример: Внедрение системы сегментации сети для ограничения доступа к критическим ресурсам.

**Регулярное обновление ПО:**

Своевременное обновление всех программ и операционных систем для защиты от известных уязвимостей.

Пример: Настройка автоматического обновления операционной системы.

Пример: Регулярное обновление антивирусных баз данных.

Пример: Проведение регулярных аудитов программного обеспечения на предмет уязвимостей.

**Резервное копирование:**

Регулярное создание резервных копий данных и их хранение в защищенных местах. Это позволяет восстановить данные в случае утраты или повреждения.

Пример: Использование облачных сервисов для хранения резервных копий.

Пример: Регулярное тестирование восстановления данных из резервных копий.

Пример: Хранение резервных копий на внешних носителях в защищенном помещении.

**Защита от DDoS-атак:**

Внедрение систем защиты от DDoS-атак для обеспечения доступности онлайн-сервисов.

Пример: Использование специализированных сервисов для защиты от DDoS-атак.

Пример: Настройка межсетевых экранов для фильтрации DDoS-трафика.

Пример: Внедрение системы балансировки нагрузки для распределения трафика.

**Защита от вредоносного ПО:**

Использование антивирусных решений и систем обнаружения вредоносного ПО.

Пример: Установка антивирусного ПО на все рабочие станции.

Пример: Регулярное сканирование системы на наличие вредоносного ПО.

Пример: Внедрение системы песочницы для тестирования подозрительных файлов.

**Защита от фишинга и социальной инженерии:**

Проведение тренингов для сотрудников по распознаванию фишинговых атак.

Пример: Организация тестов на распознавание фишинговых писем.

Пример: Внедрение системы фильтрации электронной почты для блокировки фишинговых писем.

Пример: Проведение ролевых игр, имитирующих атаки социальной инженерии.

**2. Организационные меры:**

**Обучение сотрудников:**

Проведение регулярных тренингов по основам информационной безопасности. Сотрудники должны быть осведомлены о последних угрозах и методах защиты.

Пример: Проведение ежемесячных семинаров по кибербезопасности.

Пример: Организация тренингов по распознаванию фишинговых атак.

Пример: Внедрение программы повышения осведомленности о киберугрозах.

**Регламентация процессов:**

Разработка и внедрение процедур, направленных на минимизацию рисков. Это включает управление доступом, контроль за соблюдением процедур и регулярные проверки.

Пример: Внедрение процедуры ежедневного мониторинга активности пользователей.

Пример: Разработка процедуры реагирования на инциденты информационной безопасности.

Пример: Внедрение процедуры управления изменениями в системе.

**Контроль доступа:**

Внедрение системы управления доступом, основанной на ролях и обязанностях сотрудников. Это позволяет ограничить доступ к конфиденциальной информации только для уполномоченных лиц.

Пример: Использование системы RBAC для управления доступом.

Пример: Регулярный аудит прав доступа сотрудников.

Пример: Внедрение системы контроля доступа на основе атрибутов (ABAC).

**Управление инцидентами:**

Разработка плана действий на случай инцидентов, включая процедуры уведомления, локализации и устранения последствий.

Пример: Разработка схемы оповещения сотрудников о возможных инцидентах.

Пример: Внедрение системы мониторинга инцидентов в реальном времени.

Пример: Проведение регулярных учений по реагированию на инциденты.

**3. Юридические меры:**

**Соблюдение законодательства:**

Обеспечение соответствия всех процессов и процедур требованиям законодательства в области защиты персональных данных.

Пример: Регулярный аудит соответствия GDPR.

Пример: Внедрение политики защиты данных в соответствии с национальными стандартами.

Пример: Проведение юридической экспертизы документов по защите данных.

**Заключение соглашений о неразглашении:**

Все сотрудники должны подписывать соглашения о неразглашении, обязуясь не передавать конфиденциальную информацию третьим лицам.

Пример: Включение пункта о неразглашении в трудовой договор.

Пример: Проведение инструктажа по соблюдению соглашения о неразглашении.

Пример: Внедрение системы контроля за соблюдением соглашений о неразглашении.

**Аудиты и проверки:**

Регулярное проведение внутренних и внешних аудитов для проверки соблюдения норм информационной безопасности.

Пример: Ежегодный внешний аудит системы безопасности.

Пример: Проведение внутренних проверок соблюдения процедур безопасности.

Пример: Внедрение системы самооценки соблюдения норм безопасности.

**Внутренние регламенты:**

Разработка и внедрение внутренних регламентов, определяющих порядок работы с персональными данными и меры по их защите.

Пример: Создание внутреннего документа, описывающего процедуры обработки данных.

Пример: Внедрение процедуры уведомления о нарушениях безопасности.

Пример: Разработка регламента проведения аудитов безопасности.

**4. Дополнительные меры:**

**Психологическая подготовка сотрудников к атакам социальной инженерии:**

Проведение тренингов и симуляций, направленных на повышение устойчивости сотрудников к атакам социальной инженерии.

Пример: Проведение ролевых игр, имитирующих атаки социальной инженерии.

Пример: Организация тестов на распознавание фишинговых писем.

Пример: Внедрение программы повышения осведомленности о методах социальной инженерии.

**Разработка системы быстрого реагирования на инциденты:**

Создание плана действий на случай инцидентов, включая процедуры уведомления, локализации и устранения последствий.

Пример: Разработка схемы оповещения сотрудников о возможных инцидентах.

Пример: Внедрение системы мониторинга инцидентов в реальном времени.

Пример: Проведение регулярных учений по реагированию на инциденты.

**Создание резервных каналов связи для передачи данных:**

Обеспечение наличия альтернативных каналов связи для передачи данных в случае сбоя основных систем.

Пример: Использование VPN для защищенной передачи данных.

Пример: Внедрение системы резервного копирования данных на внешние носители.

Пример: Организация резервного канала связи через спутниковую связь.

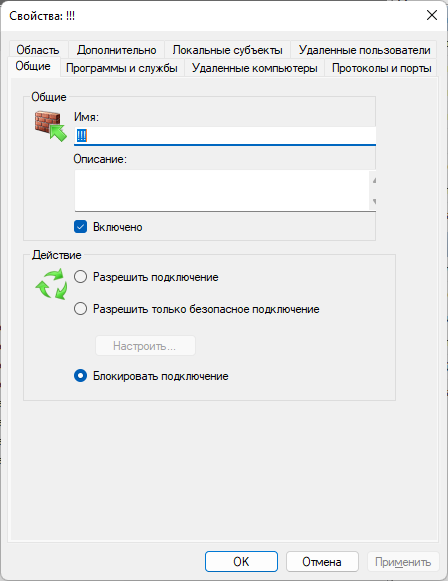
**Выводы**

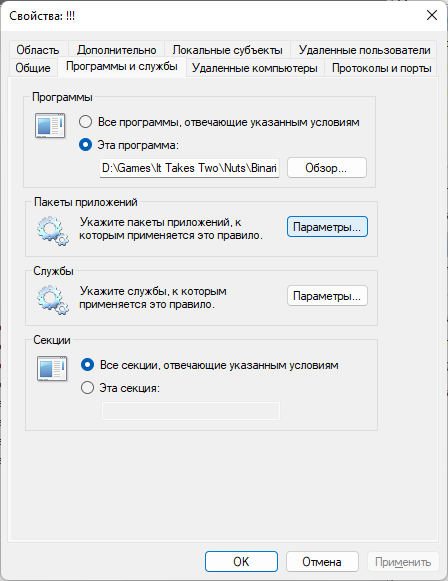
Разработка политики информационной безопасности паспортного стола позволяет минимизировать риски утечек данных и несанкционированного доступа. Введение комплекса технических, организационных, юридических и дополнительных мер гарантирует надежную защиту информации. Обучение сотрудников и регулярные аудиты позволяют своевременно выявлять угрозы и устранять их. Реализация предложенной политики повысит безопасность работы паспортного стола и обеспечит соответствие требованиям законодательства Республики Беларусь в сфере защиты персональных данных.

**Лабораторная работа №4**

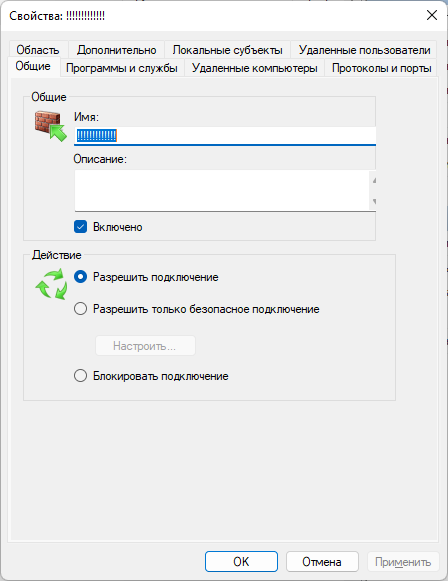
1. Создайте правила для входящих подключений (с помещением в электронный конспект копий экрана с пояснениями промежуточных действий):

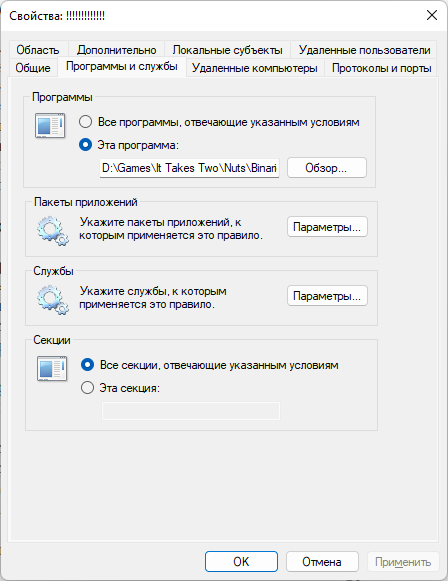
а) для одной программы (по выбору) на блокировку подключения;





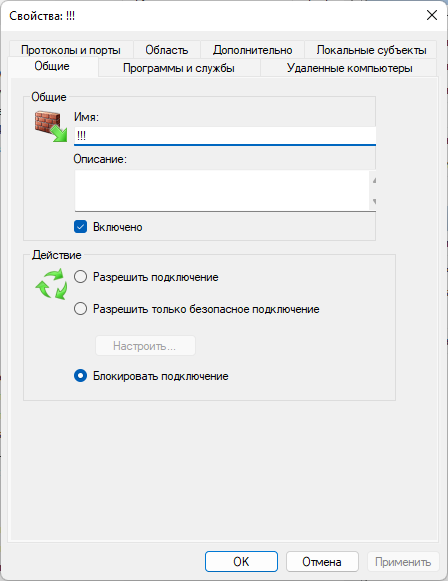
б) для одной программы (по выбору) на разрешение подключения

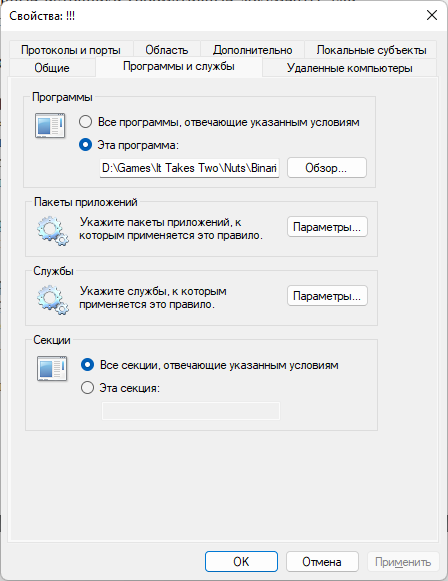
****

****

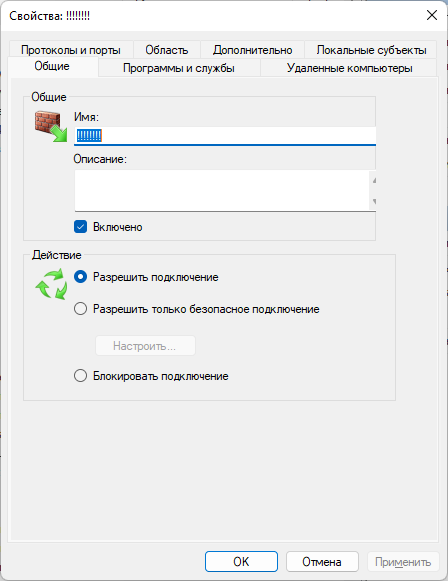
2. Создайте правила для исходящих подключений (с помещением в электронный конспект копий экрана с пояснениями действий):

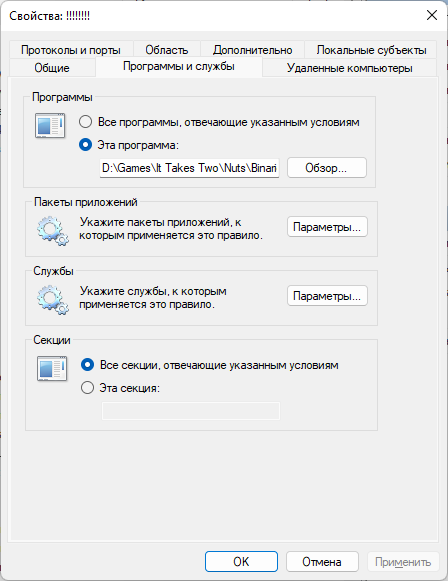
а) для одной программы (по выбору) на блокировку подключения;

****

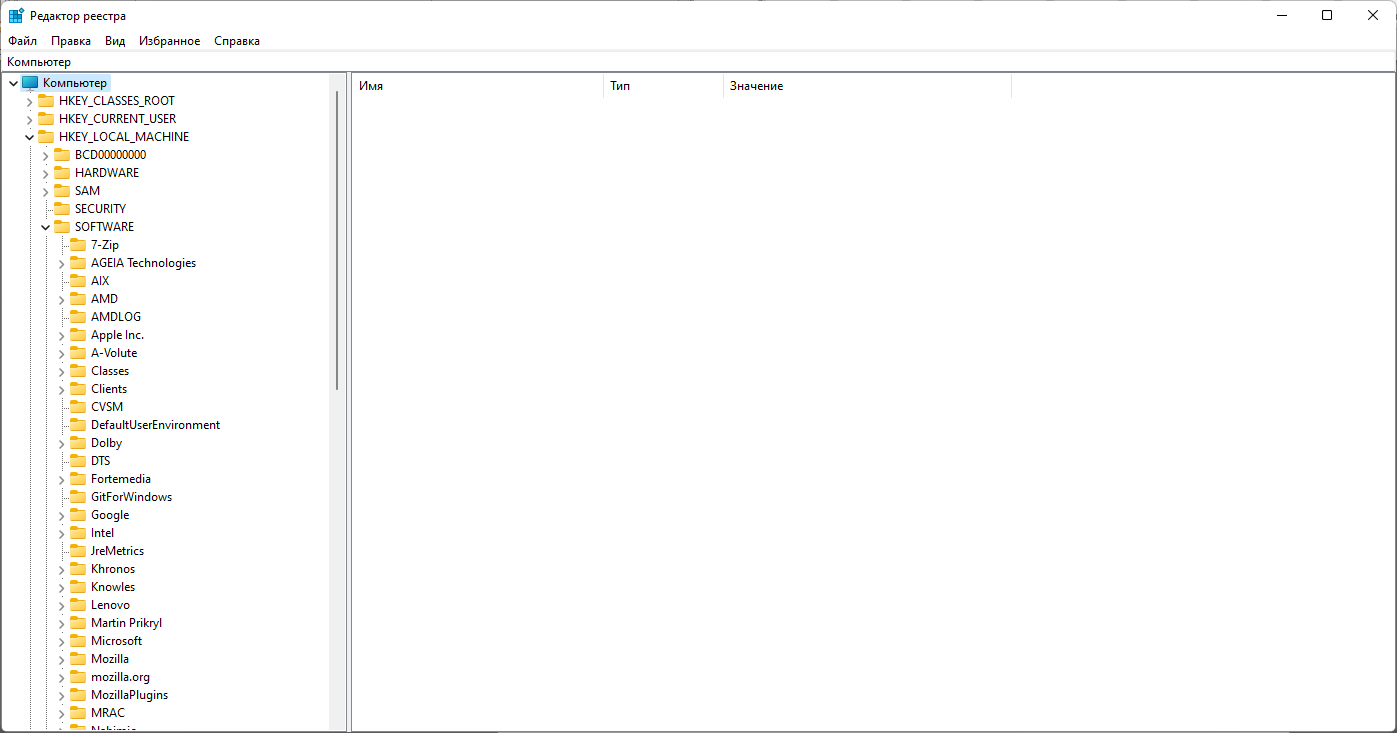
****

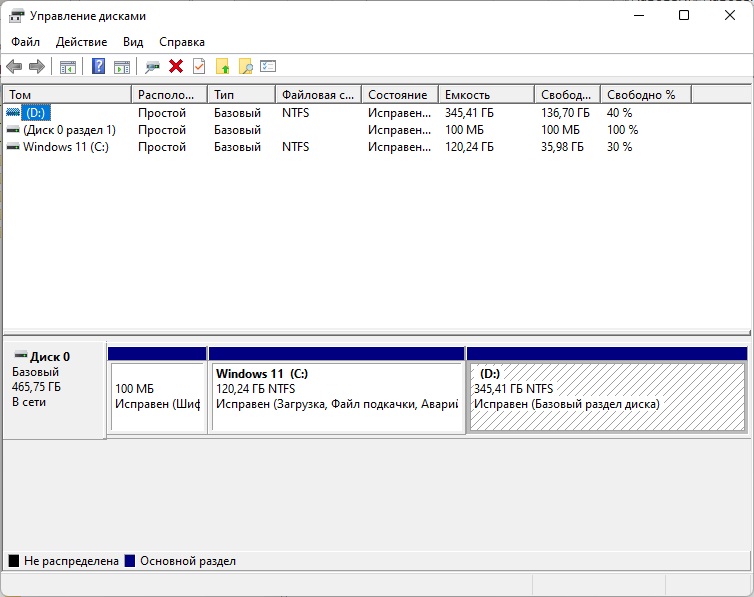
б) для одной программы (по выбору) на разрешение подключения

****

****

4. Опробуйте действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий).

****

****

**Лабораторная работа №5**

Криптография — это наука о методах обеспечения конфиденциальности и аутентичности информации. Она включает в себя как традиционные симметричные криптосистемы, где для шифрования и дешифрования используется один и тот же ключ, так и современные асимметричные системы, где для этих операций применяются разные ключи.

**Основные концепции:**

1. **Симметричные криптосистемы**:
   * Используют один ключ для шифрования и дешифрования.
   * Ключ должен быть секретным и передаваться надежным способом.
   * Примеры: потоковые и блочные шифры.
2. **Асимметричные криптосистемы**:
   * Используют пару ключей: открытый для шифрования и секретный для дешифрования.
   * Примеры: алгоритмы Диффи-Хеллмана, RSA, Эль-Гамаля.
3. **Блочные шифры**:
   * Разбивают информацию на блоки фиксированной длины и шифруют их.
   * Виды: шифры перестановки и шифры замены.
4. **Шифры замены**:
   * Заменяют элементы данных на другие по определенному правилу.
   * Примеры: моноалфавитные (код Цезаря) и полиалфавитные (шифр Виженера).

**Примеры:**

* **Код Цезаря**: каждая буква заменяется на другую, отстоящую на фиксированное количество позиций в алфавите.
* **Шифр Виженера**: использует разные символы для замены в зависимости от позиции в тексте.

**Современные системы:**

* Часто используют комбинацию замен и перестановок для повышения стойкости шифрования.
* Асимметричные системы обеспечивают более высокий уровень безопасности за счет использования разных ключей для шифрования и дешифрования.

Эти методы позволяют защитить информацию от несанкционированного доступа и обеспечить её целостность и подлинность.

2. Зашифруйте сообщение с использованием нижеперечисленных шифров и полученного секретного ключа (по номеру варианта (25) и ключевому слову «Защита»): − шифр Цезаря; − шифр Трисемуса; − шифр Плейфейра; − шифр Виженера. В качестве сообщения используйте свое полное имя (Харченко Евгений Игоревич)

**Шифр Цезаря**

Алфавит для шифра Цезаря:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч |

Результат: Ншипэёгж Эъыэнбв Быжиэъбп

**Шифр Трисемуса**

Таблица для шифрования:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| З | А | Щ | И | Т | Б | В | Г |
| Д | Е | Ж | Й | К | Л | М | Н |
| О | П | Р | С | У | Ф | Х | Ц |
| Ч | Ш | Ъ | Ы | Ь | Э | Ю | Я |

Результат шифра: Юеъзцуч Пмнпцйс Йнчъпмйз

**Шифр Плейфейра**

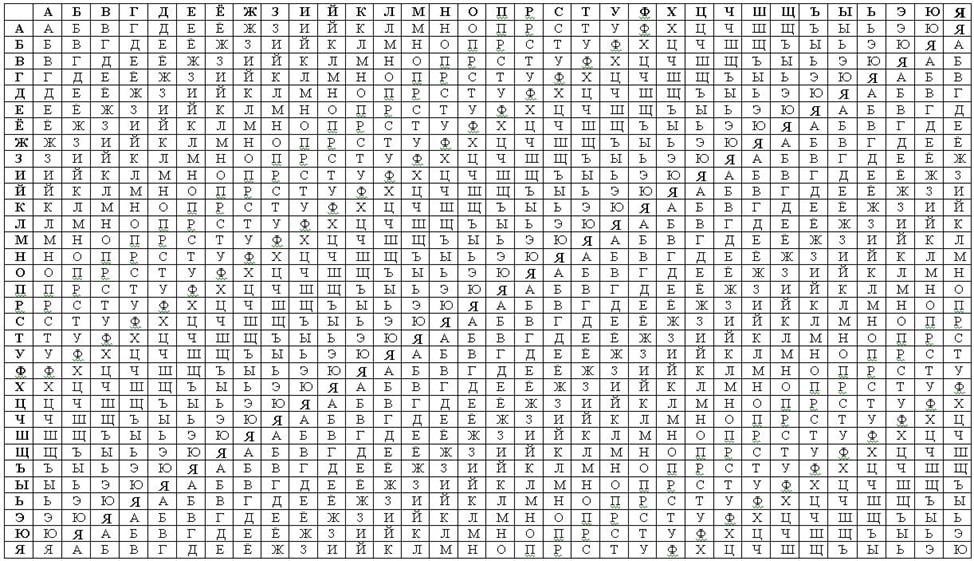
Таблица для шифра:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| З | А | Щ | И | Т | Б | В | Г |
| Д | Е | Ж | Й | К | Л | М | Н |
| О | П | Р | С | У | Ф | Х | Ц |
| Ч | Ш | Ъ | Ы | Ь | Э | Ю | Я |

Сначала разбиваем на биграммы: ХА РЧ ЕН КО ЕВ ГЕ НИ ЙЪ ИГ ОР ЕВ ИЧ

Результат шифрования: ПВ ЪО ЖД ДУ ЛЩ НА ЙС ЖЫ ТЗ ПС ЛЩ ЪТ

**Шифр Виженера**



ХАРЧЕНКО ЕВГЕНИЙ ИГОРЕВИЧ  
ЗАЩИТАЗА ЩИТАЗА ИТАЗАЩИТ

Результат: эайачнто юкхехиг схошеысй

**3. Расшифруйте сообщения по индивидуальному заданию.**



у ь т ц в ю к п ч ю ч у в у и з к щ й ю т у ф б х к ф э у е в д б е ь б ч о

в е т е р в е т е р в е т е р в е т е р в е т е р в е т е р в е т е р в е т е р в е

Результат: счастье это хорошее здоровье и плохая память

**Лабораторная работа №6**

1. Алгоритм RSA

Процесс работы:

* Генерация ключей:
  1. Выбираются два больших простых числа p и q.
  2. Вычисляется модуль n = p×q.
  3. Вычисляется функция Эйлера ϕ(n) = (p−1) × (q−1).
  4. Выбирается открытая экспонента e, взаимно простая с ϕ(n).
  5. Вычисляется секретная экспонента d, такая что d×e ≡ 1 mod  ϕ(n).
  6. Открытый ключ: (e, n). Закрытый ключ: (d, n).
* Шифрование:
  1. Сообщение m шифруется как c = m^e mod  n.
* Расшифрование:
  1. Шифротекст c расшифровывается как m = c^d mod  n.

Особенности и преимущества:

* Асимметричность: Использует пару ключей, что позволяет безопасно передавать данные по открытым каналам.
* Безопасность: Основана на сложности факторизации больших чисел.
* Широкое применение: Используется для цифровых подписей и шифрования данных.

Уникальная особенность: основывается на вычислительной сложности задачи факторизации больших целых чисел.

2. Алгоритм Диффи-Хеллмана

Процесс работы:

* Генерация ключей:
  1. Оба участника договариваются о простом числе p и примитивном элементе g.
  2. Каждый участник генерирует свой секретный ключ a и b.
  3. Вычисляются открытые значения A = g^a mod  p и B = g^b mod  p.
* Обмен ключами:
  1. Участники обмениваются открытыми значениями A и B.
* Вычисление общего секретного ключа:
  1. Участник 1 вычисляет s = B^a mod  p.
  2. Участник 2 вычисляет s = A^b mod  p*.*
  3. Оба получают одинаковый секретный ключ s.

Особенности и преимущества:

* Безопасность обмена: Даже зная открытые ключи, третья сторона не может вычислить общий секретный ключ.
* Простота: Использует простые математические операции.
* Ограничение: Не используется для непосредственного шифрования данных, только для обмена ключами.

Уникальная особенность: способность двух сторон безопасно согласовать общий секретный ключ, не передавая его напрямую.

3. Алгоритм Эль-Гамаля

Процесс работы:

* Генерация ключей:
  1. Выбирается простое число p и примитивный элемент g.
  2. Выбирается секретный ключ x.
  3. Вычисляется открытый ключ y = g^x mod  p*.*
* Шифрование:
  1. Выбирается случайное число k.
  2. Вычисляются a = g^k mod  pи b = y^k × M mod  p*.*
  3. Шифротекст: (a, b).
* Расшифрование:
  1. Используя закрытый ключ x, сообщение M вычисляется как M = b × (a \* x) − 1 mod  p*.*

Особенности и преимущества:

* Случайность: Использование случайного числа k при каждом шифровании делает каждое зашифрованное сообщение уникальным.
* Безопасность: Основана на сложности вычисления дискретных логарифмов.
* Гибкость: Может использоваться как для шифрования, так и для цифровой подписи.

Уникальная особенность: использование случайного числа k при каждом шифровании делает каждое зашифрованное сообщение уникальным.

**Лабораторная работа №7**

**1. Последовательность выполнения процедур генерации и проверки ЭЦП:**

**Генерация ЭЦП:**

1. **Вычисление хеш-образа**: Отправитель применяет хеш-функцию к исходному сообщению, чтобы получить его хеш-образ.
   * Формула: h = h(T), где T — исходное сообщение, h(T) — хеш-функция.
2. **Подписание хеш-образа**: Отправитель шифрует хеш-образ своим закрытым ключом, создавая цифровую подпись.
   * Формула: s = h^d mod n, где d — закрытый ключ отправителя, n — часть открытого ключа отправителя.
3. **Отправка**: Отправитель отправляет получателю исходное сообщение вместе с цифровой подписью.

**Проверка ЭЦП:**

1. **Вычисление хеш-образа**: Получатель применяет ту же хеш-функцию к полученному сообщению, чтобы получить его хеш-образ.
   * Формула: h' = h(T'), где T' — полученное сообщение.
2. **Расшифрование подписи**: Получатель расшифровывает цифровую подпись с использованием открытого ключа отправителя, чтобы получить исходный хеш-образ.
   * Формула: h'' = s^e mod n, где e и n — открытый ключ отправителя.
3. **Сравнение хеш-образов**: Получатель сравнивает два хеш-образа (вычисленный и расшифрованный). Если они совпадают, подпись считается действительной.

**2. Последовательность действий участников протокола при отправке и проверке ЭЦП:**

**Отправитель (Алиса):**

1. Генерирует пару ключей (открытый и закрытый).
2. Вычисляет хеш-образ сообщения.
   * Формула: h = h(T).
3. Шифрует хеш-образ своим закрытым ключом, создавая цифровую подпись.
   * Формула: s = h^d mod n.
4. Отправляет получателю (Бобу) сообщение и цифровую подпись.

**Получатель (Боб):**

1. Получает сообщение и цифровую подпись.
2. Вычисляет хеш-образ полученного сообщения.
   * Формула: h' = h(T').
3. Расшифровывает цифровую подпись с использованием открытого ключа Алисы.
   * Формула: h'' = s^e mod n.
4. Сравнивает два хеш-образа. Если они совпадают, подпись считается действительной.

**3. Схема протокола ЭЦП на основе алгоритма RSA:**

Без шифрования:

Подписываю своим закрытым

Вы проверяете моим открытым

С шифрованием:

Я шифрую вашим открытым, подписываю своим закрытым

Вы расшифровываете своим закрытым, проверяете моим открытым

**Лабораторная работа №8**

**1. Каноническое разложение чисел на простые множители**

Для разложения числа на простые множители мы ищем такие простые числа, произведение которых даёт исходное число.

Разложим a = 16088437 и b = 18216949:

* 16088437 = 241^2 \* 277. Это означает, что число 16088437 делится на 241 дважды, а затем остаётся простой множитель 277.
* 18216949 = 241 \* 269 \* 281. Здесь число 18216949 делится на 241, а оставшаяся часть разлагается на простые числа 269 и 281.

**2. НОД (a, b)**

а) По алгоритму Евклида  
Алгоритм Евклида заключается в том, что мы повторяем деление с нахождением остатка, пока не получим остаток 0.

18216949 mod 16088437 = 2128512  
16088437 mod 2128512 = 1314373  
2128512 mod 1314373 = 814139  
1314373 mod 814139 = 500234  
814139 mod 500234 = 313905  
500234 mod 313905 = 186329  
313905 mod 186329 = 127576  
186329 mod 127576 = 58753  
127576 mod 58753 = 10107  
58753 mod 10107 = 8238  
10107 mod 8238 = 1869  
8238 mod 1869 = 762  
1869 mod 762 = 345  
762 mod 345 = 72  
345 mod 72 = 57  
72 mod 57 = 15  
57 mod 15 = 12  
15 mod 12 = 3  
12 mod 3 = 0

Так как последний ненулевой остаток — 3, то (16088437, 18216949) = 241.

б) По разложению на множители  
Мы видим, что единственным общим простым множителем в разложениях a и b является 241, поэтому (16088437, 18216949) = 241.

**3. Расширенный алгоритм Евклида**

Расширенный алгоритм Евклида позволяет найти коэффициенты u и v, которые удовлетворяют уравнению Безу:

a \* u + b \* v = (a, b)

Путём вычислений мы нашли, что:

16088437 \* 31829 + 18216949 \* (-28103) = 241

Отсюда коэффициенты:  
u = 31829, v = -28103.

**4. Остаток от деления 1995^2004 mod 16**

Так как 1995 представимо как 1995 = 16 \* 124 + 11, то:

1995 ≡ 11 mod 16

Следовательно, можно упростить вычисление:

1995^2004 ≡ 11^2004 mod 16

Используем малую теорему Ферма, которая гласит, что если p — простое число, то для любого a, взаимно простого с p, верно:

a^(p-1) ≡ 1 mod p

Но нам нужно модуль 16. Сначала заметим:

11^2 = 121 ≡ 9 mod 16  
11^4 = (11^2)^2 = 9^2 = 81 ≡ 1 mod 16

Так как 2004 делится на 4, то:

11^2004 = (11^4)^501 ≡ 1^501 ≡ 1 mod 16

Окончательный ответ:

1995^2004 mod 16 = 1

**Лабораторная работа №9**

**Контрольные вопросы**

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

Авторское право распространяется на следующие объекты:

1. Произведения искусства;
2. Литературные произведения;
3. Музыкальные произведения;
4. Творения кинематографии;
5. Научные произведения.

Эти объекты отражены в законодательстве Республики Беларусь.

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

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

− импорт экземпляров произведения;

− публичный показ оригинала или экземпляра произведения;

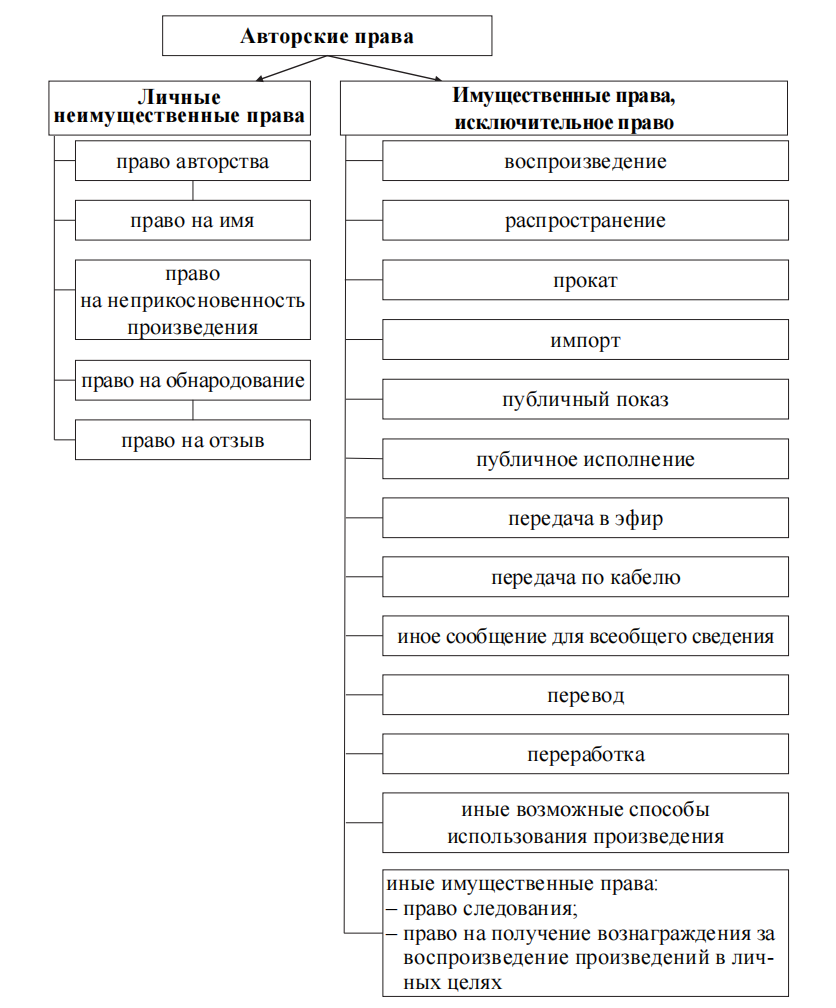
− публичное исполнение произведения;

− передачу произведения в эфир;

− иное сообщение произведения для всеобщего сведения;

− перевод произведения на другой язык;

− переделку или иную переработку произведения.



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

Особенности авторского права на составные произведения включают следующие положения:

1. Право составителя: автору составного произведения (например, сборника) принадлежит авторское право на подбор и расположение материалов как результат его творческого труда.

2. Соблюдение прав авторов: составитель обязан соблюдать права авторов произведений, включённых в составное произведение.

3. Использование включённых произведений: авторы произведений, включённых в составное произведение, могут использовать свои произведения независимо от составного произведения, если иное не оговорено в авторском договоре.

4. Свобода для других составителей: авторское право составителя не ограничивает других лиц в самостоятельном подборе и расположении аналогичных материалов для создания своих составных произведений.

5. Исключительные права на издания: лицу, выпускающему энциклопедии, словари, научные сборники, газеты, журналы и другие периодические издания, принадлежат исключительные права на использование этих изданий в целом. Оно также может требовать указания своего наименования при использовании таких изданий.

6. Сохранение прав авторов: авторы произведений, включённых в такие издания, сохраняют исключительные права на использование своих произведений независимо от издания, если иное не предусмотрено договором.

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

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.

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

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.

**Лабораторная работа №10**



**Цель:** Определить, соответствует ли разработанное устройство для счёта банкнот критериям патентной чистоты на территориях Республики Беларусь (РБ), Российской Федерации (РФ) и стран СНГ.

**Источники информации:**

* **РБ:** Национальный центр интеллектуальной собственности (НЦИС) – [https://ncis.by](https://ncis.by/)
* **РФ:** Федеральный институт промышленной собственности (ФИПС) – [https://new.fips.ru](https://new.fips.ru/)
* **СНГ:** Евразийская патентная организация (ЕАПО) – [https://www.eapo.org](https://www.eapo.org/)

**Классификационные индексы (МПК):**

* **G07D 11/00** – Устройства для обработки банкнот (счёт, сортировка, упаковка)
* **G07D 7/00** – Проверка подлинности банкнот

**Ключевые слова для поиска:**

* «Устройство для счёта банкнот»
* «Банкнотный счётчик»
* «Аппарат для пересчёта денежных средств»

**Глубина поиска:** 20 лет (2004–2024 гг.)

**2. Анализ патентной документации**

| **Предмет поиска** | **Страна, номер патента, МПК** | **Заявитель / Патентообладатель** | **Название изобретения** | **Статус** |
| --- | --- | --- | --- | --- |
| **Механизм счёта банкнот с датчиком перемещения** | РФ, патент RU 2685123, G07D 11/10 | ООО «ТехноБанк», Россия | Устройство для автоматического счёта банкнот с оптическим датчиком | Действует до 2038 г. |
| **Система сортировки банкнот по номиналу** | РБ, патент BY 15678, G07D 11/20 | НПО «БелКард», Беларусь | Устройство для сортировки и упаковки банкнот | Действует до 2035 г. |
| **Модуль детекции подлинности банкнот** | ЕАПО, патент EA 028945, G07D 7/12 | АО «КазПрибор», Казахстан | Способ и устройство для проверки подлинности банкнот | Действует до 2032 г. |
| **Устройство с функцией антизаклинивания** | РФ, патент RU 2758901, G07D 11/16 | ООО «ФинансТех», Россия | Устройство для счёта банкнот с функцией антизаклинивания | Действует до 2040 г. |
| **Счётчик с Wi-Fi-модулем** | РБ, патент BY 18902, G07D 11/34 | ОАО «БелТехника», Беларусь | Многофункциональный банкнотный счётчик с Wi-Fi-модулем | Действует до 2039 г. |
| **Система оценки ветхости банкнот** | ЕАПО, патент EA 041203, G07D 7/20 | ТОО «ТехноКазахстан», Казахстан | Способ проверки ветхости банкнот с ИИ-анализом | Действует до 2037 г. |
| **Счётчик-упаковщик банкнот** | РФ, патент RU 2789456, G07D 11/50 | ЗАО «РосИнновации», Россия | Автоматический счётчик-упаковщик для банкнот | Действует до 2042 г. |

**Лабораторная работа №11**

