Учреждение образования

«Белорусский государственный технологический университет»

**Отчеты по практическим работам**

По дисциплине: «Основы защиты информации»

Студента 2 курса 1 группы ФИТ

Пирейко Дмитрия Михайловича

**2022 г.**

**Практическая работа №1**

**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 за­ щиты 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** - 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.

**Практическая работа №2**

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

Цель: научиться решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E*0 | *E* | *K* | *C* |
| 18 | 110000 | 91000 | 50 | 5000 |

Решение:

Найдем, на какую величину уменьшается полезный эффект функционирования объекта:

Рассчитаем относительную эффективность:

Найдем снижение эффективности функционирования объекта:

В итоге формулы выше принимают следующий вид:

Если эффективность функционирования объекта имеет стоимостное выражение (доход, прибыль и т.д.), то UΣ (суммарный ущерб) непосредственно изменяет эффективность:

**Вывод**: в ходе практической работы я научился решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа. Полученная прибыль составляет 13620.

**Практическая работа №3**

**Разработка политики информационной безопасности бизнес-компании**

**Введение**

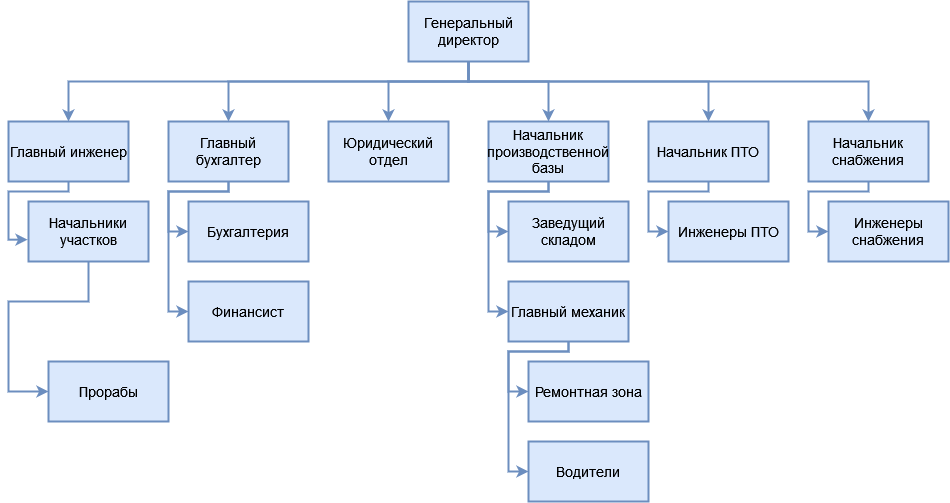
Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности 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.

**Описание структуры компании**

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.

Опишем структуру строительной организации «Новострой»:



**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 наш взгляд, этот вопрос наиболее важен, и ответ должна давать используемая методика анализа рисков.

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.

**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.**

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.

Такиим 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 так же сроки и ответственных за реализацию контрмер.

Подводя итоги вышесказанного, обобщим их. Как уже было сказано, благодаря специфике работы, атаки являются довольно редкими, так как даже при условии успешности, прибыль довольно мала. Однако вероятность угрозы все равно присутствует и руководству компании 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 следующие:

* получение несанкционированного доступа к веб-сайту. Данный тип атаки наименее опасен, поскольку у сайта так же нету связи с финансовой системой сети. Однако злоумышленники могут испортить информацию на веб-сайте и благодаря этому извлечь какую-нибудь выгоду, либо осуществить «взлом» просто ради интереса;
* атака на организацию. Данная угроза очень опасна прежде всего риском жертв среди сотрудников фирмы. При осуществлении данной атаки, преступники могут завладеть финансами и/или банковскими данными компании;
* взлом банковского счета организации. В настоящее время у любой компании имеется свой счет, на котором находятся деньги фирмы. Естественно, данная угроза наименее зависима от сети, так как атака осуществляется на банк. Тем не менее, компания должна предусмотреть данный случай и минимизировать его возможность;
* недобросовестная конкуренция. Данная угроза так же присутствует всегда у любой компании, независимо от ее размера, поэтому ей необходимо уделить внимание при разработке политики информационной безопасности;

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

**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.

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.

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, можем выделить следующие рекомендации, либо советы, следуя которым возможно снизить риски опасного воздействия и их последствий:

* охрана собственности организации;
* четкая и строгая иерархия должностей и полномочий. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь каждого работника с экстренными службами и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, милиции;
* защита важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам;
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие в колледже 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. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.

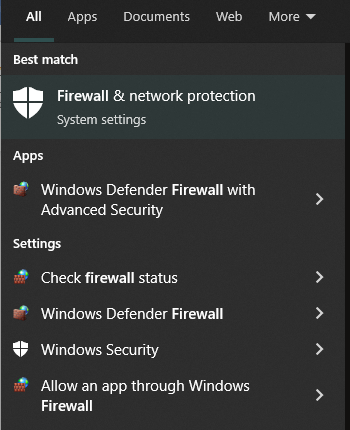
**Выводы**

Приведенные выше меры по защите информации 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.

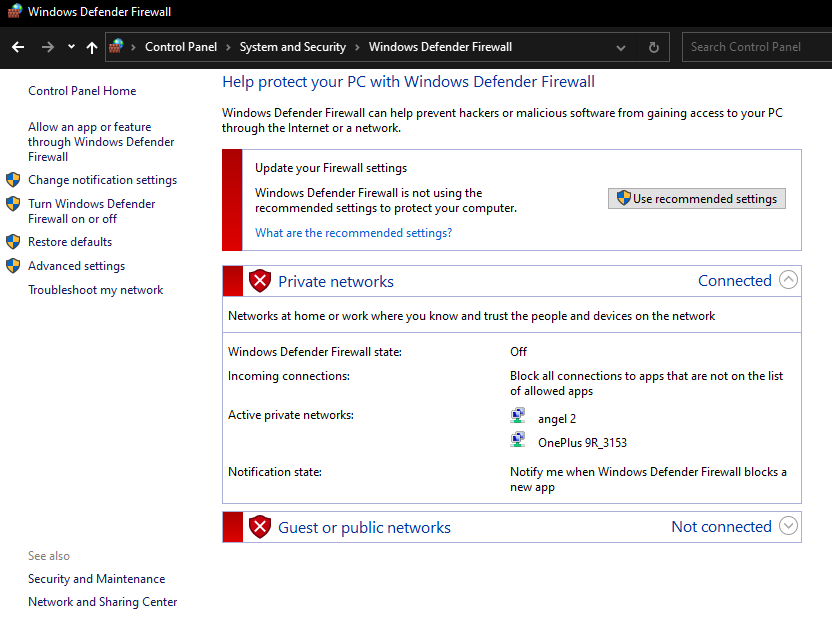
**Практическая работа №4**

**Настройка Брандмауэра Windows**

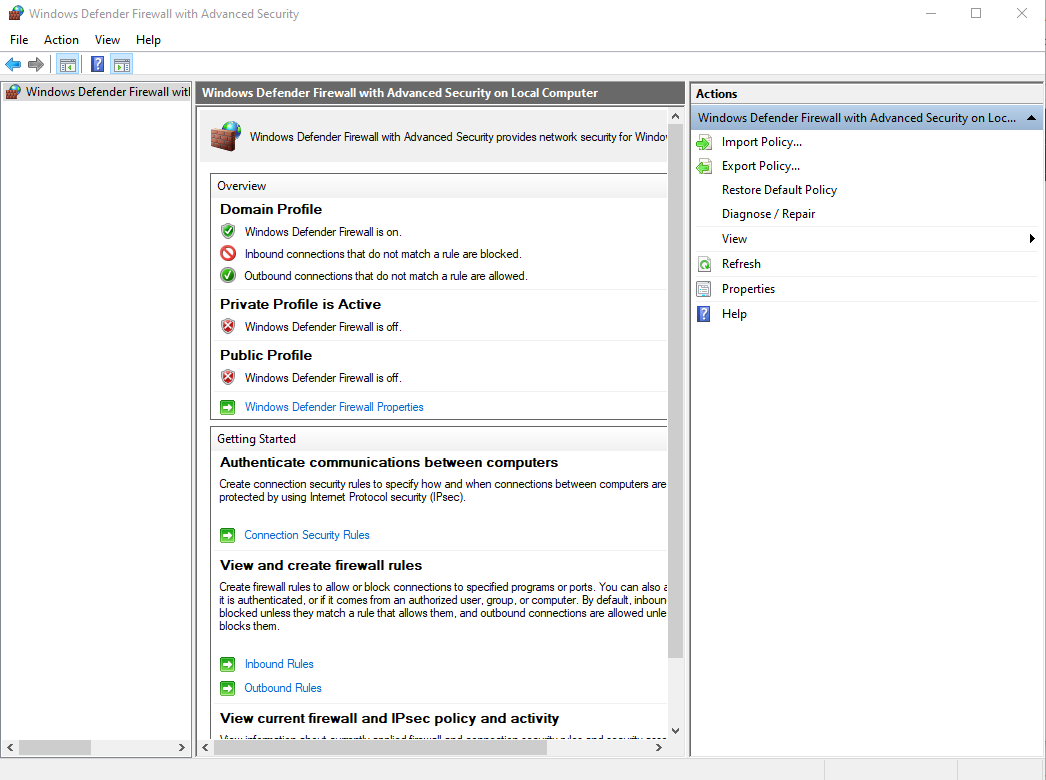
Цель: Овладение навыками настройки и использования Брандмауэра Windows.



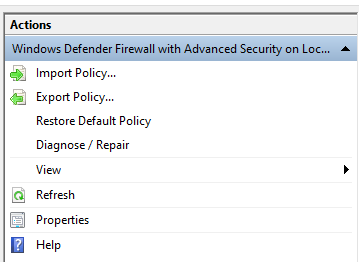
Поиск брандмауэра



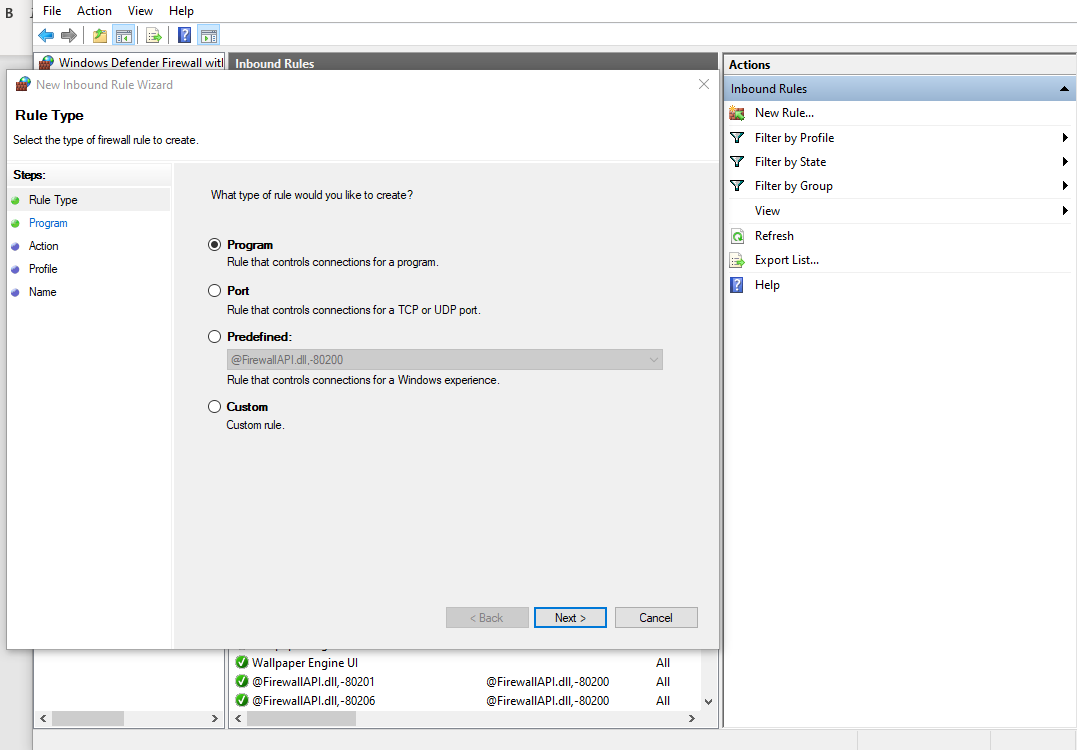
Общая информация



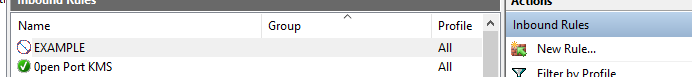
Монитор брандмауэра



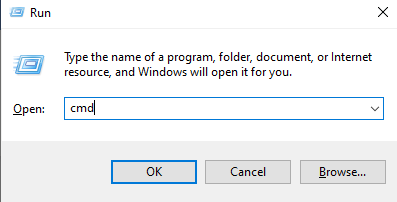
Работа с политикой



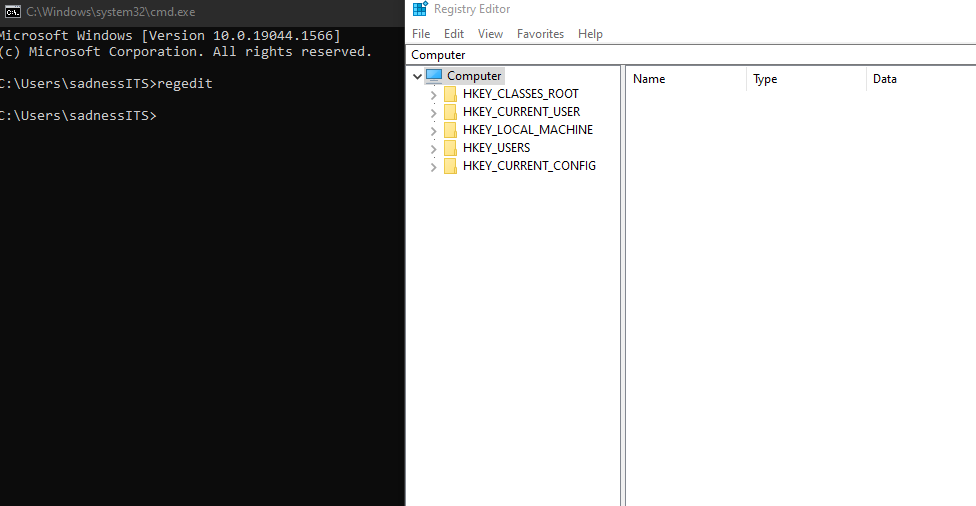
Создание правила



Итоговое созданное правило



Один из способов вывода командной строки



Пример работы командной строки

**Вывод:** в ходе практической работы я научился работать с Брандмауэром Windows

**Практическая работа №5**

**Криптографическая защита информации**

Цель: овладение основными криптографическими алгоритмами симметричного шифрования

**Задание 2**

Пирейко Дмитрий Михайлович

**Шифр Цезаря:** Ибйсвдз Уёблйбв Ёбоювезгбф (**ключ**: 2; **ключевое слово: «**Грусть**»**)

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:

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

**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: Чжшорсцнфжйшжрфжэдрулжя

**Шифр Плейфера:**

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 |

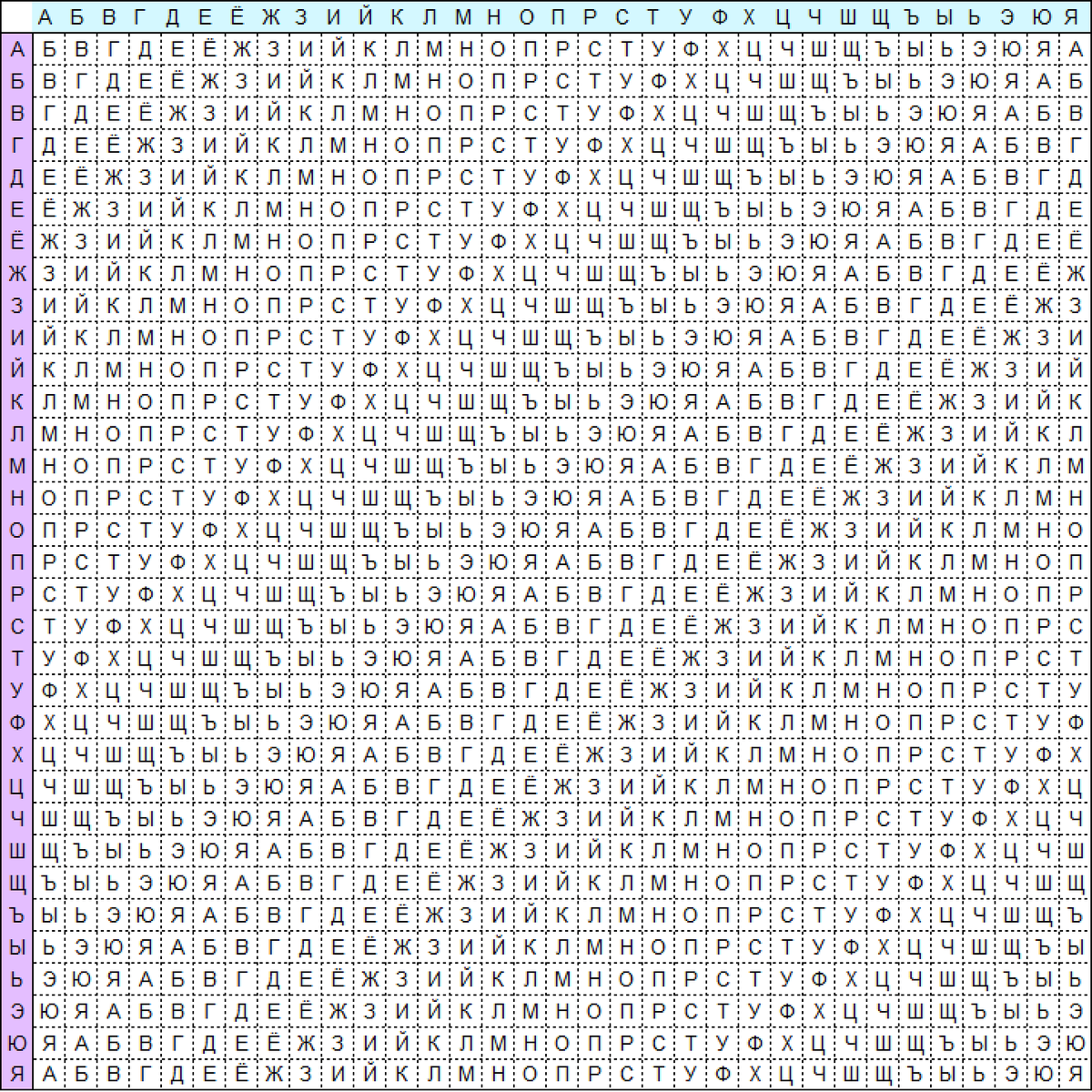
Пи ре йк од ми тр ий ми ха йл ов ич

Итог: Сапжднукнщвогннщфщенртзы

**Шифр Вижинера:**

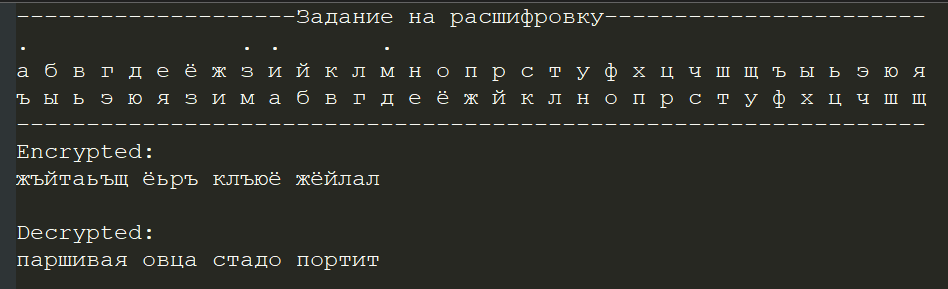
Пирейкодмитриймихайлович

Ключевое слово: защитазащитазащитазащита



**Итог**: Шйкоэлчежтёсскжтибтмильш

# **Задание 3**



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

**Практическая работа №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.

**Практическая работа №7**

**Криптографическая защита информации**

*I ЭТАП (генерация RSA-ключа)*

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.

*II ЭТАП (отправка сообщения вместе с RSA-ключом)*



*III ЭТАП (получение сообщения и проверка электронной подписи)*



***Контрольные вопросы***

*Дайте определение понятию "электронная цифровая подпись".*

Электронная цифровая подпись – 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.

*Объясните какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП.*

Порядок использования ключей обратный тому, который используется при передаче секретных сообщений. В начале отправитель использует свой закрытый ключ, а затем получатель применяет открытый ключ отправителя.

*Перечислите специальные схемы ЭЦП.*

Кроме классической схемы ЭЦП различают еще несколько специальных:

* 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.

***Вывод*:** в ходе практической работы я изучил и закрепил умение реализации ЭЦП на примере RSA.

**Практическое занятие №8**

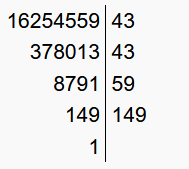
**Тема «Криптографическая защита информации»**

Цель: получение основных сведений из курса теории чисел

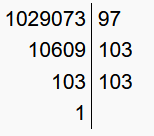
Вариант 9

1.Найти канонические разложения чисел а и b.

а = 16254559, b = 1029073



43\*43\*59\*149 = 16254559



97\*103\*103 = 1029073

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

а) Нужно отсортировать числа в порядке возрастания:**(**162545591029073**)**

Возьмем наименьшее число **(**1029073**)** как делитель

Выполним вычисления для операции по модулю оставшегося числа и делителя:

16254559mod 1029073= 818464

Получаем все остатки и делитель и сортируем их в порядке возрастания. Также удаляем все повторяющиеся номера. Тогда наш набор чисел: 818464 1029073

Имеется наименьший делитель из оставшихся чисел: 1. Следовательно, НОД(16254559; 1029073) является:**1**

б) Разложим числа на простые множители и подчеркнем общие множители чисел:

43\*43\*59\*149 = 16254559

97\*103\*103 = 1029073

Общие множители чисел: 1

НОД(16254559; 1029073) = 1

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

*au* + *bv =* 16254559*\* u +* 1029073*\* v =* НОД(16254559; 1029073) = 1

*u* = 240097 *v* = -3792414

16254559*\** (240097) *+* 1029073 *\* (*-3792414)*=* НОД(16254559; 1029073) = 1

6. Найти остаток от деления  на 19.

2006 делится на 19 с остатком **11**. 20062 делится на 19 с остатком **7**. 20063 делится на 19 с остатком **1**. 20064 делится на 19 с остатком **11.** Получили один из предыдущих остатков, значит «зациклились». Число 20065 дает тот же остаток деления на 19, что и 2006. Значит, длина цикла равна 3. Число 20061998 дает тот же остаток от деления на 19, что и 20063, то есть 1.

**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.