Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет по дисциплине

«Основы Защиты Информации»

Студент: Парибок И.А.

ФИТ 2 курс 1 группа

Преподаватель: Барковский Е.В.

Минск 2022

# Практическое занятие №1

**Тема «Концепция национальной безопасности Республики Беларусь»**

**Цель:** Изучить концепцию национальной безопасности РБ.

**Задание для выполнения.**

Ответить на следующие вопросы:

**1.Что такое информационная безопасность?**

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

**2.Перечислить основные национальные интересы в информационной сфере?**

Основными национальными интересами в информационной сфере являются:

* 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.

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

В информационной сфере внешними источниками угроз национальной безопасности являются:

* открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;
* доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;
* информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;
* нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;
* развитие технологий манипулирования информацией;
* препятствование распространению национального контента Республики Беларусь за рубежом;
* широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;
* попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

**4.Назвать основные внутренние и внешние источники угроз национальной безопасности в информационной сфере?**

В информационной сфере внутренними источниками угроз национальной безопасности являются:

* распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;
* зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;
* несоответствие качества национального контента мировому уровню;
* недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;
* рост преступности с использованием информационно-коммуникационных технологий;
* недостаточная эффективность информационного обеспечения государственной политики;
* несовершенство системы обеспечения безопасности критически важных объектов информатизации.

**В информационной сфере внешними источниками угроз национальной безопасности являются:**

* открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;
* доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;
* информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;
* нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;
* развитие технологий манипулирования информацией;
* препятствование распространению национального контента Республики Беларусь за рубежом;
* широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;
* попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

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

Нейтрализации ряда внутренних источников угроз национальной безопасности способствует информационное обеспечение государственной политики, которое заключается в доведении до граждан Республики Беларусь и внешней аудитории объективной информации о государственном курсе во всех сферах жизнедеятельности общества, официальной позиции по общественно значимым событиям внутри страны и за рубежом, о деятельности государственных органов. Важной задачей при этом является расширение каналов и повышение качества информирования зарубежной общественности. Составной частью информационного обеспечения государственной политики выступает информационное противоборство, представляющее собой комплексное использование информационных, технических и иных методов, способов и средств для воздействия на информационную сферу с целью достижения политических, экономических и иных задач либо защиты собственного информационного пространства.

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

**Вопросы для самоконтроля**

**2.Охарактеризуйте основные положения Оранжевой книги.**

В Оранжевой книге предложены три категории требований безопасности - политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних - на качество самих средств защиты.

**Политика безопасности**

Система должна поддерживать точно определённую политику безопасности. Возможность осуществления субъектами доступа к объектам должна определяться на основе их идентификации и набора правил управления доступом. Там, где необходимо, должна использоваться политика нормативного управления доступом, позволяющая эффективно реализовать разграничение доступа к категорированной информации (информации, отмеченной грифом секретности: «секретно», «сов. Секретно» и т.д.).

**Метки**

С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа. Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и/или режимы доступа к этому объекту.

**Аудит**

Идентификация и аутентификация

Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, под­тверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

Регистрация и учет

Для определения степени ответственности пользователей за действия в системе все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективность его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

**Корректность**

Контроль корректности функционирования средств защиты

Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учёт, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

**Непрерывность защиты**

Все средства защиты (вт. ч. и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, eгo выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

**4.Каковы основные положения Европейских критериев безопасности информационных технологий?**

Европейские критерии рассматривают следующие задачи средств информационной безопасности:

• защита информации от несанкционированного доступа с целью обеспечение конфиденциальности;

• обеспечение целостности информации посредством защиты от ее несанкционированной модификации или УНИЧТОЖЕНИЯ;

• обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

**5.Чем отличаются «информационная система» и «Продукт информационных технологий»?**

Система - это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.

Продукт - это аппаратно-программный «Пакет», который можно купить и по своему усмотрению встроить в ту или иную систему.

Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

**7.Что такое Профиль защиты?**

**Профиль защиты** - это нормативный документ, который регламентирует все аспекты безопасности ИТ-продукта в виде требований к его проектированию, техно­ логии разработки и квалификационному анализу.

**Профиль защиты** - специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности и их обоснования. Служит руководством для разработчика ИТ-продукта при создании Проекта защиты.

**9.Опишите структуру Общих критериев безопасности информационных технологий.**

Единые критерии регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов, используя схему из Федеральных критериев. Единые критерии предлагают достаточно сложный процесс разработки и квалификационного анализа ИТ-продуктов, требующий от потребителей и производителей составления и оформления весьма объемных и подробных нормативных документов.

Задачи защиты - базовое понятие Единых критериев, выражающее потребность потребителей ИТ-продукта в противостоянии заданному множеству угроз безопасности или в необходимости реализации политики безопасности.

Профиль защиты - специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности и их обоснования. Служит руководством для разработчика ИТ-продукта при создании Проекта защиты.

Проект защиты - специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования.

**10.Опишите технологию применения Общих критериев безопасности информационных технологий.**

Каталог функциональных классов:

• аудит,

• связь (подтверждение приёма/передачи информации),

• криптографическая поддержка,

• защита данных пользователя (конфиденциальность, целостность, доступность),

• идентификация и аутентификация,

• управление безопасностью,

• приватность (конфиденциальность работы в системе),

• надежность средств защиты,

• контроль за использованием ресурсов,

• контроль доступа к объекту оценки,

• доверенный маршрут/канал (прямое взаимодействие).

Требования уверенности в безопасности (адекватности)

• управление проектом,

• дистрибуция,

• разработка,

• документация,

• процесс разработки,

• тестирование,

• анализ защиты.

«Единые критерии» содержат совокупность предопределённых оценочных уровней уверенности в безопасности, составленных из компонентов семейств требований уверенности в безопасности. Эти уровни предназначены:

• для достижения совместимости с исходными критериями;

• для обеспечения потребителя пакетами компонентов общего назначения.

**11.Каковы тенденции развития международной нормативной базы в области информационной безопасности?**

Основное назначение международных стандартов - это создание на межгосударственном уровне единой основы для разработки новых и совершенствования действующих систем качества. Сотрудничество в области стандартизации направлено на приведение в соответствие национальной системы стандартизации с международной. Международные стандарты не имеют статуса обязательных для всех стран-участниц. Любая страна мира вправе применять или не применять их. Решение вопроса о применении международного стандарта связано в основном со степенью участия страны в международном разделении труда.

# Практическое занятие №2

**Тема «Решение задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа»**

**Задание на выполнение:**

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E*0 | *E* | *K* | *C* |
| 17 | 20000 | 19000 | 5 | 500 |

Исходные данные: E0 =20000(руб.) E =19000(руб.) K=5 C=500(руб.).

Рассчитаем ∆E: ∆𝐸=𝐸0−𝐸=20000-19000=1000(руб.)

Находим значение относительной эффективности функционирования по формуле:



Относительная эффективность = 1-(1000/20000)=0,95

Вычислим коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объекта по формуле:



Получим коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объекта равный 1000/5=200 (руб.)

Находим эффективность функционирования по формуле:



Получим 20000-200 = 19800 (руб.)

Найдём относительную эффективность функционирования по формуле:



Получим 1 - ( 1000 / 5 / 20000 ) = 0,99

В том случае, если эффективность функционирования имеет стоимостное значение, то вычисляем по формуле:



Получим 20000 – ( 1000 / 5 ) - 300 = 19500

В итоге получим прибыль 19500– 19000 = 500 (руб.)

**Вывод:** В итоге, при затратах в 19000 руб, получим прибыль в размере 500 рублей.

# Практическое занятие №3

**Тема «Разработка политики информационной безопасности военного комиссариата»**

Цель: Разработать проект политики информационной безопасности военного комиссариата

## Введение

Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Прежде всего политика необходима для того, чтобы донести до бизнеса цели и задачи информационной безопасности компании. Бизнес должен понимать, что агент безопасности – это не только инструмент для расследования фактов утечек данных, но и помощник в минимизации рисков компании, а следовательно – в повышении прибыльности компании.

Любая защитная мера есть компромисс между снижением рисков и удобством работы пользователя. Когда специалист по безопасности говорит, что процесс не должен происходить каким-либо образом по причине появления некоторых рисков, ему всегда задают резонный вопрос: «А как он должен происходить?» Специалисту по безопасности необходимо предложить модель процесса, в которой эти риски снижены в какой-то мере, удовлетворительной для бизнеса.

При этом любое применение любых защитных мер, касающихся взаимодействия пользователя с информационной системой компании всегда вызывает отрицательную реакцию пользователя.

Основой мер **административного уровня,** то есть мер, предпринимаемых руководством организации, является политика безопасности.

Под **политикой безопасности** понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Определение политики ИБ должно сводиться к следующим практическим шагам:

1. Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:

управление доступом к средствам вычислительной техники, программа и данным;

антивирусную защиту;

вопросы резервного копирования;

проведение ремонтных и восстановительных работ;

информирование об инцидентах об области ИБ.

2. Определение подходов к управлению рисками: является ли достаточным базовый уровень защищенности или требуется проводить полный вариант анализа рисков.

3. Структуризация контрмер по уровням.

4. Порядок сертификации на соответствие стандартам в области ИБ. Должна быть определена периодичность проведения совещаний по тематике ИБ на уровне руководства, включая периодический пересмотр положений политики ИБ, а также порядок обучения всех категорий пользователей информационной системы по вопросам ИБ.

Для построения системы защиты информации необходимо определить границы системы, для которой должен быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности (система защиты информации) должна строиться именно в этих границах.

## Описание структуры компании

Эффективность управления деятельностью зависит оттого, насколько грамотно сформирована организационная структура управления и насколько она соответствует цели деятельности организации.

В настоящее время под организационной структурой понимается упорядоченная совокупность устойчиво взаимосвязанных элементов, обеспечивающих функционирование и развитие организации как единого целого. Структура управления определяется также как форма разделения и кооперации управленческой деятельности. Можно сказать, что структура управления есть не что иное, как оптимальное распределение работы, прав и ответственности, порядка и форм взаимодействия между членами коллектива организации.

Составляющими организационных структур являются:

* элементы организационных структур управления – службы или органы аппарата управления, а также отдельные работники этих служб (органов);
* организационные отношения – отношения (связи) между подразделениями организации, уровнями ее управления, персоналом, посредством которых реализуются функции управления;
* уровни управления – совокупность прав, обязанностей и ответственности, характерная для должностных лиц, занимающих определенную ступень в иерархической структуре организации.

На данном рисунке (1.1) представлена организационная структура отдела военного комиссариата:

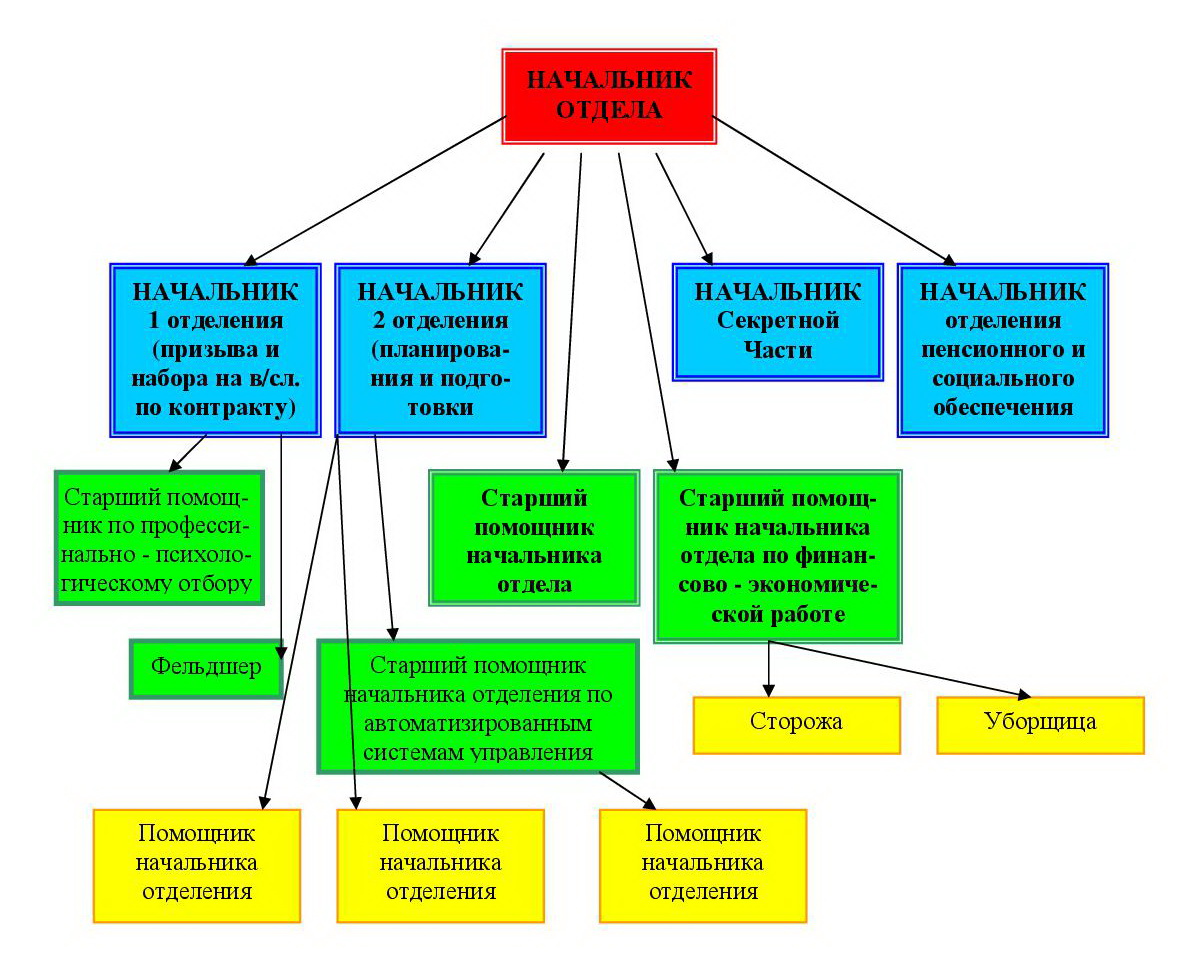


Рис 1.1 – Организационная структура отдела военного комиссариата

## Оценка рисков

Идентифицировать и оценить активы, разработать модель нарушителя и модель угроз, идентифицировать уязвимости – все это стандартные шаги, описание которых должно присутствовать в любой методике анализа рисков. Все перечисленные шаги могут выполняться с различным уровнем качества и детализации. Очень важно понять, что и как можно сделать с огромным количеством накопленной информации и формализованными моделями. На мой взгляд, этот вопрос наиболее важен, и ответ должна давать используемая методика анализа рисков.

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения:

* антропогенные,
* техногенные
* естественные (природные)

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала, так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок, и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.    
 Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре завода по производству шин могут быть как внешними, так и внутренними.

Источниками внутренних угроз являются:

* сотрудники организации;
* программное обеспечение;
* аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

* ошибки пользователей и системных администраторов;
* нарушения сотрудниками военного комиссариата установленных регламентов сбора, обработки, передачи и уничтожения информации;
* ошибки в работе программного обеспечения;
* отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

* компьютерные вирусы и вредоносные программы;
* организации и отдельные лица;
* стихийные бедствия.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации:

* информационные;
* программные;
* физические;

К информационным угрозам относятся:

* несанкционированный доступ к информационным ресурсам;
* незаконное копирование данных в информационных системах;
* хищение информации из архива, отделов и баз данных;
* нарушение технологии обработки информации;
* противозаконный сбор и использование информации;
* использование информационного оружия.

К программным угрозам относятся:

* использование ошибок и «дыр» в ПО;
* компьютерные вирусы и вредоносные программы;

К физическим угрозам относятся:

* уничтожение или разрушение средств обработки информации и связи;
* хищение носителей информации;
* хищение программных или аппаратных ключей и средств криптографической защиты данных;
* воздействие на персонал (шантаж, нападение).

Специфические угрозы безопасности

* Возможность отключения электричества, что приведет к сбою незавершенных операций и потере данных.
* Угроза возникновения неправильной адресации пакетов.
* Угроза проникновения на рабочие места сотрудников людей, не являющихся работниками отделов, которые имеют туда доступ, и попадания на завод по производству шин предметов, способных нанести ущерб.
* Угроза доступа в эксплуатационный отдел, могут быть нарушены эксплуатационные планы.
* Угроза изменения базы данных людей, получающих пенсию, в следствии чего не только заводу по производству шин, но и обществу будет нанесен урон.
* Угроза доступа в ИТ-отделе.

Полученные результаты необходимо оценить, агрегировать, классифицировать и отобразить. Так как ущерб определяется на этапе идентификации и оценки активов, необходимо оценить вероятность событий риска. Как и в случае с оценкой активов, оценку вероятности можно получить на основании статистики по инцидентам, причины которых совпадают с рассматриваемыми угрозами ИБ, либо методом прогнозирования – на основании взвешивания факторов, соответствующих разработанной модели угроз.

Хорошей практикой для оценки вероятности станет классификация уязвимостей по выделенному набору факторов, характеризующих простоту эксплуатации уязвимостей. Прогнозирование вероятности угроз производится уже на основании свойств уязвимости и групп нарушителей, от которых исходят угрозы.

В качестве примера системы классификации уязвимостей можно привести стандарт CVSS – common vulnerability scorning system. Следует отметить, что в процессе идентификации и оценки уязвимостей очень важен экспертный опыт специалистов по ИБ, выполняющих оценку рисков, и используемые статистические материалы и отчеты по уязвимостям и угрозам в области информационной безопасности

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре завода по производству шин могут быть как внешними, так и внутренними.

Величину (уровень) риска следует определять для всех идентифицированных и соответствующих друг другу наборов «актив – угроза». При этом величина ущерба и вероятности не обязательно должны быть выражены в абсолютных денежных показателях и процентах; более того, как правило, представить результаты в такой форме не удается. Причина этого – используемые методы анализа и оценки рисков информационной безопасности: сценарный анализ и прогнозирование.

Сущность любого подхода к управлению рисками заключается в анализе факторов риска и принятии адекватных решений по обработке рисков. Факторы риска – это те основные параметры, которыми мы оперируем при оценке рисков. Таких параметров всего семь:

* Актив.
* Ущерб.
* Угроза.
* Уязвимость.
* Механизм контроля.
* Размер среднегодовых потерь.
* Возврат инвестиций.

Общий подход и схема рассуждений при оценке рисков примерно одинаковая, независимо от того, какая методология используется. Процесс оценки рисков включает в себя две фазы. На первой, которая определяется в стандартах как оценка рисков, необходимо ответить на следующие вопросы:

* Что является активом компании?
* Какова ценность актива?
* Какие существуют угрозы в отношении этого актива?
* Каковы последствия этих угроз и ущерб?
* Насколько уязвима система в отношении этих угроз?
* Каков ожидаемый размер среднегодовых потерь?

На второй фазе, которая определяется стандартами как оценивание рисков, необходимо ответить на вопрос: Какой уровень риска является приемлимым для организации и, исходя из этого, какие риски превышают этот уровень.

Таким образом, по результатам оценки рисков, мы получаем описание рисков, превышающих допустимый уровень и оценку величины этих рисков, которая определяется размером среднегодовых потерь. Далее необходимо принять решение по обработке рисков, ответить на следующие вопросы:

* Какой вариант обработки рисков выбираем?
* Если принимается решение о минимизации риска, то какие механизмы контроля необходимы?
* Насколько эффективны эти механизмы контроля и какой возврат инвестиций они обеспечат?

На выходе данного процесса появляется план обработки рисков, определяющий способы обработки рисков, стоимость контрмер, а также сроки и ответственных за реализацию контрмер.

Подводя итоги вышесказанного, обобщим их для военного комиссариата. Как уже было сказано, благодаря специфике работы военного комиссариата, атаки являются довольно редкими, так как даже при условии успешности, прибыль довольно мала. Однако вероятность угрозы все равно присутствует и руководству военного комиссариата, необходимо осознавать и представлять возможные угрозы, чтобы иметь возможность подготовиться к ним и предотвратить их полностью, либо минимизировать возможный ущерб.

В связи с этим, наиболее возможными видами атаки на военный комиссариат являются следующие:

* получение несанкционированного доступа к веб-сайту военного комиссариата. Данный тип атаки наименее опасен, поскольку у сайта так же нету связи с персональными данными. Однако злоумышленники могут испортить информацию на веб-сайте и благодаря этому извлечь какую-нибудь выгоду (также политическую);
* атака на военный комиссариат. Данная угроза очень маловероятна, но опасна прежде всего риском жертв среди сотрудников комиссариата;
* взлом базы данных комиссариата. База данных с персональными данными призывников наиболее ценный актив для злоумышленников;

Ответственными за реализацию контрмер являются, безусловно, сотрудники системы безопасности компании, наравне с сотрудниками IT-отдела, которые отвечают за информационную безопасность военного комиссариата.

## Разработка мер защиты

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

Целями защиты информации являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

При разработке политики безопасности можно использовать следующую модель (рис. 1), основанную на адаптации Общих Критериев (ISO 15408) и проведении анализа риска (ISO 17799).

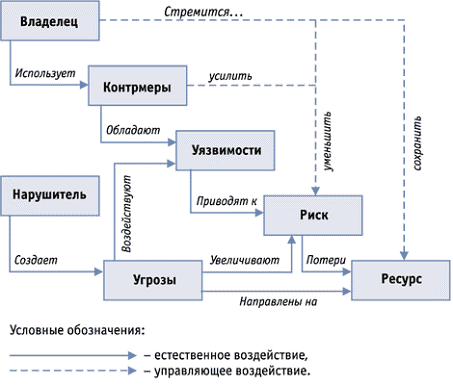


Рис 2 – Модель построения системы защиты информации

Представленная модель – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Рассматриваются следующие объективные факторы:

* угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;
* уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;
* риск – фактор, отражающий возможный ущерб в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Для создания эффективной политики безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для предприятия на основе заданного критерия. Политику безопасности и соответствующую корпоративную систему защиты информации предстоит построить таким образом, чтобы достичь заданного уровня риска.

Предлагаемая методика разработки политики информационной безопасности современного предприятия позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности, избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить различные варианты контрмер.

В ходе работ должны быть установлены границы исследования. Для этого необходимо выделить ресурсы информационной системы, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные, а также информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (архивах, фондах, банках данных, других информационных системах). Примерами внешних элементов являются сети связи, внешние сервисы и т.п.

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

Эта модель, в соответствии с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы защиты.

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

По завершении работ, можно будет определить меру гарантии безопасности информационной среды, основанную на оценке, с которой можно доверять информационной среде объекта. Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности. Адекватность оценки основана на вовлечении в процесс оценки большего числа элементов информационной среды объекта, глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения, строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки на военный комиссариат, можем выделить следующие рекомендации, либо советы, следуя которым возможно снизить риски опасного воздействия и их последствий:

* вооруженная охрана;
* четкая и строгая иерархия должностей и полномочий. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, милиции;
* защита главных серверов (если такие существуют) и важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к информации. (Уборщица не должна иметь доступ к бд и почтам сотрудникам) ;
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие наглядного отображения плана по работе во время чрезвычайных ситуаций.

Так же, эффективной мерой по защите является проведение тестовых экспериментов: наем специализированных людей, которые проведут атаку на сетевые ресурсы и выявят пробелы в защите.

Отдельный раздел законопроекта "О коммерческой тайне", посвященный организации защиты коммерческой информации, определяет необходимый комплекс мероприятий по ее защите:

* установление особого режима конфиденциальности;
* ограничение доступа к конфиденциальной информации;
* использование организационных мер и технических средств защиты информации;
* осуществление контроля за соблюдением установленного режима конфиденциальности.

Установление особого режима конфиденциальности направлено на создание условий для обеспечения физической защиты носителей конфиденциальной информации. Как правило, особый режим конфиденциальности подразумевает:

* организацию охраны помещений, в которых содержатся носители конфиденциальной информации;
* установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;
* установление пропускного режима в помещения, содержащие носители конфиденциальной информации;
* закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;
* установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);
* организацию ремонта технических средств обработки конфиденциальной информации;
* организацию контроля за установленным порядком.

Эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации (СЗИ). Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

* средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;
* средства, обеспечивающие защиту информации при передаче ее по каналам связи;
* средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
* средства, обеспечивающие защиту от воздействия программ-вирусов;
* материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако это способ требует значительных капитальных затрат и практически не применяется.

Обеспечение требуемой защиты информационных ресурсов предприятий в этих условиях достигается применением дополнительных инструментальных средств. К их числу относятся:

* средства анализа защищенности операционных систем и сетевых сервисов;
* средства обнаружения опасных информационных воздействий (атак) в сетях.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок, и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.

Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки на военкомат, можем выделить следующие рекомендации, либо советы, следуя которым возможно снизить риски опасного воздействия и их последствий:

* вооруженная охрана;
* четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, милиции;
* защита главных серверов (если такие существуют) и важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие как в магазинах, так и в офисах, наглядного отображения плана по работе во время чрезвычайных ситуаций.

Так же, эффективной мерой по защите является проведение тестовых экспериментов по атаке на фирму: наем специализированных людей, которые проведут атаку на сетевые ресурсы компании и выявят пробелы в защите.

## Выводы

Важно помнить, что, прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности. При этом политику безопасности желательно оформить в виде отдельного документа и утвердить руководством предприятия.

Приведенные выше меры по защите информации в военкомате являются лишь примерными. В реальности, следует провести комплексную оценку с привлечением специализированных людей, которые являются экспертами в вопросах обеспечения ИБ и проведением специальных тестов и экспериментов.

# Практическое занятие №4

**Тема «Настройка Брандмауэра Windows»**

**Цель**: Овладение навыками настройки и использования Брандмауэра Windows.

1. Включение брандмауэра

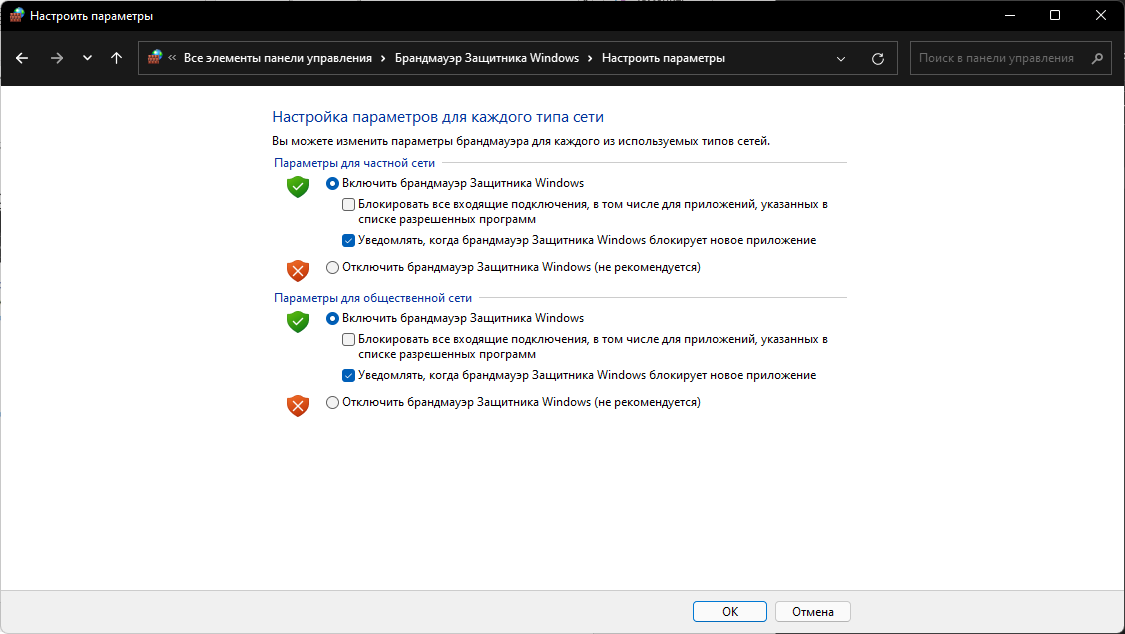
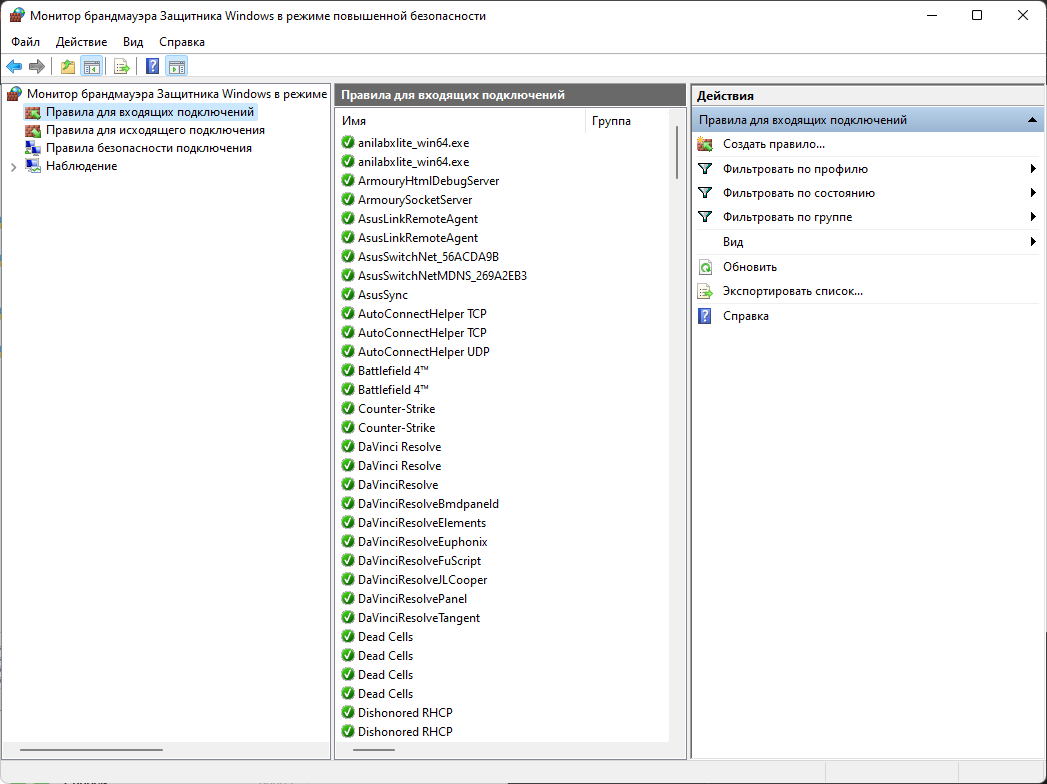


Рисунок 4.1 – Включение брандмауэра

2. Настройка входящих и исходящих подключений 

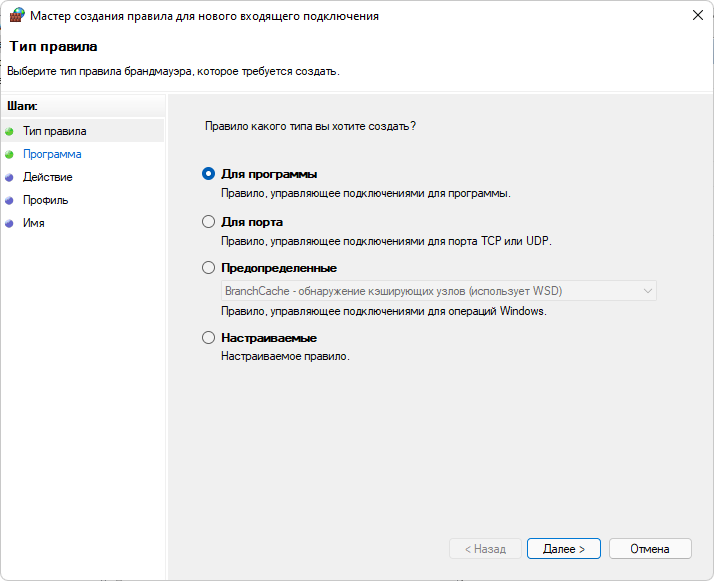
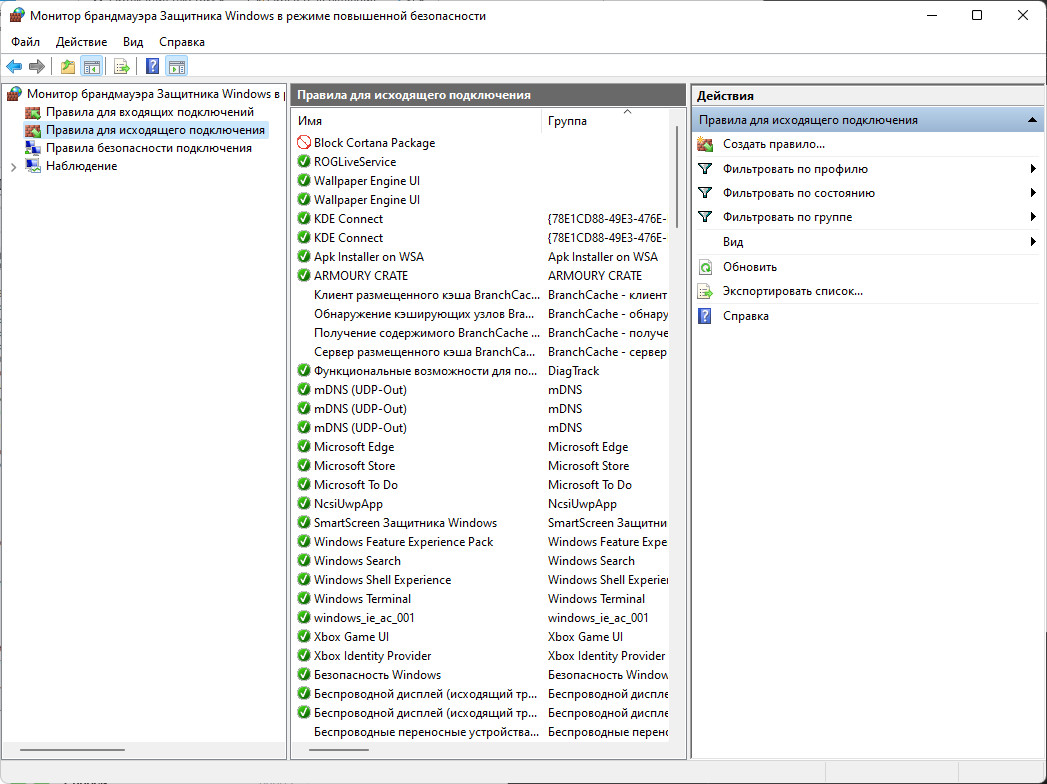
Рисунок 4.2 – Правила для входящих подключений  Рисунок 4.3 – Правила для исходящих подключений

Рисунок 4.4 - Мастер создания правил

3. Установка пути к приложению (mathcad.exe) и далее блокировка подключений.

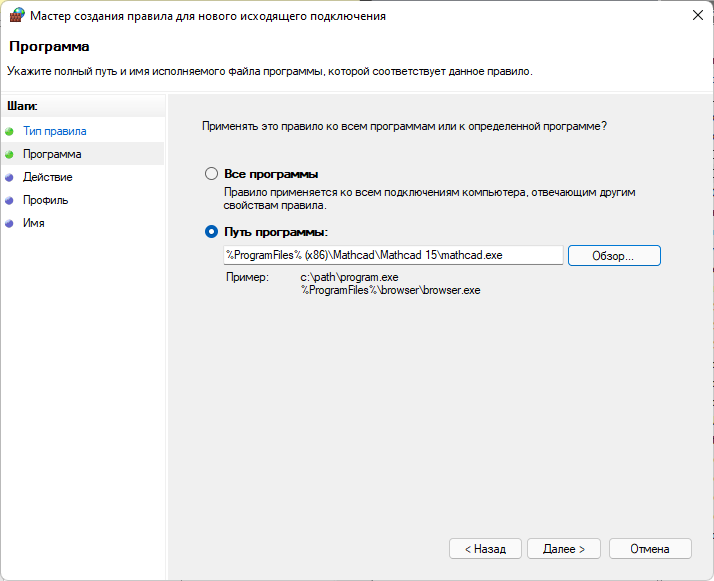


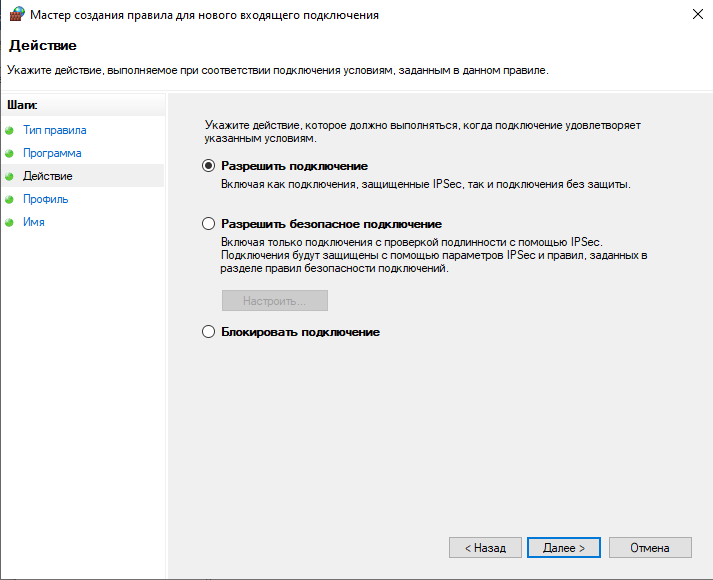
Рисунок 4.5 - Мастер создания правил, выбор пути

Рисунок 4.6 - Блокировка/разрешение подключения

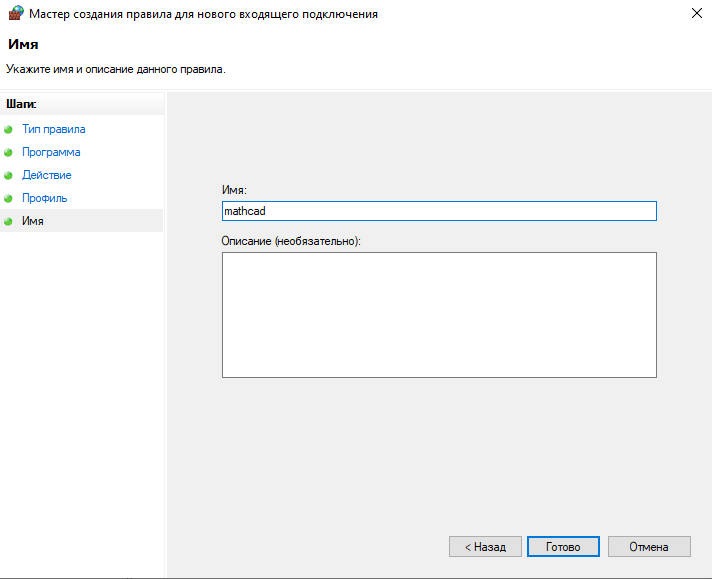


Рисунок 4.7 - Выбор имени

4. Наблюдаем правило в общем списке, а далее просматриваем его свойства.

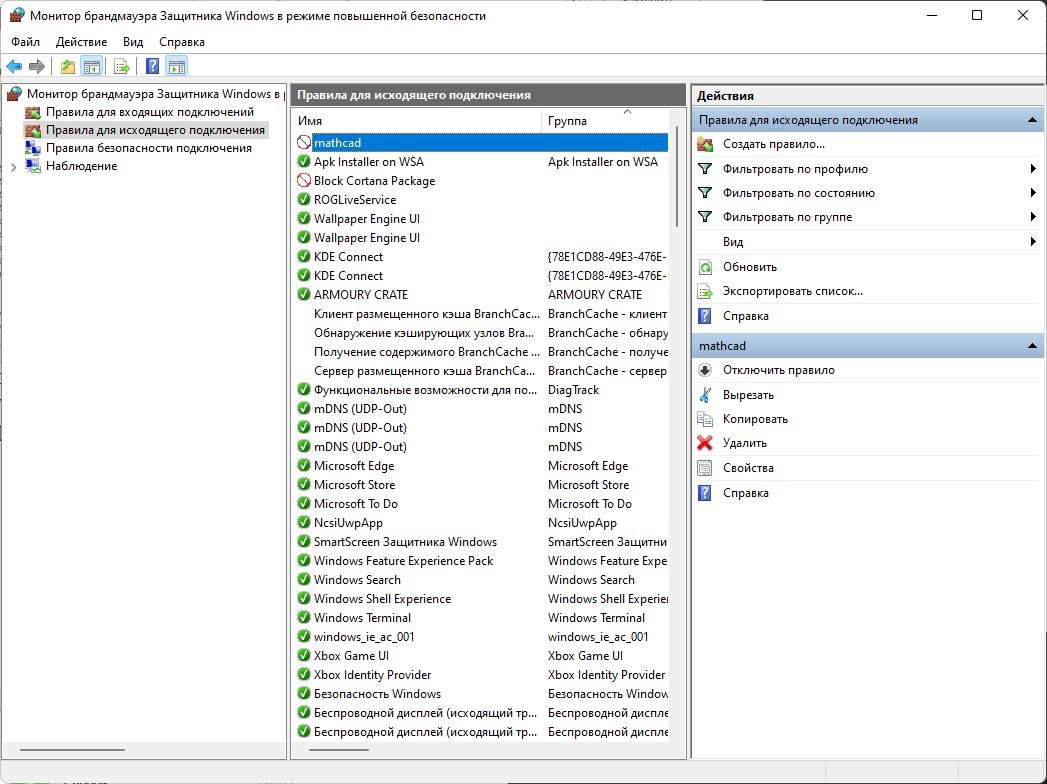


Рисунок 4.8 - Активные правила в списке

5. Проделываем такие же действия с исходящими подключениям. Ниже представленные иллюстрации соответствуют рис. 4.1-4.7.

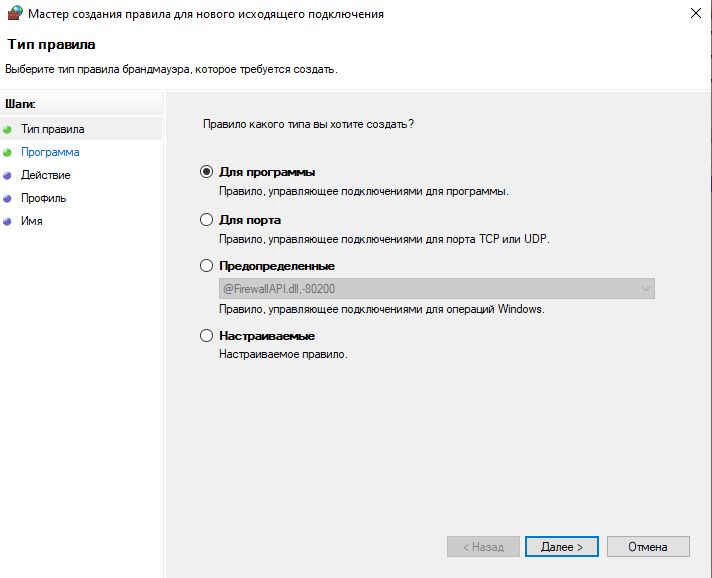


Рисунок 4.9 - Мастер создания правил

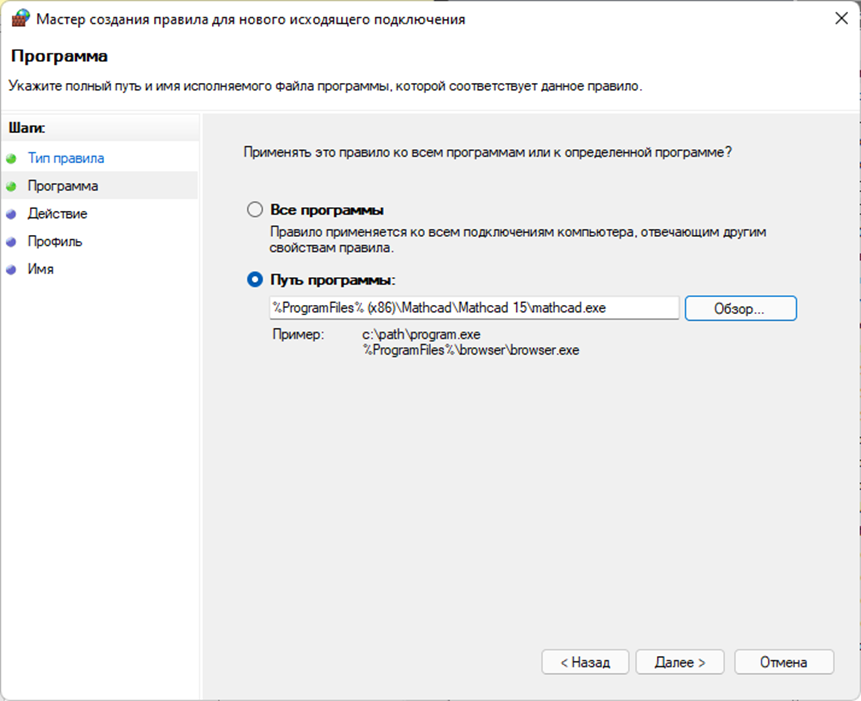


Рисунок 4.10 - Мастер создания правил, выбор пути

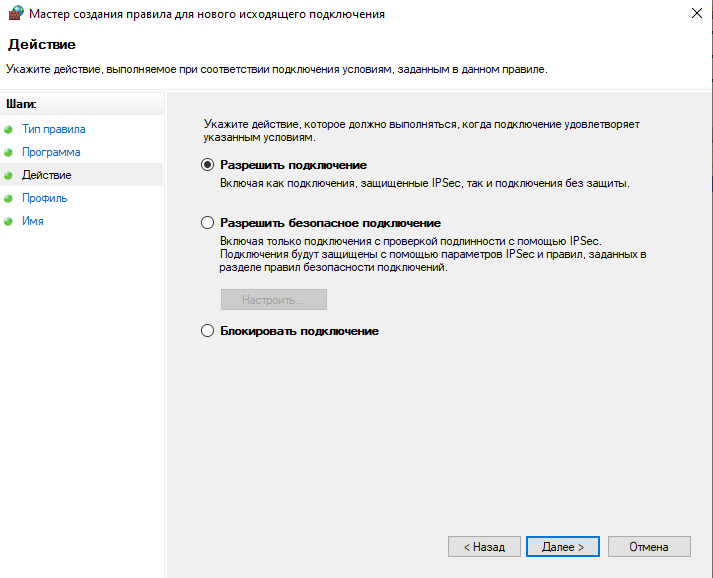


Рисунок 4.11 - Блокировка/разрешение подключения

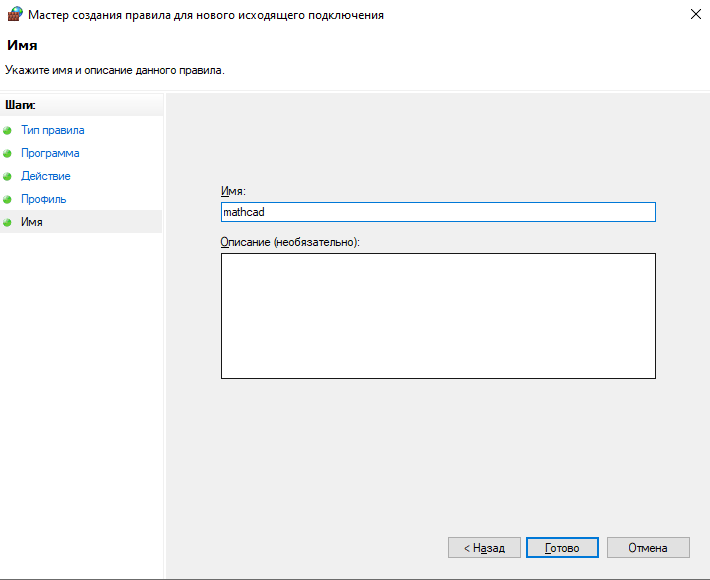


Рисунок 4.12 - Выбор имени

6. Опробовать действие нескольких команд:

1. Служба диагностики DirectX – dxdiag

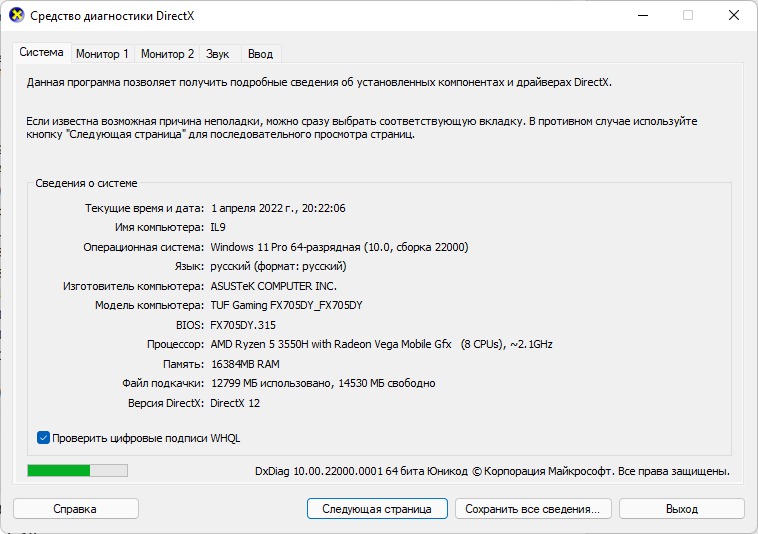


Рисунок 4.13 – Служба диагностики DirectX

2. Калькулятор – calc.

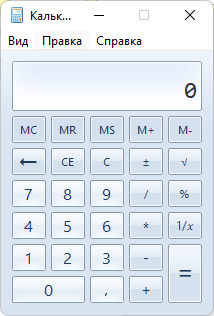


Рисунок 4.14 - Калькулятор

3. Производительность - perfmon.msc

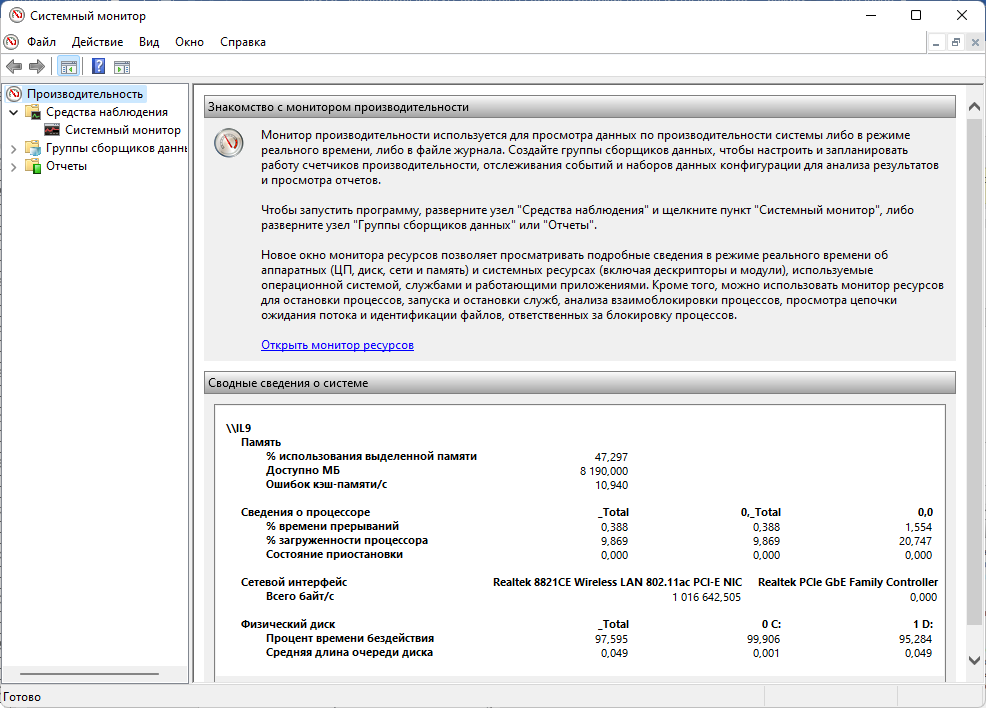


Рисунок 4.7 – Монитор производительности

**Вывод**: Я овладел навыками настройки и использования Брандмауэра Windows, научился создавать правила для блокировки и разрешения входящих и исходящих подключений.

# Практическое занятие №5

**Тема «Криптографическая защита информации»**

Цель: овладение основными криптографическими алгоритмами симметричного шифрования

Задание 1

Парибок Илья Александрович

**Шифр цезаря на 8:** Чзшрицт Рудж Зумтщзхлшцйря

Исходный алфавит: 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

Шифрованный: 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 А Б В Г Д Е Ё Ж

**Шифр Трисемуса:**

Ключевое слово: защита

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | . | , |  |

Итог: чдшжкцсжуидуосъдъншцлжя

**Шифр Плейфера:**

Ключевое слово: защита

|  |  |  |  |
| --- | --- | --- | --- |
| з | а | щ | и |
| т | б | в | г |
| д | е | ж | и |
| к | л | м | н |
| о | п | р | с |
| у | ф | х | ц |
| ч | ш | ъ | ы |
| ь | э | ю | я |

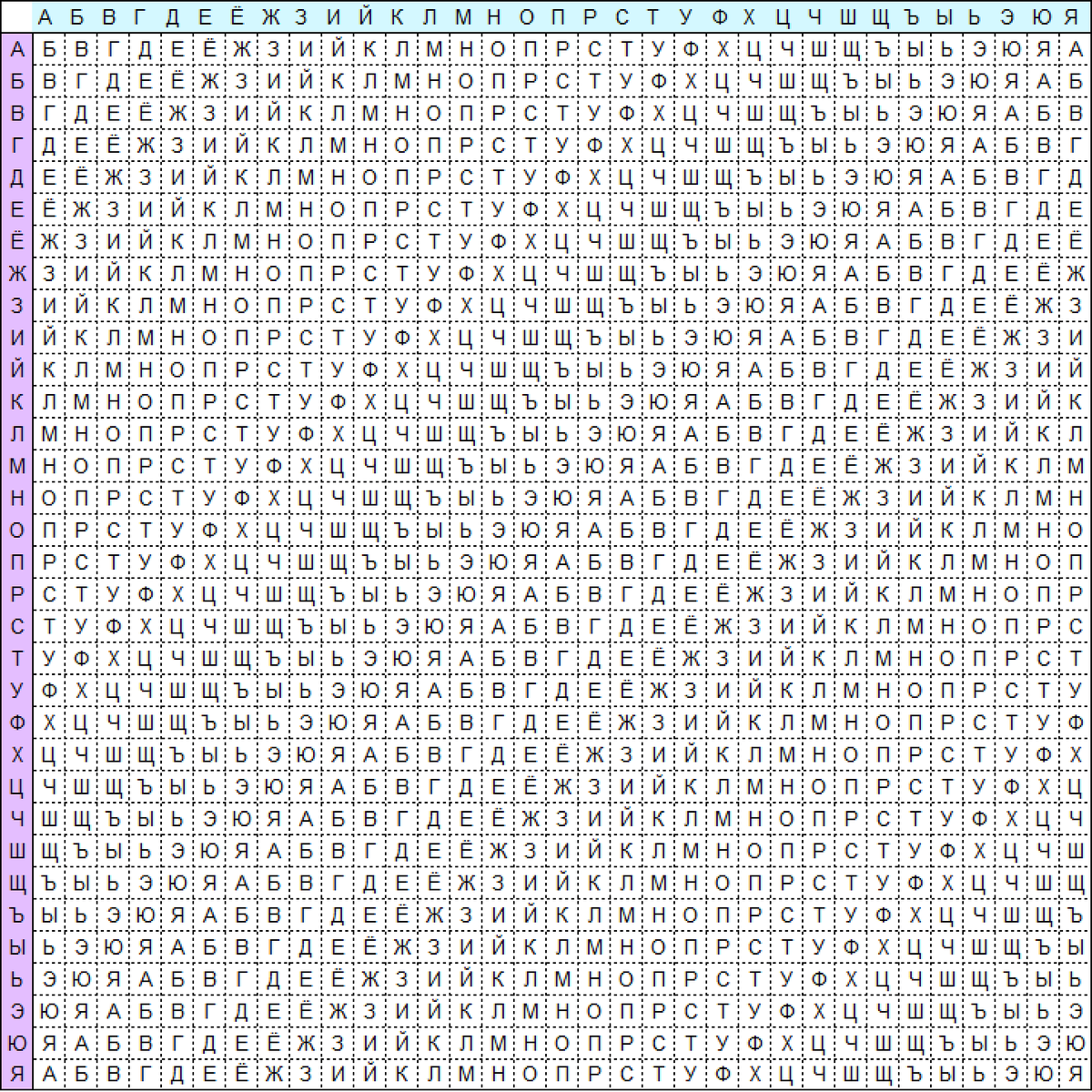
Па ри бо ки ль яа ле кс ан др ов ич

Итог: Фб сж пт нд кэ эи пл но ил ож рд ды

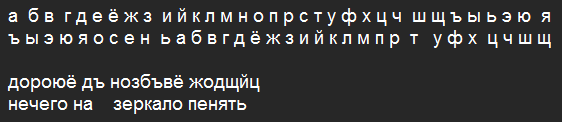
**:**

Парибокильяалександрович

Ключевое слово: защита



Итог: Шбктфпуйёётбфёеыуомсильш



|  |  |  |
| --- | --- | --- |
| 8 | **дороюё дъ нозбъвё жодщйц**  **Итог: нечего на зеркало пенять** | Расшифровать с помощью шифра Цезаря.  Ключ 5.  Ключевое слово ОСЕНЬ |

**Вывод**: овладел основными криптографическими алгоритмами шифрования.

# Практическая занятие №6

**Криптографическая защита информации**

**Цель:** Овладение основными криптографическими алгоритмами асимметричного шифрования.

**Ход работы:**

*RSA-ключи*

1) выбираются два различных случайных простых числа **p и q** заданного размера (например, 1024 бита каждое);

2) вычисляется их произведение **n = p ⋅ q**, которое называется модулем;

3) вычисляется значение функции Эйлера от числа n:

**φ ( n ) = ( p − 1 ) ⋅ ( q − 1 )**

4) выбирается целое число e ( 1 < e < φ ( n ), взаимно простое со значением функции φ ( n );

5) вычисляется число d, мультипликативно обратное к числу e по модулю φ ( n ), то есть число, удовлетворяющее сравнению:

**d ⋅ e ≡ 1**

6) пара **( e , n )** публикуется в качестве открытого ключа RSA (англ. RSA public key);

7) пара **( d , n )** играет роль закрытого ключа RSA (англ. RSA private key) и держится в секрете.

*Диффи Хеллмана*

1. генерирует случайное натуральное число **a — закрытый ключ;**
2. совместно с удалённой стороной устанавливает открытые параметры **p и g** (обычно значения p и g генерируются на одной стороне и передаются другой), где:

* **p** является случайным простым числом;
* **(p-1)/2** также должно быть случайным простым числом (для повышения безопасности);
* **g** является первообразным корнем по модулю p (также является простым числом);

1. вычисляет открытый **ключ A**, используя преобразование над закрытым ключом:

**A = g^a mod p**

1. обменивается открытыми ключами с удалённой стороной
2. вычисляет общий секретный **ключ K**, используя **открытый ключ удаленной стороны B** и свой **закрытый ключ a.**

Эль-Гамаля

1. Генерируется случайное простое число **p**.
2. Выбирается целое число **g** — первообразный корень **p**.
3. Выбирается случайное целое число **x** такое, что **( 1 < x < p − 1 )**.
4. Вычисляется:

**y = g^x (mod p)**

1. Открытым ключом является **( y , g , p )**, закрытым ключом — число **x**.

**Вывод:** в ходе практической работы я овладел основными криптографическими алгоритмами асимметричного шифрования.

# Практическое занятие №7

**Тема «Криптографическая защита информации»**

**Цель: изучить и закрепить умение реализации ЭЦП на примере RSA.**

Разберем наглядный «бумажный» пример и пример с кодом. Возьмем основу 6-ой лабораторной работы.

**«Бумажный» пример**

p = 89

q = 17

Сообщение: AAC

n = p \* q = 89 \* 17 = 1513

f(n) = (p - 1) \* (q - 1) = 88 \* 16 = 1408

e = 5;

Открытый ключ шифра: (5, 1513)

http://altaev-aa.narod.ru/security/images/im7.png

d вычисляется до тех пор, пока не получится первое целое число.

Причем k = 1, 2, 3 …

При k = 1, d – не целое число,

При k = 2, d – не целое число,

При k = 3, d = 845

Тогда закрытый ключ шифра: (845, 1513).

*Отправка сообщения и электронной подписи:*

Отправка сообщения и ЭЦП на базе алгоритма RSA (отправитель **A**).



Возьмем хеш-образ из примера h = 7.

Тогда цифровая подпись s = 7^845 mod 1513 = 1485

Далее получателю отправляется исходное сообщение и цифровая подпись.

*Получение сообщения и проверка электронной подписи:*

Получение сообщения и проверка ЭЦП на базе алгоритма RSA (получатель **B**).



**Программная реализация этой же задачи (на основе 6-ой лабораторной работы)**

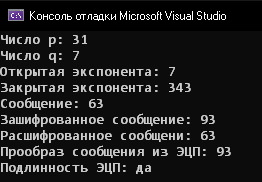


Рисунок 7.1 – Реализация ЭЦП на примере алгоритма RSA

**Контрольные вопросы:**

**1. Дайте определение понятию "электронная цифровая подпись".**

**Ответ:** реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе (Федеральный закон "Об электронной цифровой подписи").

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

**Ответ:** *отправитель* применяет к исходному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ **r** сообщения, вычисляет цифровую подпись **s** по хеш- образу **r** с использованием своего закрытого ключа, посылает сообщение **T** вместе с цифровой подписью **s** получателю. *Получатель* применяет к полученному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ **r** сообщения, расшифровывает хеш-образ **r’** из цифровой подписи **s** с использованием открытого ключа отправителя, проверяет соответствие хеш-образов r и r’ и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

**3. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП?**

**Ответ:** вначале отправитель использует свой закрытый ключ, а затем получатель применяет открытый ключ отправителя.

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

**Ответ:** выработка ЭЦП по формуле s = h^d mod n, где (d, n) – закрытый ключ отправителя. Вычисление хеш-образа из цифровой подписи по формуле h**”**= s^e mod n, где (e, n) – открытый ключ отправителя.

**5. Перечислите специальные схемы ЭЦП.**

**Ответ:**

* схема "конфиденциальной" (неотвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;
* схема подписи "вслепую" ("затемненной" подписи) - отправитель не знает подписанного им сообщения;
* схема "мультиподписи" - вместо одного отправителя сообщение подписывает группа из нескольких участников;
* схема "групповой" подписи - получатель может проверить, что подписанное сообщение пришло от члена некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано. В тоже время, в случае необходимости, отправитель может быть определен;
* и др.

**Вывод:** в ходе лабораторной работы была изучена и реализована ЭЦП на основе алгоритма RSA.

# Практическое занятие №8

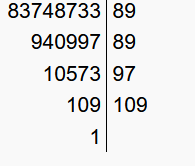
**Тема «Криптографическая защита информации»**

Цель: получение основных сведений из курса теории чисел

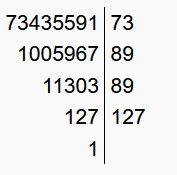
Вариант 8

1.Найти канонические разложения чисел а и b.

*а* = 83748733 = 89 ∙ 89 ∙ 97 ∙ 109



*b* = 73435591 = 73 ∙ 89 ∙ 89 ∙ 127



2. Найти НОД пользуясь a) алгоритмом Евклида, б) разложением чисел на простые множители.

а) Алгоритмом Евклида:

83748733 : 73435591 = 1 (остаток 10313142),

73435591 : 10313142 = 7 (остаток 1243597),

10313142 : 1243597 = 8 (остаток 364366),

1243597 : 364366 = 3 (остаток 150499),

364366 : 150499 = 2 (остаток 63368),

150499 : 63368 = 2 (остаток 23763),

63368 : 23763 = 2 (остаток 15842),

23763 : 15842 = 1 (остаток 7921),

15842 : 7921 = 2 (остаток 0),

Ответ: НОД (83748733; 73435591) = 7921

б) Найдём НОД (*a, b*), воспользовавшись разложением на простые множители чисел *a* и *b*, полученным в решении предыдущего задания:

*а* = 83748733 = 89 ∙ 89 ∙ 97 ∙ 109

*b* = 73435591 = 73 ∙ 89 ∙ 89 ∙ 127

Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел: НОД (83748733, 73435591) = 892 = 7921.

3. С помощью расширенного алгоритма Евклида найти целые u, v, удовлетворяющие соотношению Безу: au + bv = НОД.

*au* + *bv =* 83748733 *\* u +* 73435591*\* v =* НОД(83748733; 73435591) = 7921

u = -3425

v = 3906

83748733 *\** (-3425) *+* 73435591*\** (3906)*=* НОД(83748733; 73435591) = 7921

6. Найти остаток от деления  на 11.

1996 делится на 11 с остатком **5**. 1996 2 делится на 11 с остатком **3**. 1996 3 делится на 11 с остатком **4**. 1996 4 делится на 11 с остатком **9.** 1996 5 делится на 11 с остатком **1.** 1996 6 делится на 11 с остатком **5.** Получили один из предыдущих остатков, значит «зациклились». Число 1996 6 дает тот же остаток деления на 19, что и 1996. Значит, длина цикла равна 5. Число 1996 2003 дает тот же остаток от деления на 19, что и 1996 3, то есть 4.

1996 / 11 = 5 получили остаток от деления числа 1996 на 11 равный 5.

При последующем возведении в степень остатка при делении на 11 получаем те же остатки, что и при возведения в степень делителя.

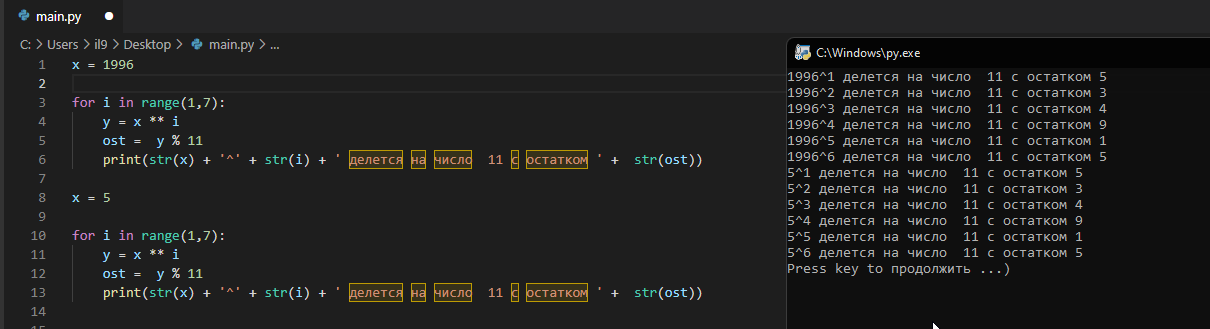
5^2 mod 11 = 3

5^3 mod 11 = 4

5^4 mod 11 = 9

5^5 mod 11 = 1

5^6 mod 11 = 5



**Вывод**: в ходе практической работы я получил основные сведения из курса теории чисел.

# Практическое занятие №9

**Тема «Авторское право и смежные права»**

Цель работы: изучить основные положения авторского права и смежных прав.

*Контрольные вопросы*:

1. На какие объекты распространяется авторское право?

Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения

1. Что относится к личным неимущественным (моральным) 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 искажении или любого иного посягательства, способных нанести ущерб чести и достоинству автора (право на защиту репутации автора).

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.

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?

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.

1. 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. 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.

1. Что такое авторский договор?

Авторский договор — это соглашение двух или более лиц, направленное на установление, изменение и прекращение взаимных прав и обязанностей, касающихся имущественных и связанных с ними личных неимущественных прав.

1. Наиболее распространенные виды авторских договоров?

Наиболее распространенные виды авторского договора:

* Издательский (издание и переиздание любых произведений, которые могут быть зафиксированы на бумаге, т.е. произведений литературы (научных, художественных, учебных и т.п.), драматических, сценарных, музыкальных произведений, произведений изобразительного искусства)
* Постановочный (основным способом использования произведения является его публичное исполнение)
* Сценарный (договор, который регламентирует отношения, связанные с использованием текста, по которому снимается кинофильм, телефильм, делается радио- или телепередача, проводится массово-зрелищное мероприятие)
* художественного заказа (опосредует отношения, связанные с созданием произведений изобразительного искусства в целях их публичной демонстрации)

- об использовании в промышленности неопубликованного произведения декоративно-прикладного искусства.

1. Основные составляющие авторского договора?

Авторский договор должен предусматривать способы использования произведения (конкретные права, передаваемые по данному договору)

При отсутствии в авторском договоре условия о сроке передачи прав договор может быть расторгнут автором по истечении пяти лет с даты его заключения

При отсутствии в авторском договоре условия о территории, на которую распространяется действие этого права на указанный срок, действие передаваемого по договору права ограничиваются территорией РБ.

Размер и порядок начисления авторского вознаграждения за использование произведений литературы, науки и искусства устанавливаются в авторских договорах и (или) в договорах на право использования произведений, которые пользователи обязаны заключить с иными правообладателями либо с организациями, управляющими имущественными правами авторов.

Вознаграждение определяется в авторском договоре в виде процента от дохода за соответствующий способ использования произведения, или в виде твердо зафиксированной суммы, или иным образом.

**Вывод**: в ходе практической работы я изучил основные положения авторского права и смежных прав.

# Практическое занятие №10

**Тема «Составление и оформление заявок на объекты промышленной собственности»**

Цель работы: овладеть навыками составления и оформления заявок на объекты промышленной собственности.

*Контрольные вопросы:*

1. Основные составляющие описания изобретения?

* область техники, к которой относится изобретение;
* уровень техники;
* сущность изобретения;
* перечень фигур чертежей, если они прилагаются с кратким указанием на то, что изображено на каждой из них. Если представлены иные материалы, поясняющие сущность изобретения, то перечисляют их;
* сведения, подтверждающие возможность осуществления изобретения.

1. Правила оформления описания изобретения?

Описание начинается с названия изобретения и указания индекса или индексов рубрики действующей редакции международной патентной классификации, к которой относится заявляемое изобретение. Названия разделов в тексте описания не указываются. Не допускается замена раздела «Описание» в целом или его части отсылкой к источнику, в котором находятся необходимые сведения. В разделе «Уровень техники» приводятся сведения об аналогах и прототипах.

1. Какие основные пункты должна содержать заявка на изобретение?

Заявка должна содержать документы:

* заявление о выдаче свидетельства;
* депонируемые материалы, содержащие комплект одного из следующих видов материалов: фотографии фотошаблонов; сборочный Топологический чертеж; послойные топологические чертежи; фотографии каждого слоя топологии;
* образцы ИМС с данной топологией в случае использования ее до даты подачи заявки;
* реферат;
* доверенность (в случае подачи через патентного поверенного).

1. Основные документы, необходимые для подачи заявки на изобретения?

Заявка подается в трех экземплярах и должна содержать:

* заявление о выдаче патента (типовой бланк);
* описание изобретения, раскрывающее его с полнотой достаточной для осуществления изобретения;
* формулу изобретения, выражающую его сущность и полностью основанную на описании;
* чертежи и иные материалы, если они необходимы для понимания сущности изобретения;
* реферат;
* доверенность в случае подачи заявки патентным поверенным.

1. ОТЛИЧИЯ заявок на охранные документы различных объектов промышленной собственности?

*Заявка на изобретение:*

Заявка на выдачу патента на изобретение подается автором изобретения, нанимателем, если изобретение служебное. Заявка подается в трех экземплярах. Вместе с заявкой или не позднее 2-х месяцев с даты ее подачи в одном экземпляре предоставляется документ, подтверждающий уплату пошлины в установленном размере.

*Заявка на выдачу патента:*

В данном разделе необходимо указать состав заявки, сколько экземпляров заявки необходимо подавать в патентный орган, а также на каких языках оформляется заявка. Временная правовая охрана заявленному изобретению предоставляется с даты публикации заявки до даты публикации сведений о патенте. Заявку на полезную модель преобразовать в заявку на изобретение возможно до даты получения решения о выдаче патента на полезную модель.

*Заявка на полезную модель:*

Заявка на полезную модель должна относиться к одной полезной модели или группу полезных моделей, связанных между собой так, что они образуют единый творческий замысел. До даты получения заявителем решения о выдаче патента на полезную модель, а в случае принятия решения об отказе в выдаче патента - до момента истечения срока его обжалования, возможно преобразование заявки на полезную модель в заявку на изобретение. Патент на полезную модель действует в течение пяти лет, считая с даты подачи заявки в патентный орган.

1. На какие ОПС выдаются патенты?

Патентно-лицензионная деятельность, регистрация объектов интеллектуальной собственности (ОИС), изобретения, полезные модели, промышленные образцы, товарные знаки и знаки обслуживания, топологии интегральных микросхем, компьютерные программы, оценка объектов интеллектуальной собственности (ОИС), процедура получения охранных документов.

1. На какие ОПС выдаются свидетельства?

Топологии интегральной микросхемы.

**Вывод**: в ходе практической работы я овладел навыками составления и оформления заявок на объекты промышленной собственности.

# Практическое занятие №11-12

**Тема «Патентный поиск»**

Цель работы: изучить виды, содержание и порядок проведения патентных исследований.

**Теоретическая часть**

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 сами либо о содержании которых ему может быть законным путем сообщено.

*Международные классификаторы*

Для обеспечения единообразия в международном масштабе распределения патентных документов, а также упрощения поиска необходимой патентной документации применяются специально разработанные патентные классификаторы.

**Международная патентная классификация (МПК)**, принятая в соответствии со Страсбургским соглашением 1971 года, предусматривает создание единой системы классификации, охватывающей патенты на изобретения, включая опубликованные патентные заявки, авторские свидетельства, полезные модели и свидетельства о полезности. Аббревиатура **«МПК»** является общепринятым обозначением Международной патентной классификации.

**Международная классификация промышленных образцов (МКПО)** была принята 8 октября 1968 года дипломатической конференцией в г. Локарно (Швейцария), на которую были приглашены все страны-участницы Парижской конвенции по охране промышленной собственности.

**Международная классификация товаров и услуг (МКТУ)** в соответствии с Ниццким соглашением от 15 июня 1957 г., отражая единую классификацию товаров и услуг для регистрации товарного знака, позволяет c максимальной достоверностью идентифицировать и, соответственно, классифицировать товар или услугу с обеспечением их единообразного восприятия всеми заинтересованными лицами.

**Универсальная десятичная классификация** **(УДК),** первое сводное издание которой, вышло в 1905 г. в Брюсселе, получила широкое применение в качестве единой системы классификации информационных материалов в области естественных и технических наук. Ее применение позволяет обеспечить единообразие в организации справочно-информационных фондов в органах научно-технической информации, научных и технических библиотеках страны.

*Международная патентная классификация (МПК)*

**МПК** является средством для единообразного в международном масштабе классифицирования патентных документов, позволяет эффективно осуществлять поиск патентных документов с целью установления новизны и оценки вклада изобретателя в заявленное техническое решение (включая оценку технической прогрессивности и полезного результата).

**МПК**, кроме того, является:

* инструментом для упорядоченного хранения патентных документов, что облегчает доступ к содержащейся в них технической и правовой информации;
* основой для избирательного распределения информации среди потребителей патентной информации;
* основой для определения уровня техники в отдельных областях;
* основой для получения статистических данных в области промышленной собственности, что в свою очередь позволит определять уровень развития различных отраслей техники.

**МПК** охватывает все области знаний, объекты которых могут подлежать защите охранными документами. Иерархическая структура МПК выражается в разбивке всех областей знаний на несколько классификационных уровней. В нисходящем порядке эти уровни иерархии соответствуют разделам, классам, подклассам, основным группам и подгруппам.

По своей структуре МПК разделена на восемь основных разделов.

***Индекс раздела.*** Каждый раздел обозначен заглавной буквой латинского алфавита от **А** до **Н**.

***Заголовок раздела*** лишь приблизительно отражает его содержание. Разделы имеют следующие названия:

**A** – удовлетворение жизненных потребностей человека;

**B** – различные технологические процессы; транспортирование;

**C** – химия; металлургия;

**D** – текстиль; бумага;

**E** – строительство; горное дело;

**F** – механика; освещение; отопление; двигатели и насосы; оружие; боеприпасы; взрывные работы;

**G** – физика;

**H** – электричество.

***Содержание раздела***. В оглавлении к каждому разделу помещен перечень относящихся к нему *классов* и *подклассов*.

***Подраздел.*** Внутри разделов родственные классы условно объединяются в подразделы, которые не обозначаются индексами.

**Практическая часть**

Необходимо выполнить экспертизу патентной чистоты разработанных конструктивных решений:

* + - методов испытания материалов и устройств для их осуществления;
    - устройств и механизмов для реализации технологических процессов

*Задание.* В результате проведения исследовательских работ было предложено конструктивное выполнение ПС Криптовалютного кошелька.

Наличие предполагаемых существенных признаков и планируемый выпуск продукции являются предпосылками для патентования разработки.

Необходимо выполнить экспертизу патентной чистоты разработанного конструктивного решения (ОПС).

В качестве существенных признаков при патентовании предполагаемого изобретения, выносится конструктивный признак: разработка бизнес-логики для транзакций и хранения криптоактивов.

*Выполнение задания*. Для выявления патентной чистоты разработанного объекта промышленной собственности следует использовать следующий регламент поиска:

* объект – *Криптовалютный кошелёк*;
* страна поиска – *Российская Федерация*;
* источники информации – *МПК*;

Для проведения патентного поиска необходимо определить классификационную рубрику предполагаемого изобретения, которая в данном случае, классифицируется по разделу **«Технологические процессы»**

Проведенный патентный поиск по указанному классу, выявил следующие аналогичные по конструктивному выполнению патенты и полезные модели, данные по которым сводятся в соответствующую таблицу.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Предмет поиска (объект исследования, его составные части) | Страна выдачи, вид и номер охранного документа. Классификационный индекс | Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвенционный приоритет, дата публикации | Название изобретения (полезной модели, промышленного образца) | Сведения о действии охран-ного документа или причина его аннулирования (только для анализа патентной чистоты) |
| Cryptocurrency wallet | USA  G06Q20/3674  G06Q20/065 | Michael Strong  Daniel Khesin  2019-11-28  Publication of US20190362340A1 | «Secure multiple cryptocurrency wallet and methods of use thereof» | Abandoned |
| USA  G06Q20/367  G06Q20/0658  G06Q20/3678  G06Q20/38215  G06Q20/3829  G06Q2220/00 | Massimiliano PalaBrian  A. ScriberSteven  J. Goeringer  2019-09-26  Publication of US20190295069A1 | «Systems and methods for integrating cryptocurrency wallet identifiers with digital certificates» | Pending |
| USA  G06Q20/3678  G06F21/57  G06F21/62  G06F21/645 | Lior Lamesh  2021-02-18  Publication of US20210049591A1 | «Cryptocurrency wallet and cryptocurrency account management» | Pending |
| USA  G06Q20/065  G06Q20/0855  G06Q20/145  G06Q20/3678  H04L2209/56 | Anthony Loera  2015-08-13  Publication of US20150227897A1 | Method of Making, Securing, and Using a Cryptocurrency Wallet | Abandoned |

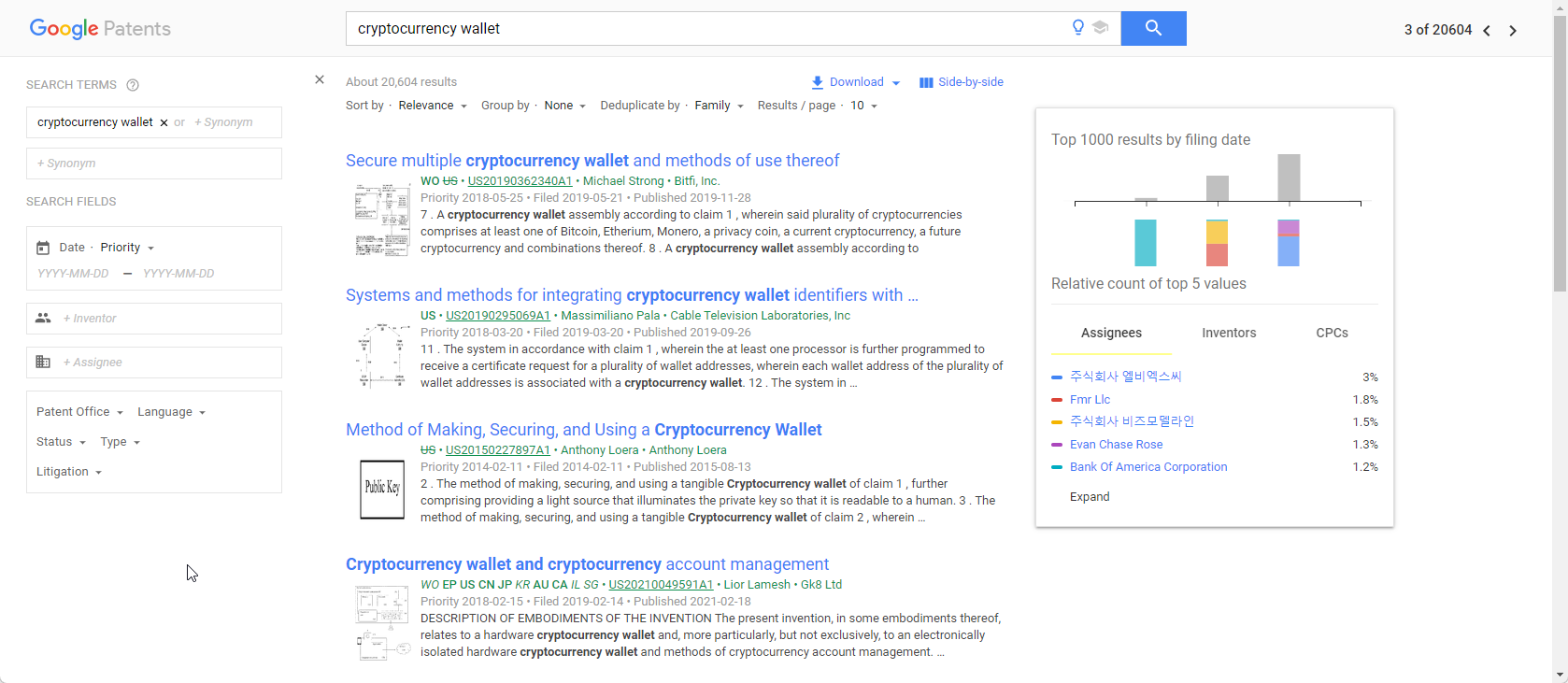
*Патентный поиск*

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

Патентный поиск выполнен по ключевым словам: «пациенты медицинского учреждения»

Данные-результаты были получены в ходе выполнения поиска на сайте:

<https://patents.google.com/?q=cryptocurrency+wallet&oq=cryptocurrency+wallet>

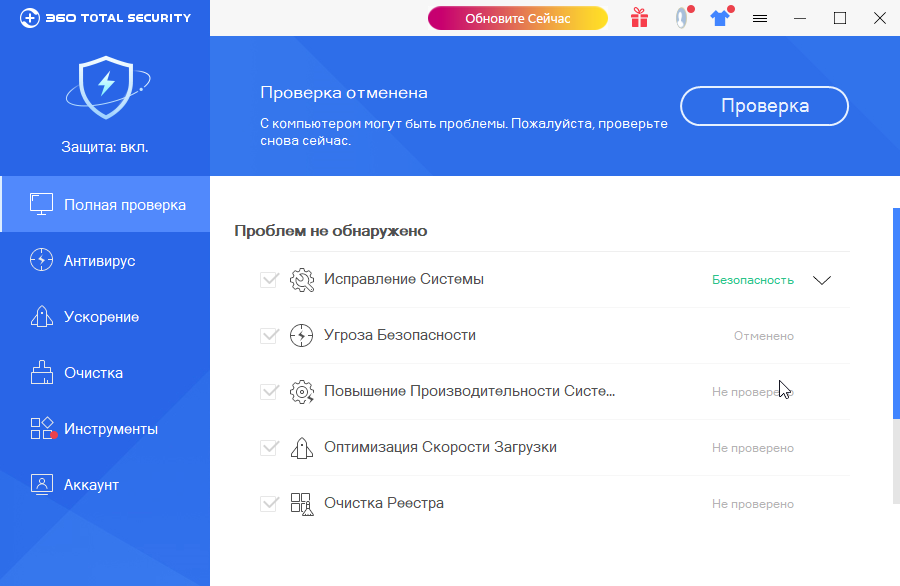


# Практическое занятие №13

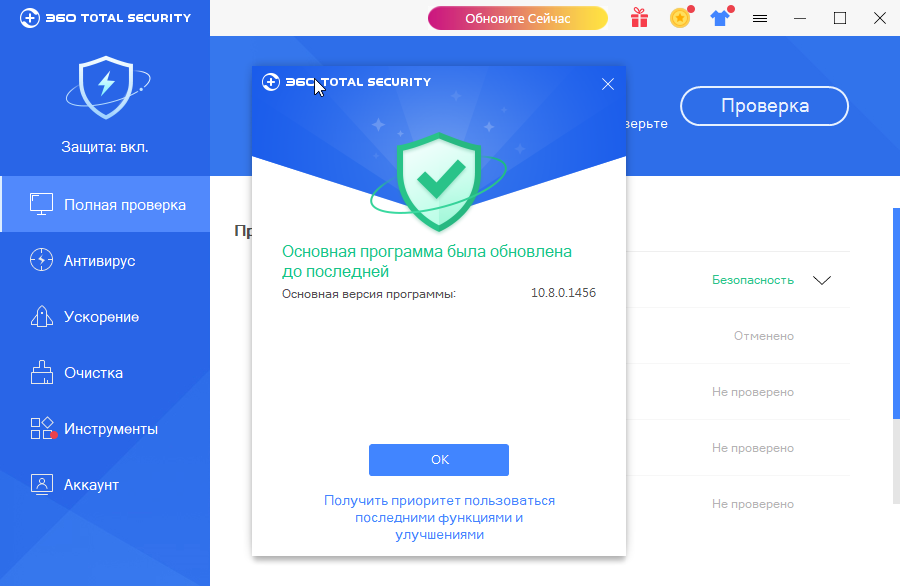
**Тема «Настройка антивирусов»**

Цель работы: овладение навыков настройки и использования антивирусов.

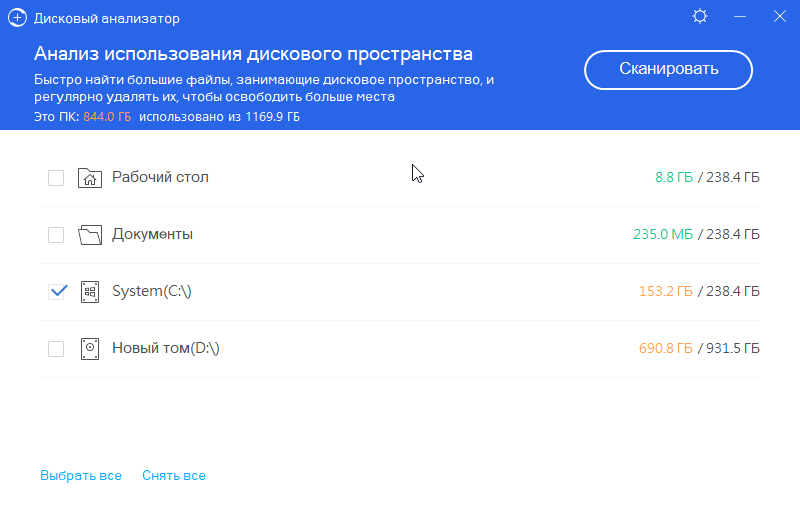
Рассмотрим антивирусное программное обеспечение 360 Total Security.



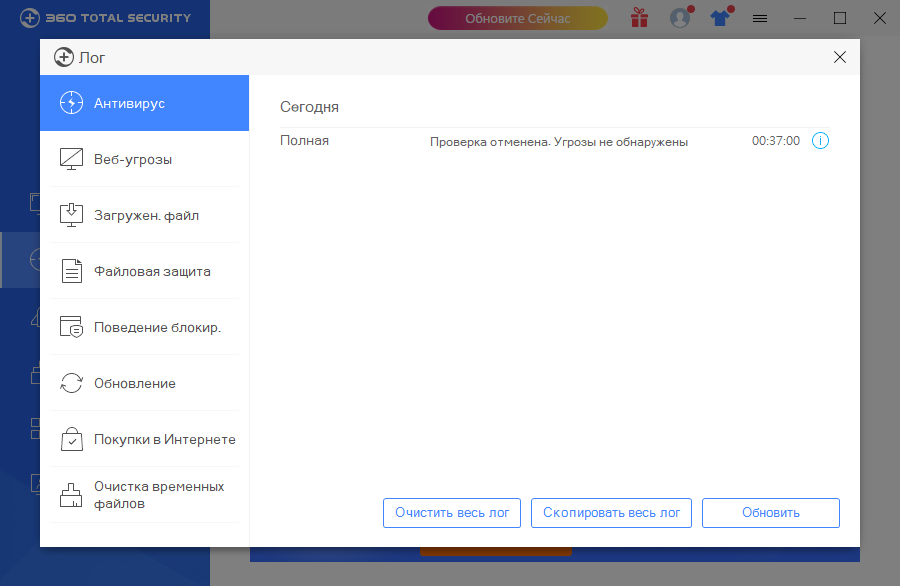
Основной экран настроек



Проверка установки обновлений



Проверка дисковых устройств



Журнал сканирования

Вывод: в ходе практической работы я овладел навыками настройки и использования антивирусов.

# Практическое занятие №14

**Тема « Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование с использованием библиотеки** [**System.Security.Cryptography**](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography)**»**

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. Какие симметричные алгоритмы шифрования Вы знаете?

В симметричном шифровании один и тот же ключ используется как для шифрования, так и для дешифрования. В этом методе исходное сообщение преобразуется в нераспознаваемое сообщение, которое невозможно идентифицировать. Это преобразованное сообщение называется зашифрованным текстом. Это делается с помощью ключа и алгоритма шифрования. На принимающей стороне зашифрованный текст преобразуется обратно в исходное сообщение с использованием того же ключа и алгоритма дешифрования.

Поскольку обе стороны используют один и тот же ключ, симметричное шифрование намного быстрее. С другой стороны, ключ должен быть доступен для расшифровки сообщения. Поэтому для передачи ключа требуется защищенный канал. В целом, симметричное шифрование является простым методом и не требует много времени для завершения. RC4, AES, DES, 3DES - это некоторые распространенные алгоритмы симметричного шифрования.

1. Какие ассиметричные алгоритмы шифрования Вы знаете?

Асимметричное шифрование использует два ключа для шифрования и дешифрования. Эти два ключа называются закрытым ключом и открытым ключом. Он использует открытый ключ для шифрования и закрытый ключ для расшифровки. Открытый ключ доступен для стороны, которая хочет отправить сообщение. Закрытый ключ принадлежит владельцу сообщения. Сообщение, которое зашифровано открытым ключом и алгоритмом шифрования, может быть дешифровано с использованием алгоритма дешифрования и соответствующего закрытого ключа соответствующего открытого ключа.

В целом, асимметричное шифрование обеспечивает большую безопасность данных. С другой стороны, использование двух ключей делает асимметричное шифрование трудоемким и более сложным. Алгоритм Диффи-Хеллмана и RSA - это некоторые распространенные алгоритмы асимметричного шифрования.

1. Основное назначение библиотеки System.Security.Cryptography?

Предоставляет криптографические службы, включая безопасное кодирование и декодирование данных, а также множество других операций, таких как хэширование, генерация случайных чисел и проверка подлинности сообщений.

1. Влияет ли размер ключа на криптостойкость алгоритма?

Размер ключа измеряется в битах (двоичных разрядах). Чем он больше, тем, соответственно, больше времени необходимо на перебор возможных значений, но и тем продолжительнее работает алгоритм. Поэтому выбор оптимальной длины ключа — это вопрос баланса.

1. Назовите основные классы библиотеки System.Security.Cryptography?

Класс CSPParameters – содержит параметры, передаваемые поставщику служб шифрования (CSP), который выполняет криптографические вычисления.

Класс CspParameters представляет параметры, которые можно передавать управляемым криптографическим классам, использующим службы шифрования (CSP), с помощью интерфейса Microsoft Cryptography API (CAPI).

Класс RSACryptoServiceProvder - выполняет шифрование и дешифрование данных с помощью реализации асимметричного алгоритма RSA, предоставляемого поставщиком служб шифрования (CSP).

Структура RSAParameters - представляет стандартные параметры для алгоритма RSA (значения d, e, n, p, q и т.д.)

Класс RijndaelManaged – реализует симметричный алгоритм шифрования Rijndael. Поддерживаются ключи длиной 128, 192 и 256 бит.

*Вывод*: в ходе практической работы я изучил модель криптографии .NET Framework, основные классы и структуры данных.