Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Электронная тетрадь по дисциплине

«Основы Защиты Информации»

Студент: Цвирко А.О.

ФИТ 2 курс 2 группа

Преподаватель: Берников В.О.

Минск 2020

Практическое занятие №1

Тема «Концепция национальной безопасности Республики Беларусь»

Цель: изучить концепцию национальной безопасности Республики Беларусь.

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

Информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств. Усиливается роль и влияние средств массовой информации и глобальных коммуникационных механизмов на экономическую, политическую и социальную ситуацию. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Происходит эволюция информационного противоборства как новой самостоятельной стратегической формы глобальной конкуренции. Распространяется практика целенаправленного информационного давления, наносящего существенный ущерб национальным интересам.

**Информационная безопасность** – такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Обмен информацией между людьми характеризуется интенсивным внедрением современных инфокоммуникационных технологий, широким распространением локальных корпоративных и глобальных сетей во всех сферах жизни государства, создает новые возможности и качества информационного обмена. В связи с этим **проблемы информационной безопасности** приобретают первостепенное значение актуальность и важность которых обусловлена следующими факторами:

* высокие темпы роста парка персональных компьютеров и резкое расширение круга пользователей;
* увеличение объемов информации;
* бурное развитие аппаратно-программных средств и технологий, не соответствующих современным требованиям безопасности;
* несоответствие темпов роста стандартам и правовым нормам, обеспечивающим необходимый уровень защиты информации (ЗИ);
* повсеместное распространение сетевых технологий, создание единого ИК пространства на базе сети Интернет.

Проблема защиты от информации существенно сложнее проблемы защиты информации в силу многообразности информационных угроз, воздействие которых не всегда очевидно. Предотвращение и нейтрализация таковых требуют как технических решений, так и организационно-правовых и политических на внутригосударственном, межгосударственном и международном уровнях.

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.

**Основные угрозы национальной безопасности, связанные с ИТ-сферой:**

Сохраняется отставание от ведущих стран мира по уровню информатизации. В условиях открытости информационного пространства страны и конкуренции со стороны иностранного информационного продукта недостаточными остаются качество и популярность белорусского национального контента.

* деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;
* нарушение функционирования критически важных объектов информатизации;
* недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;
* снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента.

**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.

В информационной сфере с целью нейтрализации **внутренних источников угроз национальной безопасности** совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

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.

**Вывод:** я изучил концепцию национальной безопасности Республики Беларусь. Я считаю, что информационная безопасность является важным аспектом государственной безопасности в целом. 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.

**Практическое занятие №2**

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

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

**Теоретическое введение**

Все методы защиты информации по характеру проводимых действий можно разделить на:

* законодательные (правовые);
* организационные;
* технические;
* комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации. К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты. Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т.е. комплексно.

Принципиальным вопросом при определении уровня защищенности объекта является выбор критериев. Рассмотрим один из них ‑ широко известный критерий "эффективность - стоимость".

Пусть имеется информационный объект, который при нормальном (идеальном) функционировании создает положительный эффект (экономический, политический, технический и т.д.). Этот эффект обозначим через *Е0*. Несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования (нарушается нормальная работа, наносится ущерб из-за утечки информации и т.д.) на величину *ΔЕ*. Тогда эффективность функционирования объекта с учетом воздействия несанкционированного доступа:

|  |  |
| --- | --- |
|  | (2.1) |

Относительная эффективность:

|  |  |
| --- | --- |
| , | (2.2) |

Уменьшение эффективности функционирования объекта приводит к материальному ущербу для владельца объекта. В общем случае материальный ущерб есть некоторая неубывающая функция от ΔЕ:

|  |  |
| --- | --- |
| , | (2.3) |

Будем считать, что установка на объект средств защиты информации уменьшает негативное действие несанкционированного доступа на эффективность функционирования объекта. Обозначим снижение эффективности функционирования объекта при наличии средств защиты через ΔЕ3, а коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объект ‑ через К, тогда:

|  |  |
| --- | --- |
|  | (2.4) |

где К≥1.

Выражения (2) – (1) примут вид:

|  |  |
| --- | --- |
|  | (2.5) |

|  |  |
| --- | --- |
| , | (2.6) |

Стоимость средств защиты зависит от их эффективности, и в общем случае К – есть возрастающая функция от стоимости средств защиты (С):

|  |  |
| --- | --- |
| , | (2.7) |

Поскольку затраты на установку средств защиты можно рассматривать как ущерб владельцу объекта от возможности осуществления несанкционированного доступа, то суммарный ущерб объекту:

|  |  |
| --- | --- |
| , | (2.8) |

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

|  |  |
| --- | --- |
| , | (2.9) |

Таким образом, классическая постановка задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа имеет вид:

|  |  |
| --- | --- |
|  | (2.10) |

или

|  |  |
| --- | --- |
| , | (2.11) |

Несмотря на кажущуюся простоту классической постановки задачи, на практике воспользоваться приведенными результатами удается редко. Это объясняется отсутствием зависимостей K = f(C) и особенно ущерба от несанкционированного доступа. И если зависимость коэффициента защищенности от стоимости средств защиты можно получить, имея технические и стоимостные характеристики доступных средств защиты, то оценить реальный ущерб от несанкционированного доступа чрезвычайно трудно, так как этот ущерб зависит от множества трудно прогнозируемых факторов: наличия физических каналов несанкционированного доступа, квалификации злоумышленников, их интереса к объекту, последствий несанкционированного доступа и т.д.

Вместе с тем для объектов, на которые возлагаются ответственные задачи и для которых несанкционированный доступ влечет катастрофические потери эффективности их функционирования, влиянием стоимости средств защиты на эффективность можно пренебречь, т.е. если:

|  |  |
| --- | --- |
|  | (2.12) |

то:

|  |  |
| --- | --- |
| , | (2.13) |

В этом случае (2.11) и (2.12) принимают вид:

|  |  |
| --- | --- |
|  | (2.14) |

или:

|  |  |
| --- | --- |
| , | (2.15) |

где Cдоп — допустимые расходы на защиту.

**Задание на выполнение**

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

Таблица 2.1 - Исходные данные к решению задачи

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E0, бел. р*. | *E, бел. р.* | *K* | *C, бел. р.* |
| 3 | 20000 | 18000 | 10 | 1000 |

Е0 – положительный эффект, создаваемый некоторым информационным объектом при его нормальном (идеальном) функционировании.

Несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования на величину Е.

С - Стоимость средств защиты.

Эффективность функционирования объекта с учетом воздействия несанкционированного доступа:

* (руб).*

Относительная эффективность:



Снижение эффективности функционирования объекта при наличии средств защиты Коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объект – К. Высчитывается по формуле (2.4):

* (руб).*

Выражения (2.6) – (2.1) примут вид:

* (руб).*



Если эффективность функционирования объекта имеет стоимостное выражение (доход, прибыль и т.д.), то U (суммарный ущерб объекту из-за затрат на установку средств защиты) непосредственно изменяет эффективность по формуле (2.9):



**Вывод:**

При решении поставленной задачи было вычислено, что коэффициент = 0,9. Так как коэффициент стремится к максимуму, то можно утверждать, что все вычисления произведены правильно.

**Практическое занятие №3**

**Тема «Разработка политики информационной торговой сети»**

Цель: разработать проект политики информационной безопасности торговой сети.

**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 (3.1) представлена организационная структура завода по производству шин:

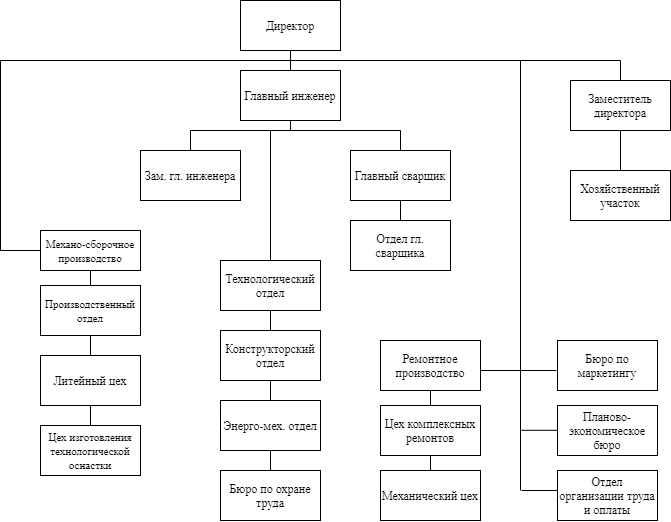


Рис.3.1 – Организационная структура завода по производству шин

В зависимости от масштабов фирмы структура ее может отличаться. Например, часть обслуживающего персонала, такая как системные администраторы, могут быть выделены в отдельный IT-отдел.

**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.

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 завода по производству шин 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 для бизнеса?
* Насколько уязвим бизнес 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 торговой сети. Как уже было сказано, благодаря специфике работы торговой сети, атаки являются довольно редкими, так как даже при условии успешности, прибыль довольно мала. Однако вероятность угрозы все равно присутствует и руководству магазинов торговой сети, как и руководству компании в целом, 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 торговую сеть являются следующие:

* ограбление магазина торговой сети. При данном типе атаки, злоумышленники могут довольствоваться лишь выручкой магазина и товаром, который в нем находится. Связи с финансовой системой у магазинов нет. Однако данный тип атаки является наиболее опасным для жизни как персонала, так и посетителей;
* получение несанкционированного доступа к веб-сайту торговой сети. 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 головной офис компании. 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 компании. 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;
* физическое воздействие на магазины компании (например, поджог).

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

**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).

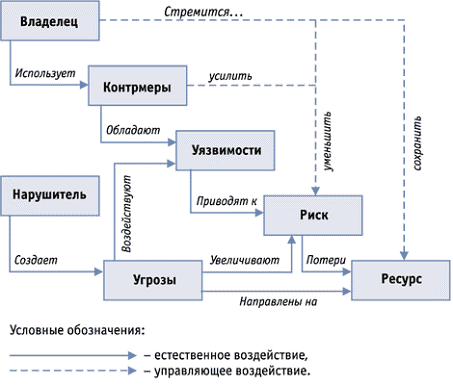


Рис.3.2.–Модель построения корпоративной системы защиты информации

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

* вооруженная охрана магазинов торговой сети и офисов компании;
* четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь каждого магазина 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 компании (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 финансовым отделам. Уборщица не должна знать номер банковского счета фирмы и тем более, его пароля;
* 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. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.

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

* вооруженная охрана магазинов торговой сети и офисов компании;
* четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь каждого магазина 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 компании (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 финансовым отделам. Уборщица не должна знать номер банковского счета фирмы и тем более, его пароля;
* 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. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.

**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 торговой сети 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

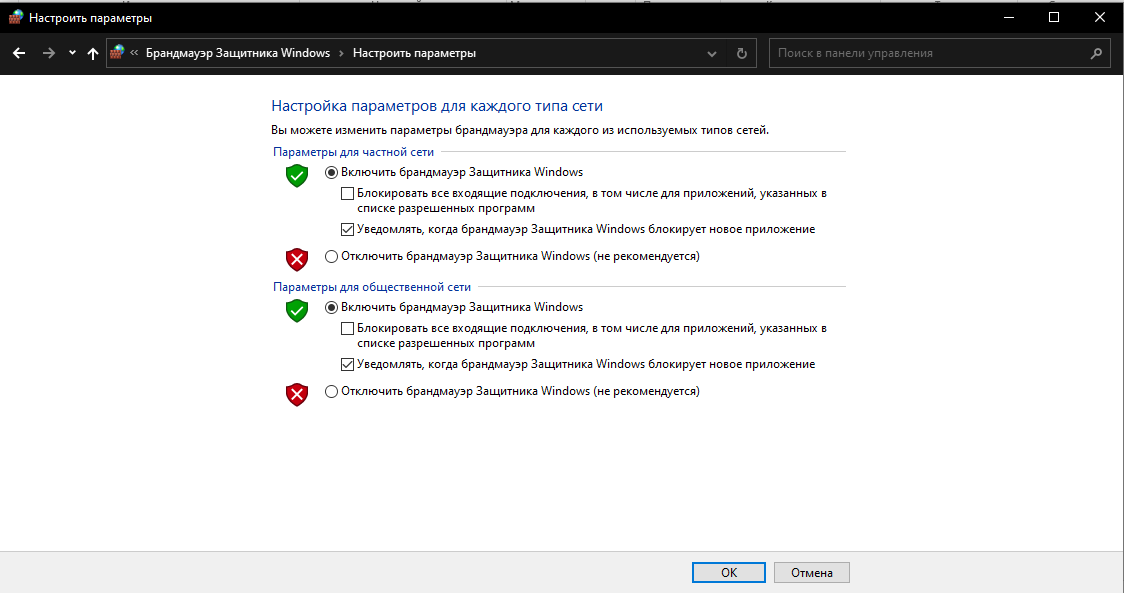
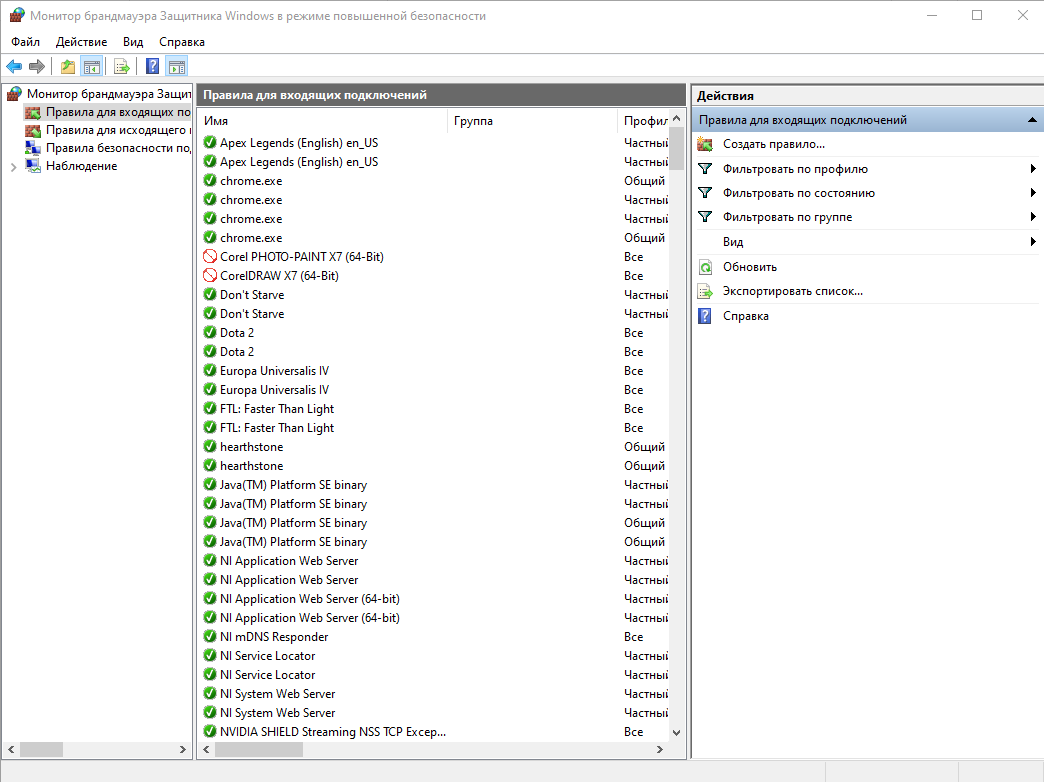


Рисунок 4.1 – Включение брандмауэра

2. Настройка входящих и исходящих подключений 

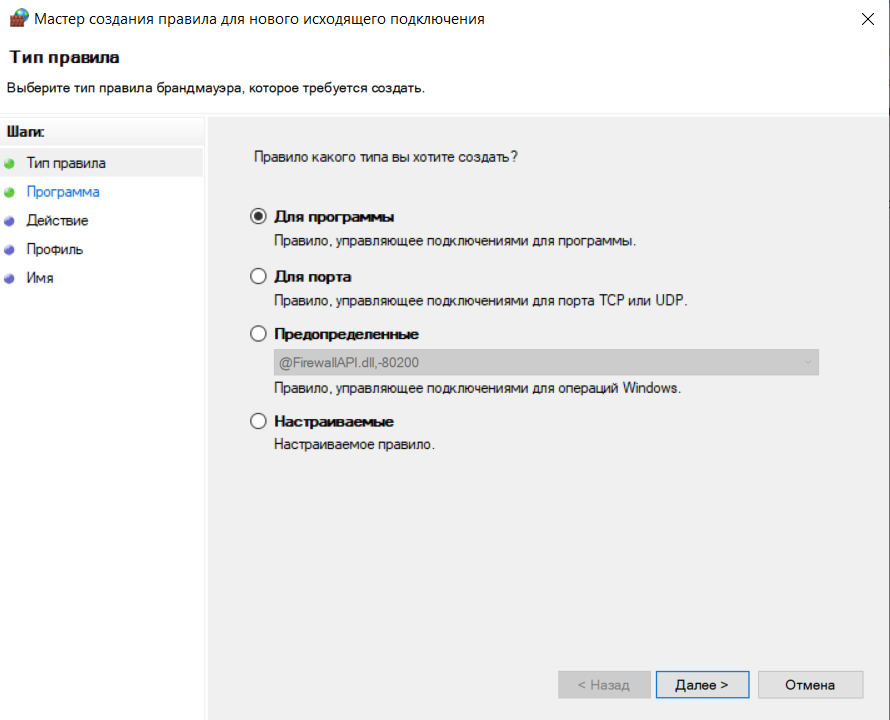
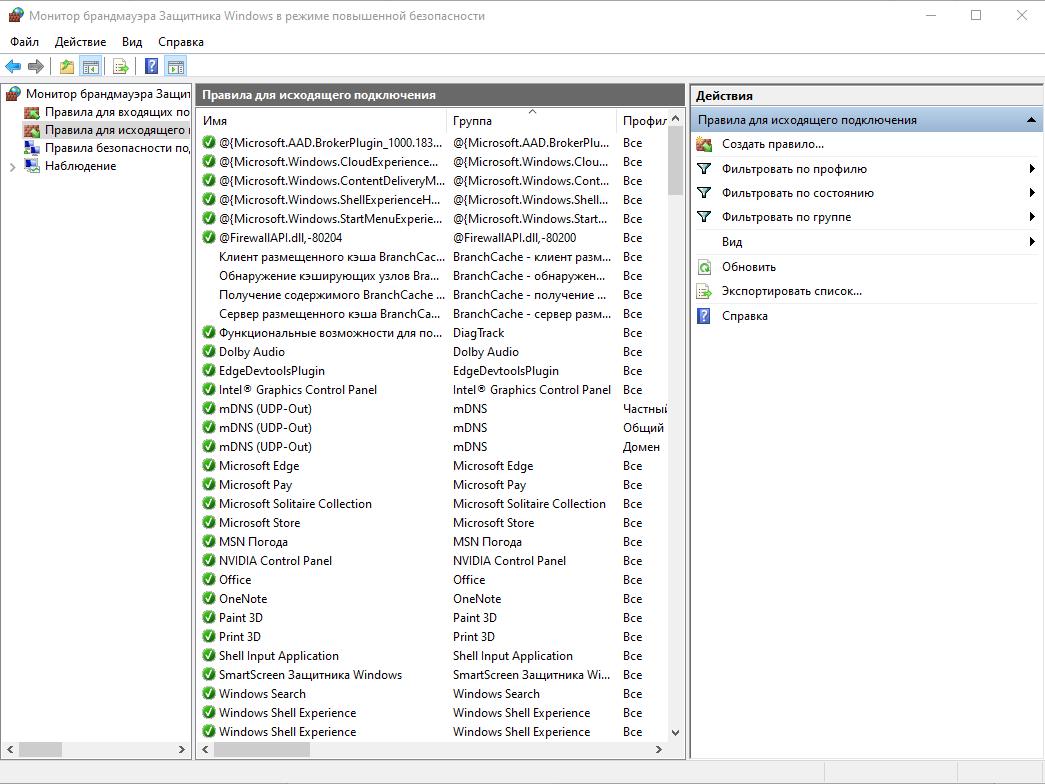
Рисунок 4.2 – Правила для входящих подключений  Рисунок 4.3 – Правила для исходящих подключений

Рисунок 4.4 - Мастер создания правил

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

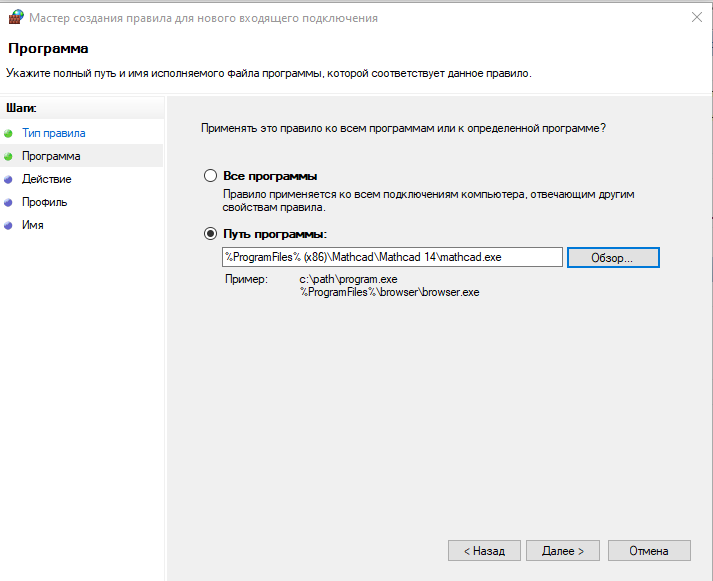


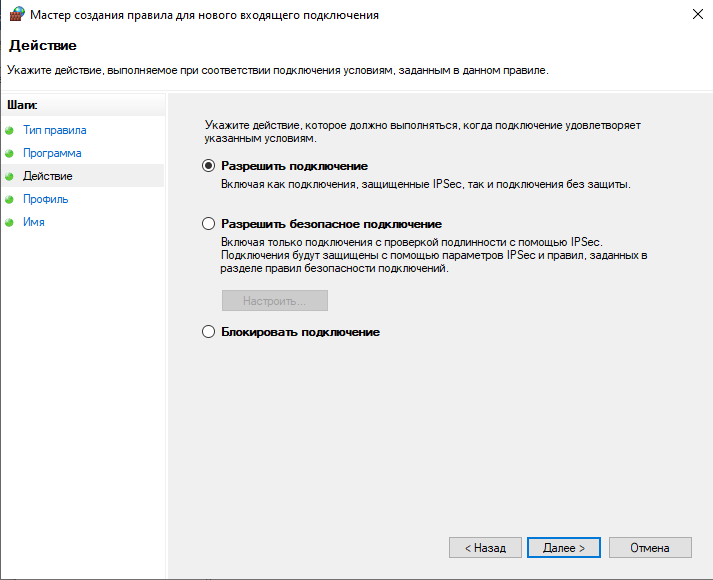
Рисунок 4.5 - Мастер создания правил, выбор пути

Рисунок 4.6 - Блокировка/разрешение подключения

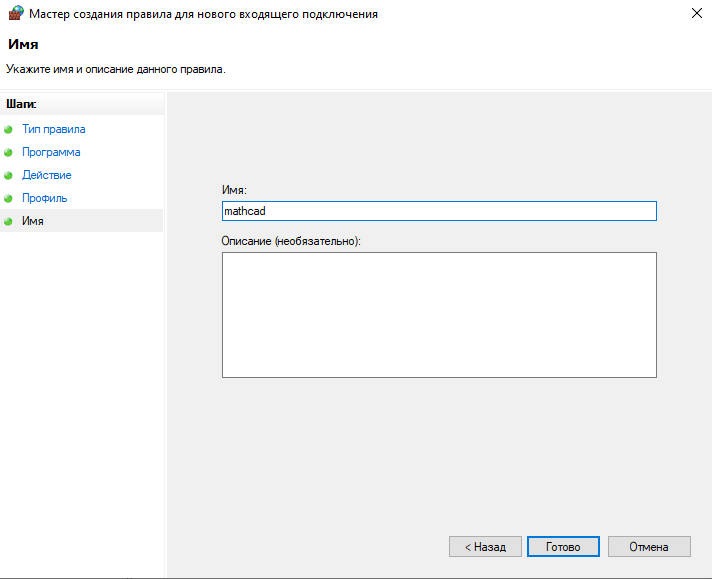


Рисунок 4.7 - Выбор имени

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

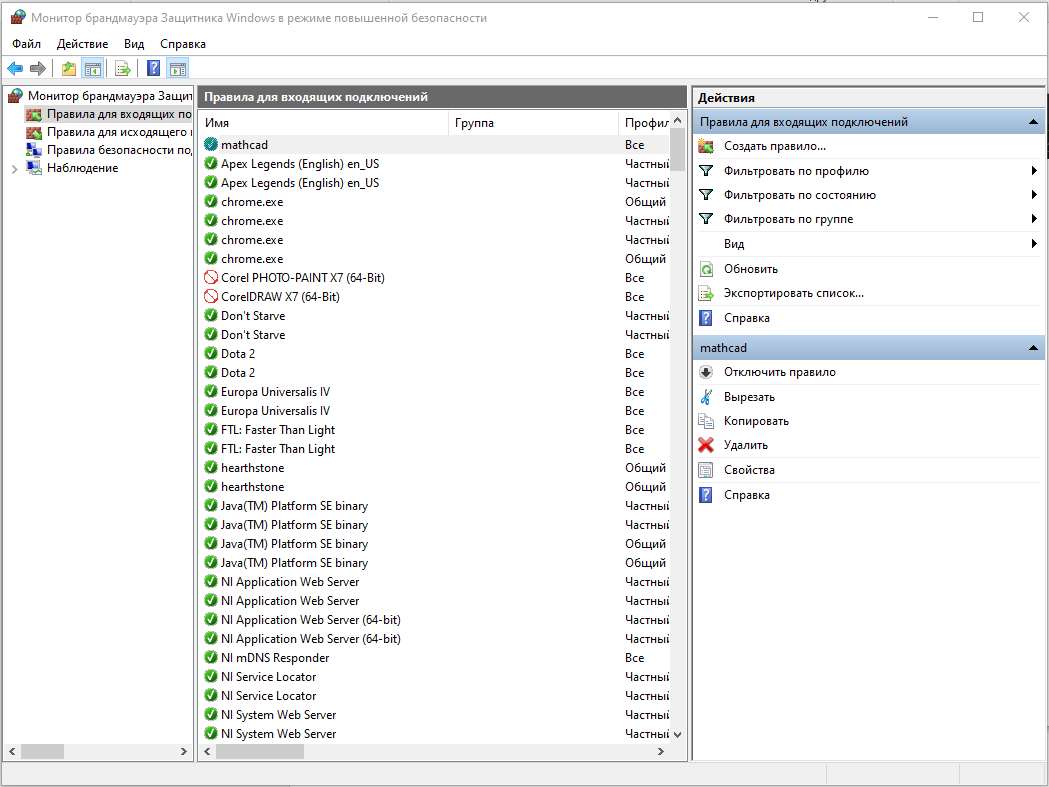


Рисунок 4.8 - Активные правила в списке

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

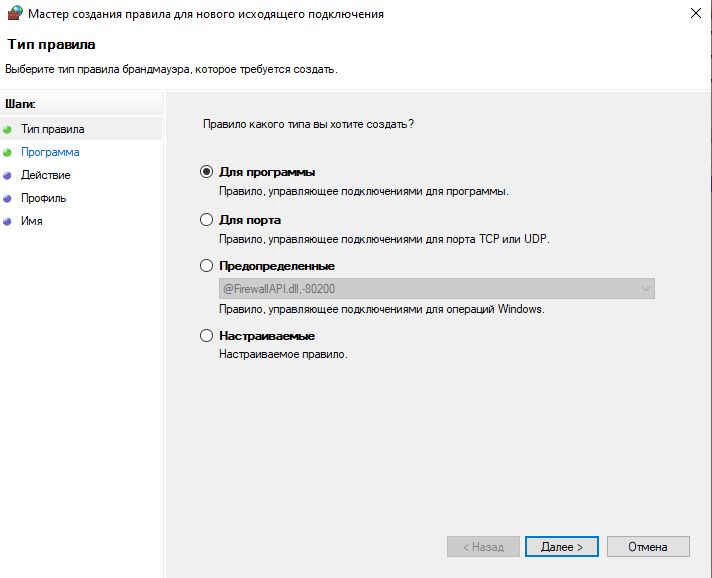


Рисунок 4.9 - Мастер создания правил

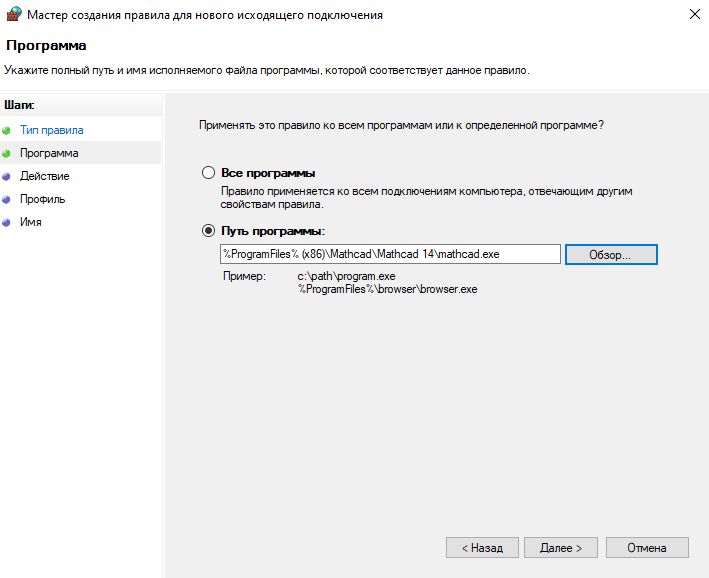


Рисунок 4.10 - Мастер создания правил, выбор пути

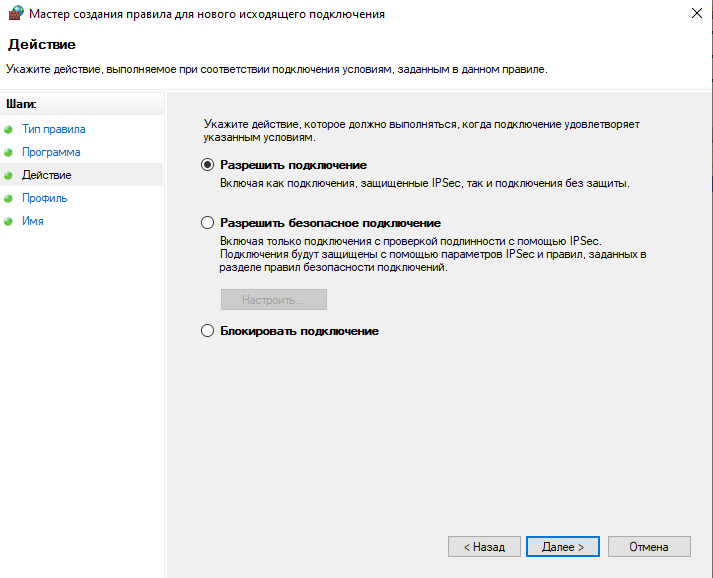


Рисунок 4.11 - Блокировка/разрешение подключения

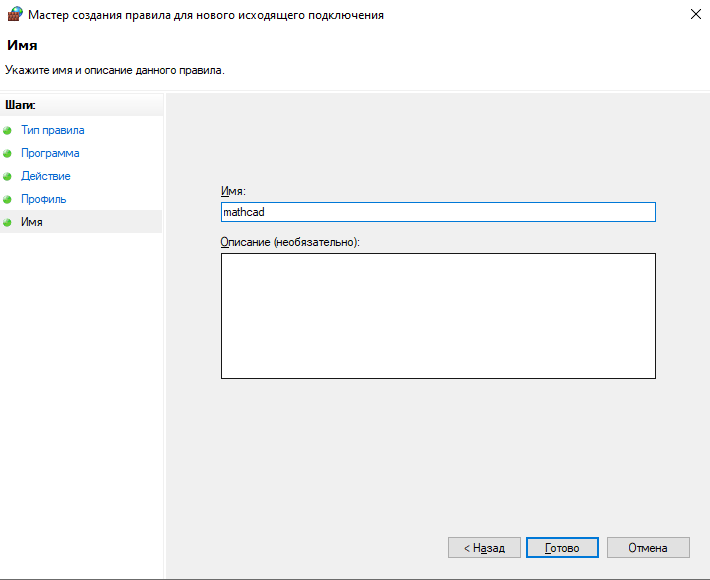


Рисунок 4.12 - Выбор имени

6. Опробовать действие нескольких команд:

1. Служба диагностики DirectX – dxdiag

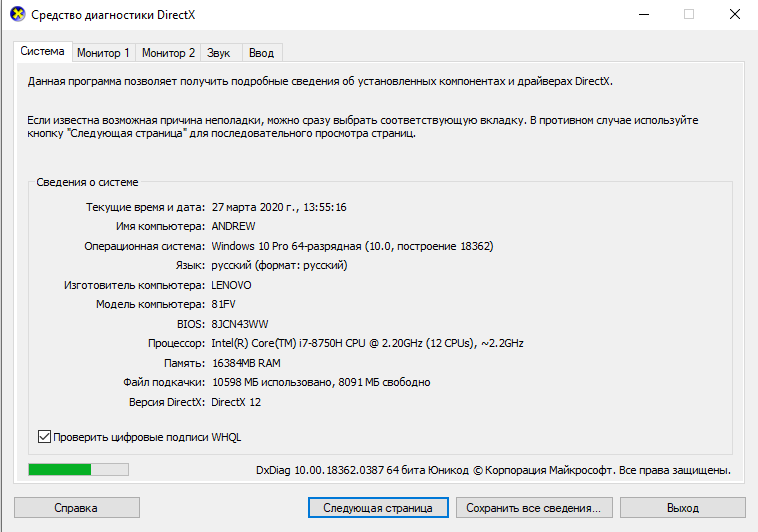


Рисунок 4.13 – Служба диагностики DirectX

2. Калькулятор – calc.

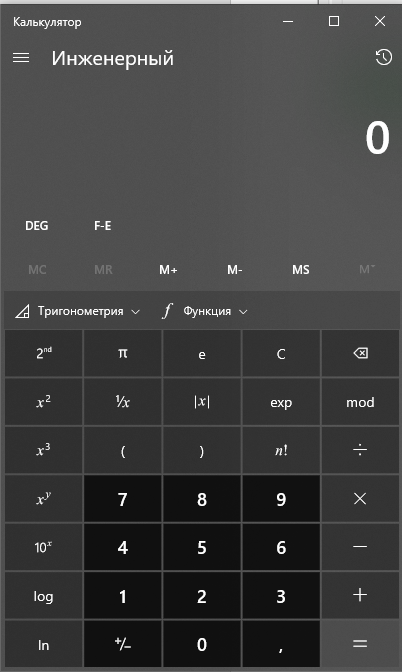


Рисунок 4.14 - Калькулятор

3. Производительность - perfmon.msc

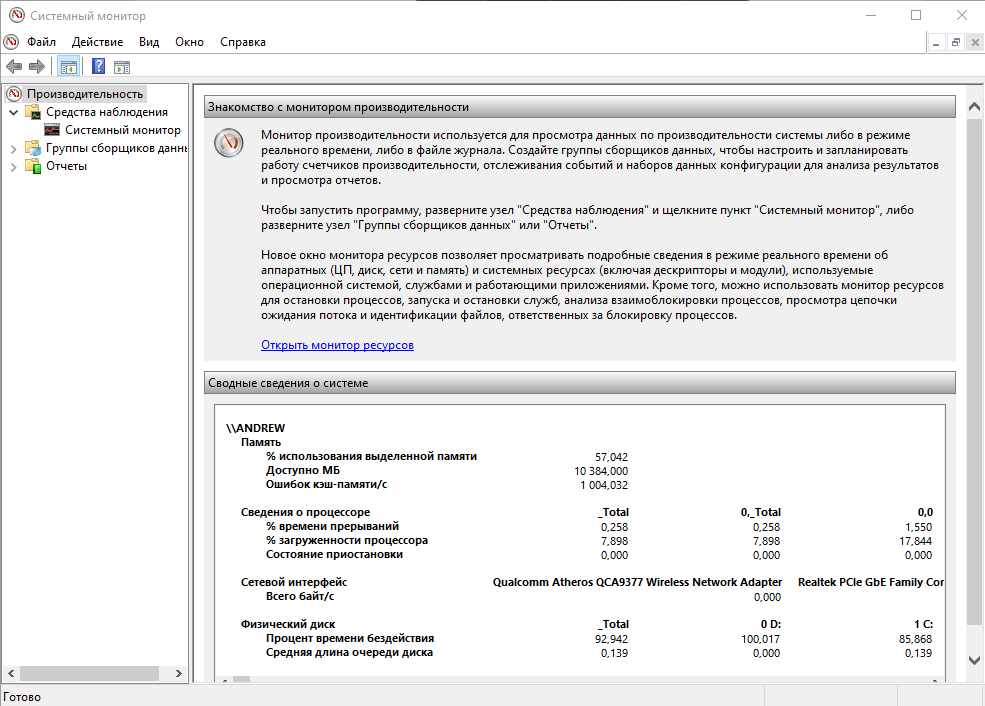


Рисунок 4.7 – Монитор производительности

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

**Практическое занятие №5**

**Тема «**Настройка антивирусов**»**

**Цель работы:** Овладение навыками настройки и использования различных антивирусов.

**Теоретическое введение**

При заражении компьютера вредоносными программами важно их обнаружить. Для этого следует знать об основных признаках проявления вредоносных программ. К ним можно отнести следующие:

* прекращение работы или неправильная работа ранее успешно функционировавших программ;
* медленная работа компьютера;
* невозможность загрузки операционной системы;
* исчезновение файлов и каталогов или искажение их содержимого;
* изменение даты и времени модификации файлов;
* изменение размеров файлов;
* неожиданное значительное увеличение количества файлов на диске;
* существенное уменьшение размера свободной оперативной памяти;
* вывод на экран непредусмотренных сообщений или изображений;
* подача непредусмотренных звуковых сигналов;
* частые зависания и сбои в работе компьютера.

**Режимы работы файервола ESET NOD32 Internet Security и взаимодействие с пользователем**

Персональный файервол – это устройство, выполняющее функции драйвера сетевого трафика и управляющее взаимодействием в рамках локальной сети или Интернета. При помощи заранее определенных правил файервол анализирует это взаимодействие и принимает решение о его разрешении или запрете. Самая основная функция файервола – защита частных сетей или компьютеров от вторжения со стороны потенциально опасных внешних сетей и компьютеров.

Доступны 5 отдельных режимов работы файервола, выбор которых зависит от требуемого уровня ограничений. Чтобы изменить поведение файервола, необходимо выбрать нужный режим фильтрации.

Самая основная функция файервола – защита частных сетей или компьютеров от вторжения со стороны потенциально опасных внешних сетей и компьютеров.

**Автоматический режим**

В автоматическом режиме сетевое взаимодействие автоматически контролируется параметрами, определенными пользователем. После подключения к сети пользователь решает, следует ли считать ее доверенной зоной. Взаимодействие в доверенной зоне не ограничивается в обоих направлениях. Взаимодействие в зоне ограничений: взаимодействие с Интернетом – разрешается только приложениям, устанавливающим исходящие подключения. Такие приложения считаются доверенными и для входящих подключений. Данный режим не требует участия пользователя (за исключением момента подключения к новой сети).

В общем, автоматический режим не использует заранее определенные правила, но при этом автоматически анализирует взаимодействие. Приложениям разрешается устанавливать исходящие подключения. Приложения, уже установившие исходящие подключения, считаются доверенными и для установки входящих подключений.

**Интерактивный режим**

В интерактивном режиме сетевое взаимодействие анализируется в соответствии с заранее определенными правилами. Если для подключения нет доступных правил, пользователю при помощи диалогового окна предлагается разрешить или запретить подключение. Через некоторое время пользователем будет создана группа правил, соответствующая его потребностям. Будьте осторожны, устанавливая этот режим в корпоративной среде, поскольку со временем некоторые пользователи могут начать игнорировать регулярно появляющиеся диалоговые окна и просто разрешать все, что предлагает им программа.

**Режим на основе политик**

В режиме на основе политик сетевое взаимодействие анализируется в соответствии с правилами, определенными администратором. Если доступных правил нет, подключение автоматически блокируется без уведомления пользователя. Данный режим рекомендуется выбирать только администраторам, желающим контролировать сетевое взаимодействие и знающим, каким приложениям следует его разрешить или запретить.

**Автоматический режим с исключениями**

Данный режим позволяет настроить вручную правила. В этом случае, если будет запрос на соединение извне, файервол сначала проверит правила, которые прописал пользователь, и если найдет соответствующее, то оно будет задействовано. Если правила не будет, тогда соединение будет разорвано. Во всех остальных случаях этот режим полностью соответствует автоматическому режиму.

**Режим обучения**

Автоматическое создание и сохранение правил, предназначен для первоначальной настройки персонального брандмауэра. Участие пользователя не требуется, потому что **ESET Internet Security** сохраняет правила согласно предварительно настроенным параметрам. Режим обучения является небезопасным, поэтому рекомендуется использовать его только до момента создания правил для всех необходимых соединений.

**Задание к выполнению**

* + - 1. Настройка режима фильтрации файервола антивируса.

Открыть программу ESET Internet Security, щелкнув по значку программы в области уведомлений Windows.

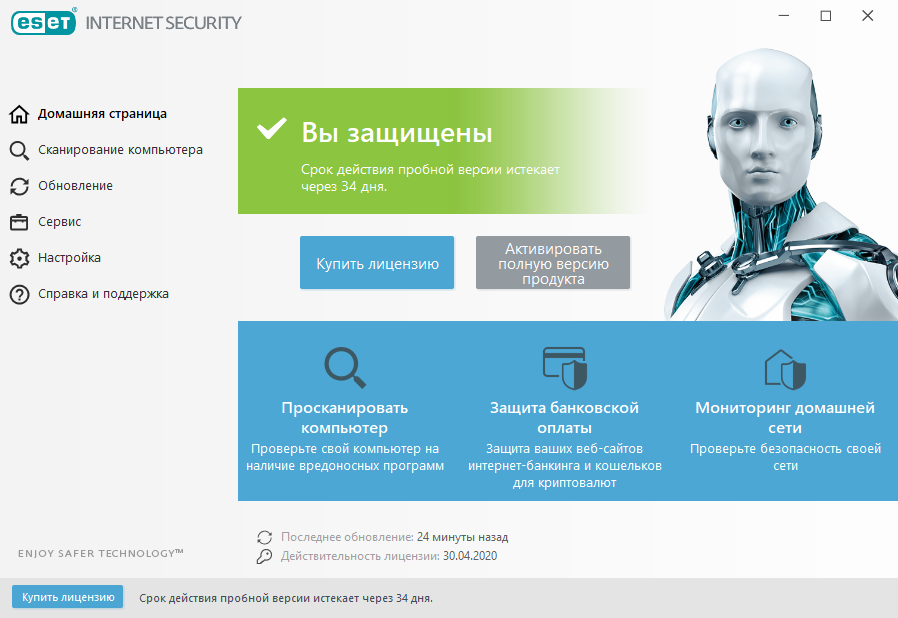


Рисунок 5.1 – ESET Internet Security.

C помощью клавиши F5 заходим в расширенные параметры антивируса и выбираем пункт меню «Защита сети - Файервол» (рис. 5.2). Затем в разделе режим фильтрации выбираем нужный режим. (рис. 5.3).

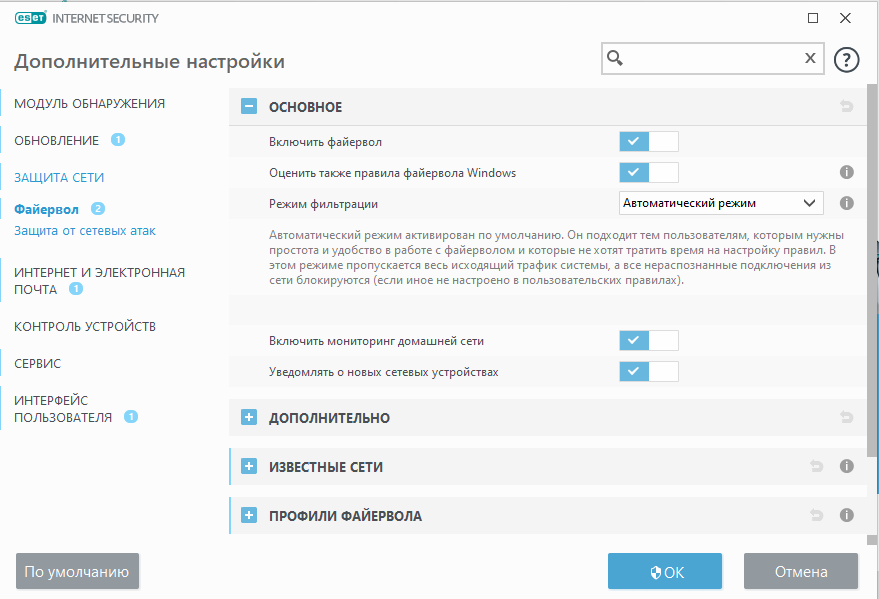


Рисунок 5.2 – пункт меню «Защита сети - Файервол».

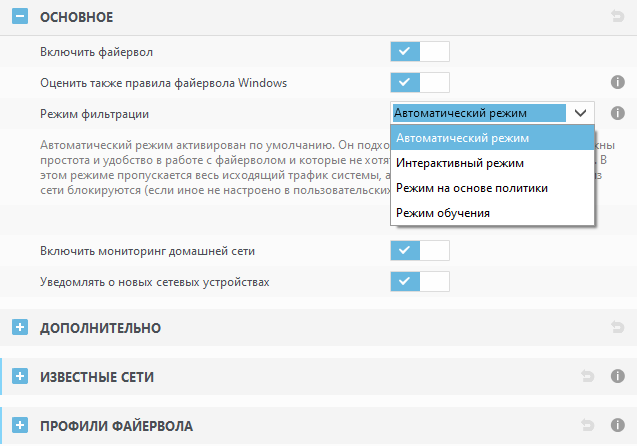


Рисунок 5.3 – Режимы фильтрации

Существуют следующие режимы фильтрации файервола антивируса:

* автоматический режим;
* интерактивный режим;
* режим на основе политик;
* автоматический режим с исключениями;
* режим обучения.
  + - 1. Настройка Оффлайн обновления сигнатур угроз из локальной папки.

В дополнительных настройках (при нажатии клавиши F5) необходимо выбрать пункт «Обновление». В строке «Сервер обновлений» выбрать «Изменить» и вставить путь к файлам сигнатур.

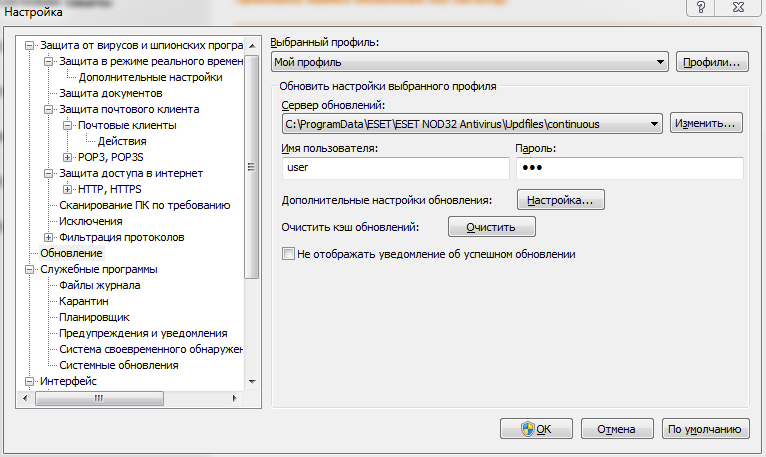


Рисунок 5.4 – Оффлайн обновление.

Для обновления компьютеров по локальной сети или отдельно стоящих компьютеров был реализован процесс ретрансляции антивирусных баз и программных модулей в локальный источник (папку на диске, сетевой ресурс). Для организации обновления антивирусных баз из локальной папки необходим как минимум один компьютер, имеющий доступ к сети Интернет.

Если у вас в локальной сети установлено несколько копий антивируса, то обновление для каждой копии можно настроить из локальной папки с помощью ретрансляции (приема и передачи) баз в эту папку.

* + - 1. Настройка Оффлайн обновления сигнатур угроз с локального сервера по HTTP

Вы можете настроить ваши клиенты для загрузки обновления сигнатур вирусов напрямую с серверов компании ESET через интернет. Вы можете выбрать этот метод, если ваш локальный сервер является ненадежным или работает не постоянно. Таким образом, ваши клиенты будут иметь возможность производить обновления, если ваш сервер не работоспособен. Кроме того, ваши клиенты получат обновления моментально после их выхода на серверах ESET, а не будут дожидаться планового обновления на вашем сервере.

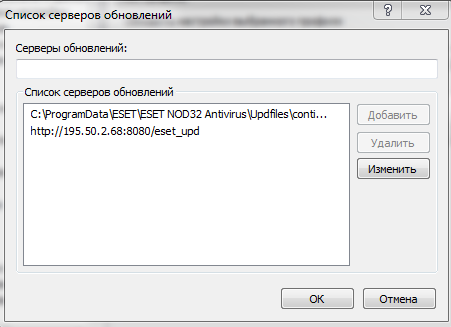


Рисунок 5.5 – Задание сервера для обновлений

Файлы обновлений можно увидеть по введенному адресу и данным пользователя через проводник.

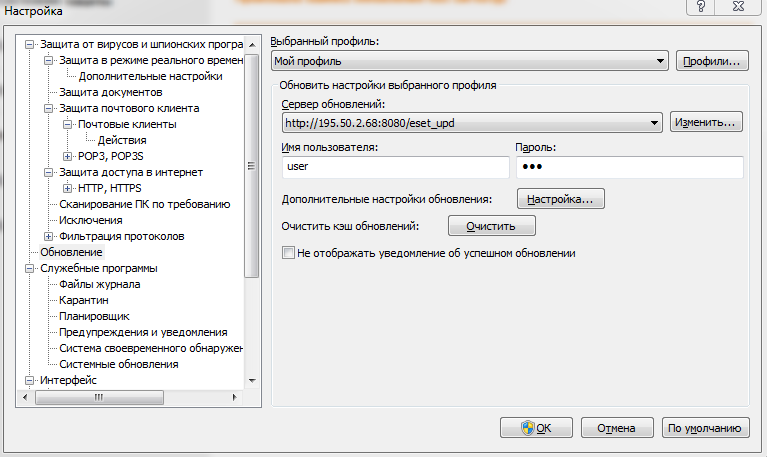


Рисунок 5.6 – Оффлайн обновление с сервера.

**Вывод**

Антивирус способен в большинстве случаев удалить вредоносный программный объект не только из программного файла, но и из файла офисного документа, не нарушив его целостность. В некоторых случаях антивирус может удалить тело вредоносного объекта из зараженного файла, восстановив файл.

Использование антивирусных программ не требует высокой квалификации и доступно практически любому пользователю компьютера.

# Практическое занятие №6

**Изучение принципов работы с компьютерными программами для криптографической защиты информации при передаче и хранении**

Цель: Овладение навыками работы с компьютерными программами для криптографической защиты информации при передаче и хранении.

**Порядок работы с программой TrueCrypt**

**Этап 1:** Установить и запустить

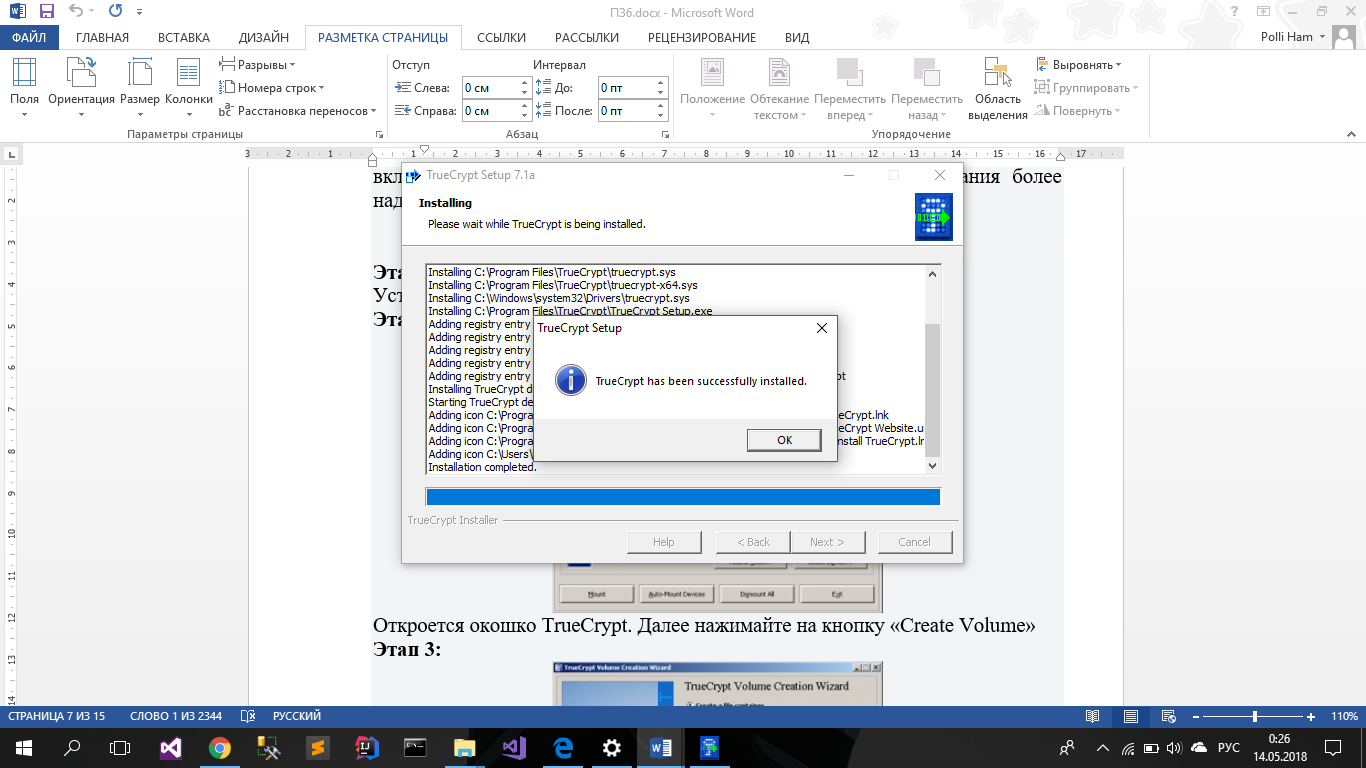


Рисунок 6.1 – Установка TrueCrypt

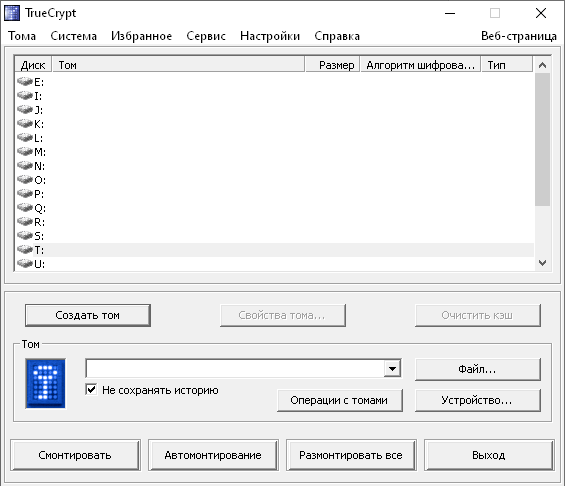
**Этап 2:** Откроется окно TrueCrypt. Далее нажмите на кнопку «Создать том»

Рисунок 6.2 – Окно TrueCrypt

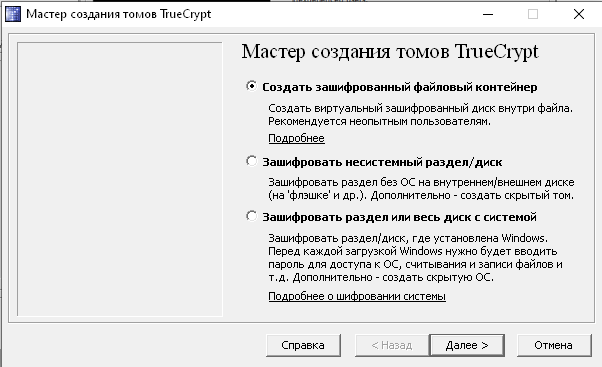
**Этап 3:** На экране появится окошко для создания TrueCrypt раздела. На этом этапе вы выбираете место для создания раздела. Он может находится непосредственно в файле, пользователи называют его контейнером, в разделе диска (партиции) либо внутри дискового устройства. Приступаем к созданию раздела TrueCrypt в файле. Данное изображение имеет установку по умолчанию, поэтому жмем «Далее».

Рисунок 6.3 – Создание раздела TrueCrypt

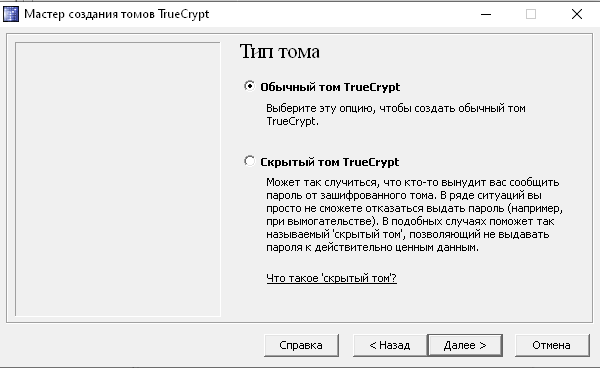
**Этап 4:** Необходимо определится, какой раздел вы создадите: скрытый или обычный. Руководство покажет создания обычного раздела. Поэтому нажимаем «Далее».

Рисунок 6.4 – Создание раздела TrueCrypt

**Этап 5:** Этап предполагает указание места расположения раздела TrueCrypt. При этом поведение контейнера идентичное с поведением самого обыкновенного файла.

Жмем Выбрать файл Открывается окошко для выбора файла.

**Этап 6:** Создаём раздел TrueCrypt, который будет располагаться в папке G:\ИНСТИТУТ\лабы\2 курс\ОЗИ\123, а файл будет иметь название 12345. «lab6» не будет пока TrueCrypt его не создаст. TrueCrypt не может зашифровать существующие документы, если попробовать это сделать, то просто на просто потеряете свои данные. Шифровать файлы можно будет немного позже, путем размещения их на шифрованном разделе TrueCrypt.

Выбираем место в окне для выбора, где будущий контейнер будет располагаться. Вводим любое имя и жмем «Save». После этого окошко должно исчезнуть

**Этап 7:** После выбора места жмем «Далее».

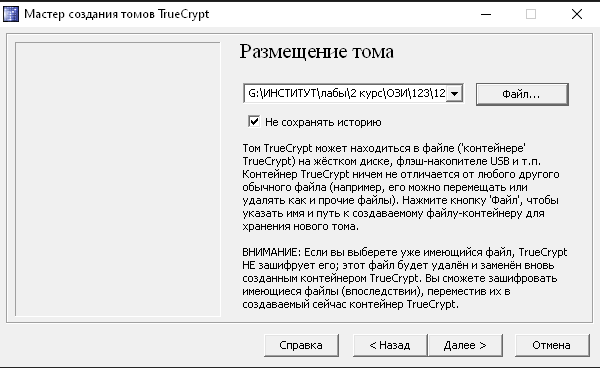


Рисунок 6.5– Выбор места

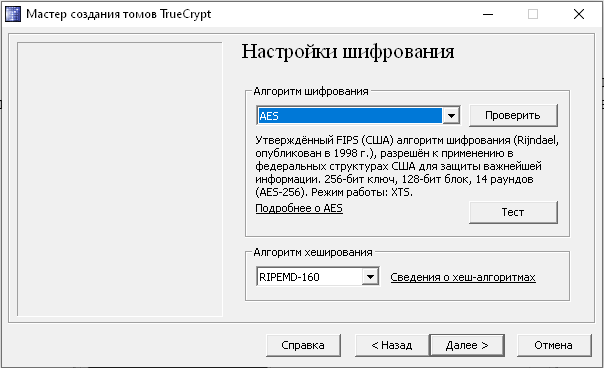
**Этап 8:** В данном разделе предлагается сделать выбор алгоритма для шифрования, а так же хеш – алгоритма предназначенного для раздела. Оставляем всё как есть и жмем  «Далее».

Рисунок 6.6– Выбор алгоритмов

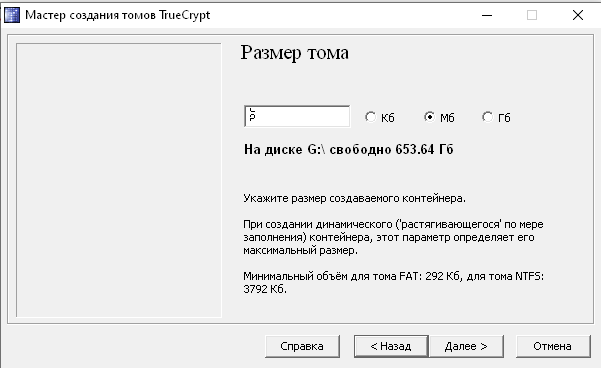
**Этап 9:** Далее в окне указываем предполагаемый размер контейнера TrueCrypt в 5 мегабайт, затем нажимаем «Далее».

Рисунок 6.7 – Выбор размера

**Этап 10:** Далее выбираем пароль для нашего раздела и нажимаем «Далее»

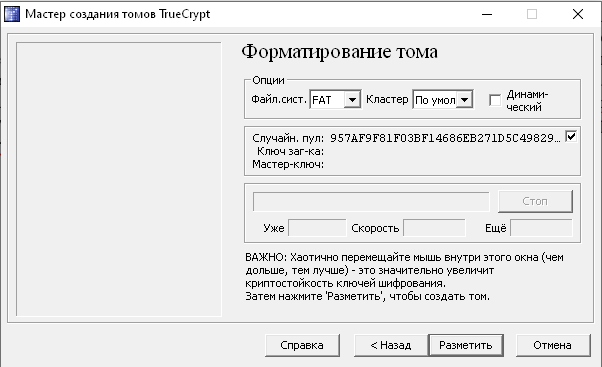
**Этап 11:** В открывшемся окне следует двигать мышкой в случайном порядке не менее 30 секунд. Чем дольше будет продолжаться процесс – тем лучше. Это повлияет на увеличение криптографических свойств ключей. Жмем Format. Далее начинается процесс создания раздела. На диске T:\Doc\ появится файл Volume. Он будет выступать контейнером в котором будет находится шифрованный раздел TrueCrypt. По окончанию вы увидите окно показанное ниже.

Рисунок 6.8 – Создание раздела

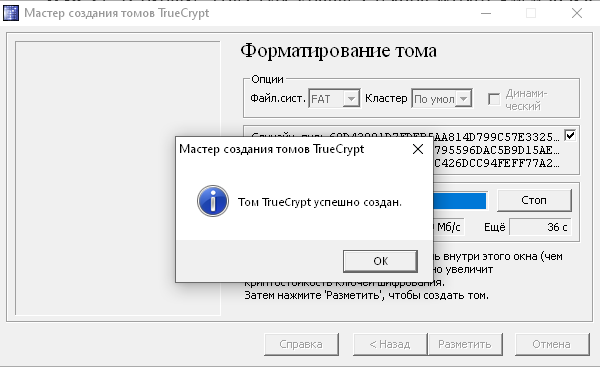
**Этап 12:** В окошке TrueCrypt Volume Creation Wizard жмем «Ок». После этого окно пропадает. Нажимаем «выход».Возвращаемся к главному окну программы TrueCrypt, если оно исчезло повторяем 1 этап и приступаем к монтировке.

Рисунок 6.9 – Завершение создания раздела

**Этап 13:** Выбираем одну из букв представленных в списке, это будет буква диска к которому примонтируем контейнер.

**Этап 14:** Жмем «Файл». При этом должна открыться стандартная версия окна в которой необходимо выбрать файл.

**Этап 15:** В данном окне находим файл, который вы создали с 6 по 11 этап и выбираем его. Жмем «Открыть», после этого окно должно исчезнуть.

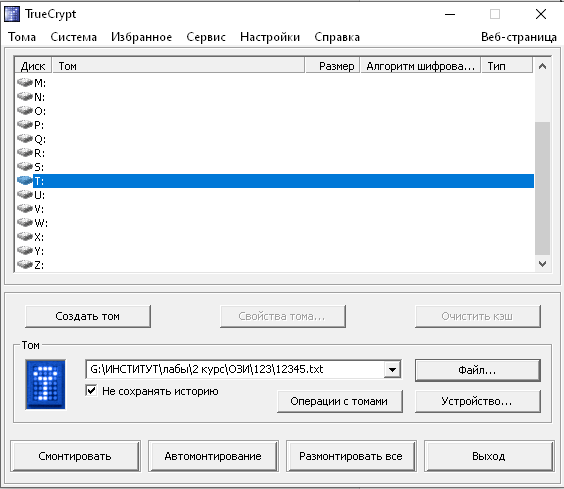
**Этап 16:** В оставшемся окошке TrueCrypt жмем Mount. Появляется окно, которое запрашивает ваш пароль.

Рисунок 6.10 – Выбор файла

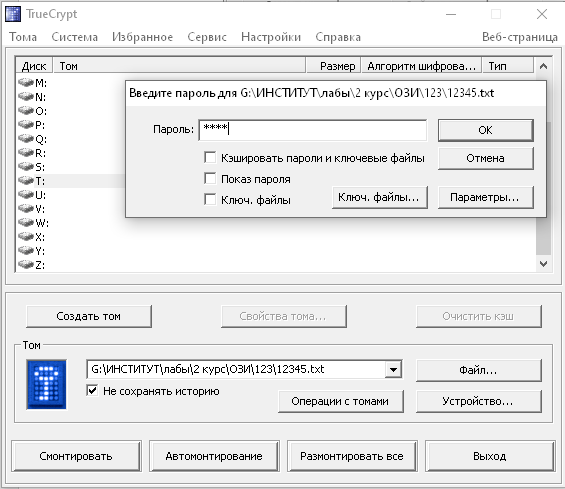
**Этап 17:** Вводим пароль, который вы установили на 10 этапе.

Рисунок 6.11 – Ввод пароля

**Этап 18:** Жмем «ОК».

Далее TrueCrypt приступает к монтировке раздела. В случае неправильного введения пароля TrueCrypt запросит повторный ввод, если пароль введен верно монтировка раздела пройдет успешно.

**Финальный этап:**

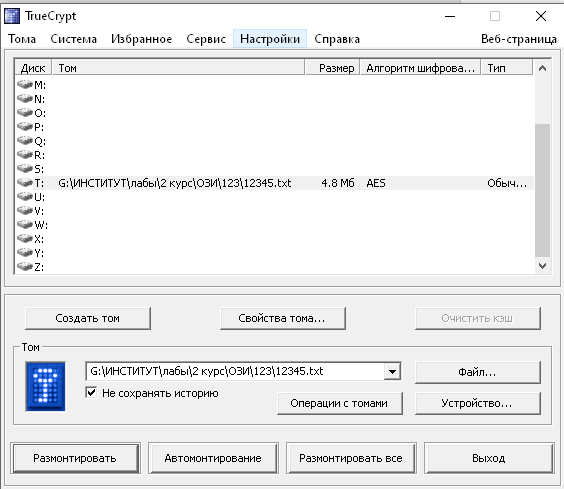


Рисунок 6.12 – Удачное завершение

Только что успешно прошла монтировка на один из виртуальных дисков. Диск полностью зашифрован и при этом ничем не отличается от прочих дисков. Вы можете помещать данные на данный диск и при этом они автоматически будут зашифровываться.

Если вы решите открыть файл, который размещен в TrueCrypt, то расшифровка будет производится автоматически через ОЗУ во время воспроизведения.

Важно: Обратите внимание, что при каждом открытие документа у вас будут требовать пароль.

Открыть уже смонтированный раздел можно два раза нажав на него мышкой как указанно на картинке ниже. Открыть его так же можно как и все прочие диски, через вкладку «Мой компьютер».

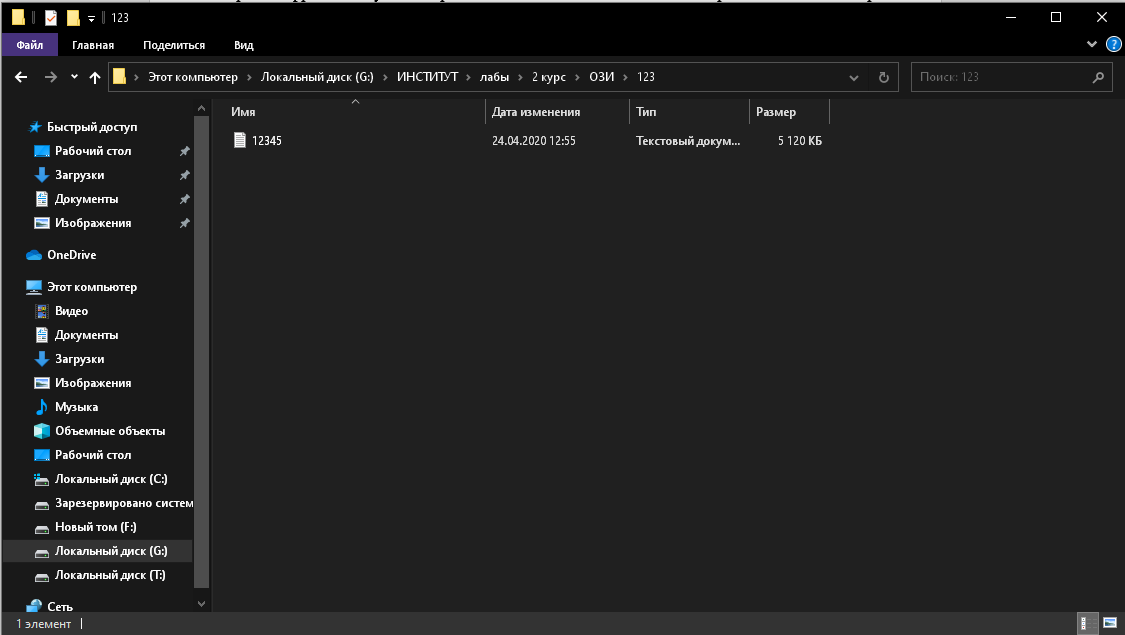


Рисунок 6.13 – Открытие

Вы имеете возможность осуществить копирование как с раздела TrueCrypt, так и на него. Все файлы автоматически расшифровываются или наоборот – зашифровываются.

Обратите внимание, что ни одна расшифрованная информация не подлежит сохранению, а лишь временно сохраняется в ОЗУ. Даже во время открытия файла данные по прежнему зашифрованные. Во время выключения или перезагрузки вашего компьютера, даже несанкционированного, раздел размонтируется и в доступе к файлам будет отказано. Для возобновления доступа необходимо произвести примонтировку описанную в с 13 по 18 этап.

Для закрытия раздела и отказа в доступе к данным вам следует выполнить следующие действия:

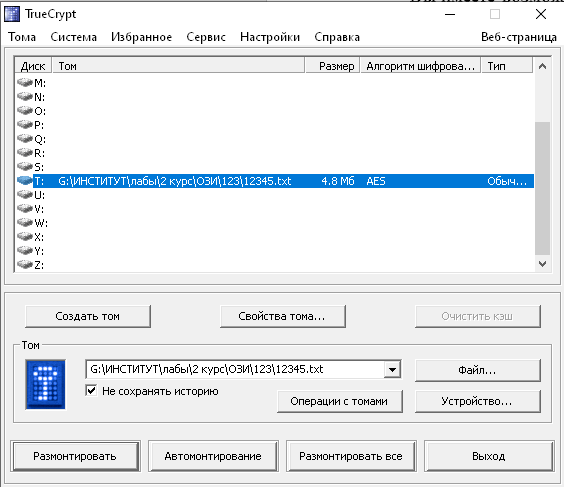


Рисунок 6.14 – Отказ в доступе

Из списка разделов, представленных в главном окне, необходимо выбрать один раздел и нажать «Размонтировать». Для открытия доступа к разделам необходимо повторить с 13 по 18 этап.

**Вывод:** таким образом, я овладел навыками работы с компьютерными программами для криптографической защиты информации при передаче и хранении.

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

**Теоретическое введение**

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

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа.

Помимо этого современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Шифрованием (encryption) называют процесс преобразования открытых данных (plaintext) в зашифрованные (шифртекст, ciphertext) или зашифрованных данных в открытые по определенным правилам с применением ключей.

В англоязычной литературе зашифрование / расшифрование – enciphering / deciphering.

Классификация алгоритмов шифрования

1. Симметричные (с секретным, единым ключом, одноключевые, single-key).

1.1. Потоковые:

· с одноразовым или бесконечным ключом (infinite-key cipher);

· с конечным ключом;

· на основе генератора псевдослучайных чисел.

1.2. Блочные:

1.2.1. Шифры перестановки (permutation, P-блоки);

1.2.2. Шифры замены (substitution, S-блоки):

· моноалфавитные;

· полиалфавитные;

2. Асимметричные (с открытым ключом, public-key):

· Диффи-Хеллман DH (Diffie, Hellman);

· Райвест-Шамир-Адлeман RSA (Rivest, Shamir, Adleman);

· Эль-Гамаль (ElGamal).

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

Обмен информацией осуществляется в 3 этапа:

* отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);
* отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;
* получатель получает сообщение и расшифровывает его.

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

При блочном шифровании информация разбивается на блоки фиксированной длины и шифруется поблочно. Блочные шифры бывают двух основных видов:

· шифры перестановки (transposition, permutation, P-блоки);

· шифры замены (подстановки, substitution, S-блоки).

Шифры перестановок переставляют элементы открытых данных (биты, буквы, символы) в некотором новом порядке. Различают шифры горизонтальной, вертикальной, двойной перестановки, решетки, лабиринты, лозунговые и др.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу. Paзличают шифры простой, сложной, парной замены, буквенно-слоговое шифрование и шифры колонной замены. Шифры замены делятся на две группы:

·моноалфавитные (код Цезаря);

·полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma).

В моноалфавитных шифрах замены буква исходного текста заменяется на другую, заранее определенную букву. Например в коде Цезаря буква заменяется на букву, отстоящую от нее в латинском алфавите на некоторое число позиций.



Очевидно, что такой шифр взламывается совсем просто. Нужно подсчитать, как часто встречаются буквы в зашифрованном тексте, и сопоставить результат с известной для каждого языка частотой встречаемости букв.

В полиалфавитных подстановках для замены некоторого символа исходного сообщения в каждом случае его появления последовательно используются различные символы из некоторого набора. Понятно, что этот набор не бесконечен, через какое-то количество символов его нужно использовать снова. В этом слабость чисто полиалфавитных шифров.

В современных криптографических системах, как правило, используют оба способа шифрования (замены и перестановки). Такой шифратор называют составным (product cipher). Oн более стойкий, чем шифратор, использующий только замены или перестановки.

В асимметричных алгоритмах шифрования (или криптографии с открытым ключом) для зашифровывания информации используют один ключ (открытый), а для расшифровывания - другой (секретный). Эти ключи различны и не могут быть получены один из другого.

Схема обмена информацией такова:

· получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);

· отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;

· получатель получает сообщение и расшифровывает его, используя свой секретный ключ.

**Алгоритм Диффи-Хелмана**

Алгоритм Диффи-Хелмана (Whitfield Diffie и Martin Hellman, 1976 год) использует функцию дискретного возведения в степень.

Сначала генерируются два больших простых числа n и q. Эти два числа не обязательно хранить в секрете. Далее один из партнеров P1 генерирует случайное число x и посылает другому участнику будущих обменов P2 значение A = qx mod n

По получении А партнер P2 генерирует случайное число у и посылает P2 вычисленное значение B = qy mod n

Партнер P1, получив В, вычисляет Kx = Bx mod n, а партнер P2 вычисляет Ky = Ay mod n. Алгоритм гарантирует, что числа Ky и Kx равны и могут быть использованы в качестве секретного ключа для шифрования. Ведь даже перехватив числа А и В, трудно вычислить Kx или Ky.

Алгоритм Диффи-Хелмана, обеспечивая конфиденциальность передачи ключа, не может гарантировать того, что он прислан именно тем партнером, который предполагается. Для решения этой проблемы был предложен протокол STS (station-to-station). Этот протокол для идентификации отправителя использует технику электронной подписи. Подпись шифруется общим секретным ключом, после того как он сформирован. Подпись включает в себя идентификаторы как P1, так и P2.

**Выполнение задания**

Практическая часть

1. Реализовать пример генерации секретного ключа методом Диффи-Хелмана:

a) В качестве p и g взять два любых простых числа.

b) Секретный ключ 1-го человека должен быть: номер варианта + 8.

открытое простое число p= 5;

открытое простое число g= 3;

секретный ключ 1 a=15+8=23;

открытый ключ 1 A = 333 mod 5=3;

секретный ключ 2 b=23;

открытый ключ 2 B = 323 mod 5 = 2;

секретный ключ s= 233 mod 5= 2;

Секретный ключ s = 323 mod 5=2;

2=2

2. Зашифровать сообщение «цвирко андрей» с использованием шифра Цезаря и полученного секретного ключа.

Шифр Цезаря один из наиболее древнейших известных шифров. Схема шифрования очень проста - используется сдвиг буквы алфавита на фиксированное число позиций.

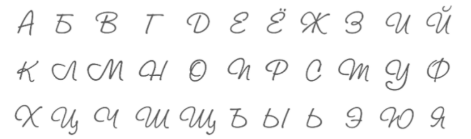
Шифруем по полученному ключу, равному 5, поэтому сдвиг будет происходить на пять разрядов вправо.

Рисунок 7.1 – Алфавит

Ключ 2: “ыгяжук ”

Аффинной преобразование буквы п зашифровать и расшифровать со своими параметрами и ключевое слово Фамилия, ключ Имя, зашифровать по Цезарю, смещение произвольное.

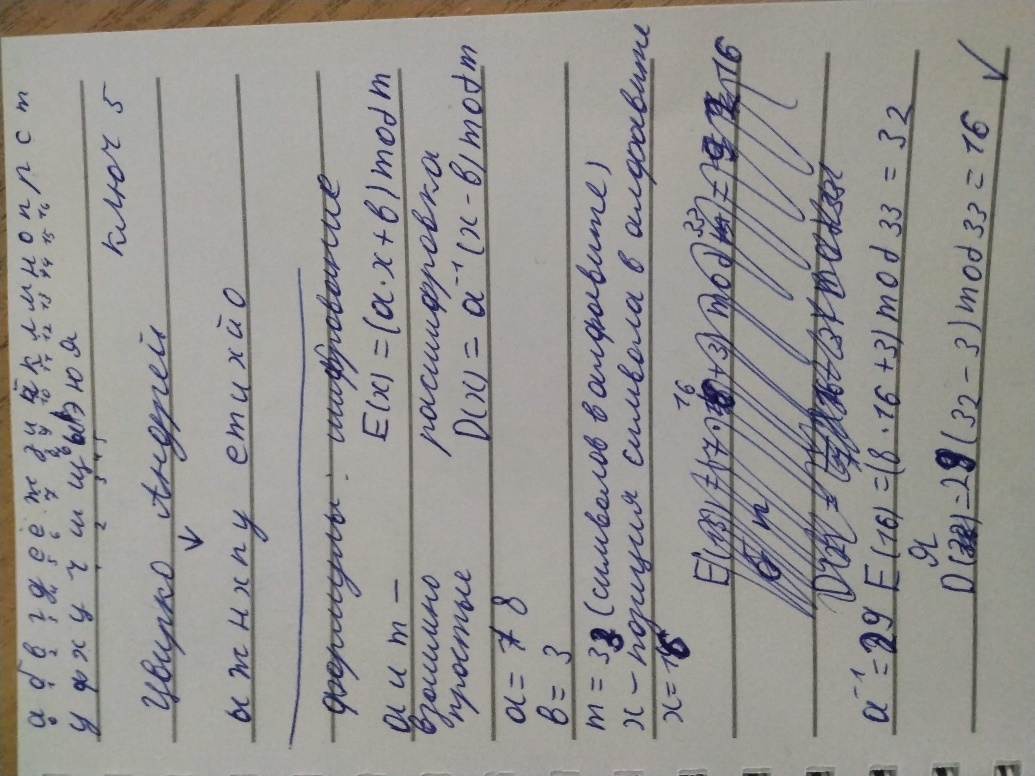
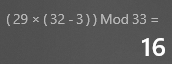
Результат решения:

Рисунок 7.2 – Выполнение задания

Вывод: овладел основными криптографическими алгоритмами шифрования.

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

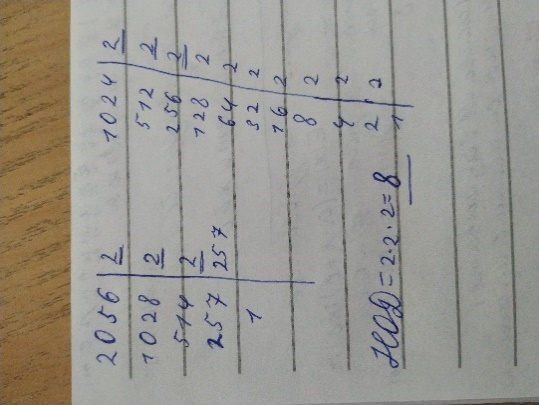
**Цель:** получение основных сведений из курса теории чисел

**Вариант 15**

**Условие**

1-3. *а* = 2056, *b* =1024.

**Задание 1**

Найти канонические разложения чисел *а* и *b*.

**Решение:**

Делается это так: в левую колонку выписываем исходное число, затем

Шаг 1: Берём самое маленькое простое число — 2 и по признакам делимости или обычным делением проверяем, делится ли исходное число на 2.

Шаг 2: Если делится, то в правую колонку выписываем 2. Далее делим исходное число на 2 и записываем результат в левую колонку под исходным числом.

Шаг 3: Если не делится, то берём следующее простое число — 3.

Повторяем эти шаги, при этом работаем уже с последним числом в левой колонке и с текущим простым числом. Разложение заканчивается, когда в левой колонке будет записано число 1.

**Задание 2**

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

**Решение.** Применим алгоритм Евклида. 2056=1024∙1 + 615738; 6793883 = 615738∙11 + 20765; 615738 = 20765 29 + 13553; 20756 = 13553∙1 + 7203; 13553 = 7203 1 + 6350; 7203 = 6350 1 + 853; 6350 = 853\*7 +379;853 = 379 2 + 95; 379 = 95\*3 +94; 95 = 94 1+1; 94 = 94 1

Следовательно, НОД (2056; 1024) = 8.

Найдём НОД (*a, b*), воспользовавшись разложением на простые множители чисел *a* и *b*, полученным в решении предыдущего задания: 2056=2\*2\*2\*257; 1024=2\*2\*2\*2\*2\*2\*2\*2\*2\*2. Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел: НОД (2056; 1024) = 8.

# Практическое занятие №9

**Криптографическая защита информации**

**Цель:** Овладение навыков работы с известными криптографическими алгоритмами.

Каждый пользователь выбирает два больших простых числа p и q, и в соответствии с описанным выше алгоритмом выбирает два простых числа e и d; как результат умножения первых двух чисел устанавливается n. После этого {e, n} образует открытый ключ, а {d, n} – секретный (хотя можно взять и наоборот).

Открытый ключ публикуется и доступен каждому, кто желает послать владельцу ключа сообщение, которое зашифровывается указанным алгоритмом. После шифрования, сообщение невозможно дешифровать с помощью открытого ключа. Владелец же секретного ключа без труда может pасшифpовать принятое сообщение.

Процедура создания ключей RSA заключается в следующем.

Выбирается два простых числа ***p*** и ***q***, например ***p = 7*** и ***q = 13***

Вычисляется произведение ***n = p\*q***, в нашем примере ***n = 7\*13 = 91***

Вычисляется функция Эйлера ***φ(n)***

***φ(n) = (p-1)\*(q-1)***

В нашем примере ***φ(n) = (7-1)\*(13-1) = 72***. Функция Эйлера определяет количество целых положительных чисел, не превосходящих ***n*** и взаимно простых с ***n***.

Целые числа называются взаимно простыми, если они не имеют никаких общих делителей, кроме 1.

Выбирается произвольное целое ***e***: ***0 < e < n*** взаимно простое с значением функции Эйлера ***φ(n)***. В нашем примере возьмём ***e = 5***. Пара чисел ***(e, n)*** объявляется открытым ключом шифра. В нашем примере ***(e, n) = (5, 91)***

Вычисляется целое число ***d***  (обратное число по модулю от е) из соотношения

***(d\*e) mod φ(n) = 1***.

Операция ***mod*** вычисляет остаток от целочисленного деления двух чисел.

Это соотношение означает, что результатом деления произведения чисел ***e*** и ***d*** на значение функции Эйлера должно быть число 1. Поэтому ***d*** можно рассчитать по формуле

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

придавая ***k*** последовательно значения 1, 2, 3,.. до тех пор, пока не будет получено целое число ***d***.

***Подсказка*.** Подбор ***k*** удобнее проводить в табличном процессоре Excel.

Найдём ***d*** в рассматриваемом примере:

http://altaev-aa.narod.ru/security/images/im8.png

при ***k = 1***, ***d*** – не целое, при ***k = 2***, ***d = 29***. Пара чисел ***(d, n)*** будет закрытым ключом шифра. В нашем примере ***(d, n) = (29, 91)***.

RSA-шифрование сообщения ***T*** выполняется с помощью открытого ключа получателя ***(e, n)*** по формуле

http://altaev-aa.narod.ru/security/images/im9.png,

где ***Ti*** и ***Ci*** числовые эквиваленты символов исходного и зашифрованного сообщений.

Реализовать пример шифрования сообщения в соответствии с вариантом, исходные данные которого представлены в таблице 9.

*Таблица 9 – “Исходные данные”*

|  |  |  |  |
| --- | --- | --- | --- |
| № варианта | Сообщение | p | Q |
| 26 | DCD | 107 | 5 |

Вычисляем произведение

Находим функцию Эйлера .

Выбирается произвольное целое ***e***: ***0 <e <n*** взаимно простое с значением функции Эйлера ***φ(n)***. В нашем примере возьмём ***e = 7***. Пара чисел ***(e, n)*** объявляется открытым ключом шифра. В нашем задании ***(e, n) = (7,535)***

Вычисляется целое число ***d*** (обратное число по модулю от е) по формуле:

Пара чисел ***(d, n)*** будет закрытым ключом шифра. В нашем задании ***(d, n) = (303, 535)***.

RSA-шифрование сообщения ***T*** выполняется с помощью открытого ключа получателя ***(e, n)*** по формуле

,

где ***Ti*** и ***Ci*** числовые эквиваленты символов исходного и зашифрованного сообщений (см. табл. 9.2).

*Таблица 9.2 - Числовые эквиваленты английских букв, цифр и символа пробела*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** |
| А | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **24** | **25** | **26** | **27** | **28** | **29** | **30** | **31** | **32** | **33** | **34** | **35** | **36** | **37** |
| X | Y | Z | пробел | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

Зашифруем сообщение «DCD» с помощью открытого ключа (7,535) (см. табл. 9.3).

*Таблица 9.3 - Вычисление шифрограммы*

|  |  |  |
| --- | --- | --- |
| **Символы исходного сообщения, *Ti*** | **Коды символов *Ti* (табл. 1)** | **Зашифрованные коды символов*Ci*** |
| D | 68 | ***687mod 535 =32*** |
| C | 67 | ***677mod 535 =78*** |
| D | 68 | ***687mod 535 =32*** |

Таким образом, мы исходное сообщение «DCD» представили в виде шифрограммы «1252,1,1».

Расшифровка RSA-закодированного сообщения ***T*** выполняется с помощью закрытого ключа получателя ***(d, n)*** по формуле

Восстановим исходное сообщение, применив закрытый ключ ***(d, n) = (303, 535)*** той же пары (см. табл. 9.4).

*Таблица 9.4 - Восстановление сообщения*

|  |  |  |
| --- | --- | --- |
| **Зашифрованные коды символов *Ci*** | **Дешифрованные коды символов *Ti*** | **Символы исходного сообщения, *Ti*** |
| 32 | ***1303mod 535 = 68*** | D |
| 78 | ***1303mod 535 = 67*** | C |
| 32 | ***1303mod 535 = 68*** | D |

Таким образом, мы восстановили исходное сообщение «DCD».

**Вывод**: Овладели навыками работы с известными криптографическими алгоритмами, зашифровали и расшифровали сообщение с помощью алгоритма RSA.

# Практическое занятие №9

**Авторское право и смежные права**

Цель: Изучить основные положения авторского права и смежных прав.

* Объекты, на которые распространяется авторское право.

Объекты авторского права и смежных прав (литературные, художественные, научные произведения, компьютерные программы, базы данных, музыкальные произведения, исполнительская деятельность артистов, аудио- и видеозаписи, радио- и телевизионные передачи и др.). Авторское право распространяется как на обнародованные, так и на необнародованные произведения, существующие в какой-либо объективной форме.

Произведения

* литературные (включая компьютерные программы и базы данных);
* научные (статьи, монографии, отчеты);
* драматические и музыкально-драматические, сценарные;
* хореографические и пантомимы;
* музыкальные с текстом или без текста;
* аудиовизуальные;
* живописи, скульптуры и другие изобразительного искусства;
* декоративно-прикладного искусства;
* архитектуры, градостроительства и садово-паркового искусства;
* фотографические;
* карты, планы, эскизы и иные, относящиеся к архитектуре, географии, топографии, другим наукам и технике;
* другие произведения.

2.Производные произведении

* переводы, обработки, инсценировки, музыкальные аранжировки, обзоры.аннотации, рефераты;
* сборники произведений: энциклопедии, антологии, атласы и другие составные произведения как результат творческого труда.

3.Компьютерные программы (все виды программ)

* прикладные программы и операционные системы на любом языке и в любой форме, включая исходный текст и объектный код.
* Базы данных или компиляции иных материалов в любой форме, представляющие собой по подбору и расположению материалов результат интеллектуального творчества.

Авторские права распространяются на:

* произведения, обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) на территории РБ, независимо от гражданства авторов и их правопреемников;
* произведения авторов-граждан РБ (и их правопреемников), обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) за пределами РБ;
* произведения авторов- фаж дан других государств (и их правопреемников), обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) за пределами РБ - в соответствии с международными договорами РБ.

Авторское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты.

Авторское право на произведение не связано с правом собственности на материальный объект, в котором произведение выражено.

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).

Принадлежат автору независимо от его имущественных прав и сохраняются за ним даже после уступки исключительных прав на использование произведения.

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.

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 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.
* Общественное достояние по истечении срока действия имущественных прав на объекты авторского права или смежных прав означает переход этих объектов в общественное достояние и может свободно использоваться любым физическим или юридическим лицом без выплаты вознаграждения.
* Переход авторского права по наследству, кроме прав авторства, на имя и на защиту репутации автора без ограничения срока.
* Автор вправе указать лицо, на которое он возлагает охрану своих личных неимущественных прав после своей смерти и осуществляет свои полномочия пожизненно. При отсутствии указаний охрана осуществляется его наследниками или специально уполномоченным государственным органом РБ при отсутствии наследников.

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 имею; права самостоятельно совершать какие-либо сделки, связанные с использованием авторского права. Несовершеннолетние в возрасте от 14 до 18 лет могут самостоятельно осуществлять авторские права на свои произведения.

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

Лицо, обозначенное в качестве автора на оригинале или экземпляре произведения, считается его автором, если отсутствует доказательство иного.

Авторское право может принадлежать нескольким лицам - соавторам. Авторское право на произведение, созданное совместным творческим трудом двух или более лиц, принадлежит соавторам совместно, независимо от того, образует ли такое произведение одно неразрывное целое или состоит из частей, каждая из которых имеет самостоятельное значение.

Субъектами авторского права после смерти автора становятся наследники. Наследование авторских прав может происходить как по закону, так и по завещанию.

Авторский договор - это соглашение, в силу которого одна сторона (автор) передает или обязуется передать другой стороне (пользователю) свои права на использование произведения, а пользователь обязуется уплатить автору установленное вознаграждение за использование или предоставление такого права.

Выступая в качестве особого вида гражданско-правового договора, авторский договор, в свою очередь, подразделяется на ряд разновидностей, каждая из которых имеет свои особенности.

Наиболее распространенным видом авторского договора является издательский договор. В рамках данного договора осуществляется 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 и т.д. Издательский договор наиболее полно урегулирован действующим законодательством и исследован юридической наукой. Нередко выводы, которые первоначально делаются на базе применения норм об издательском договоре, а также сложившейся практики разрешения споров, впоследствии распространяются и на другие авторские договоры.

Наиболее распространенным видом авторского договора является издательский договор. В рамках данного договора осуществляется 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 и т.д. Издательский договор наиболее полно урегулирован действующим законодательством и исследован юридической наукой. Нередко выводы, которые первоначально делаются на базе применения норм об издательском договоре, а также сложившейся практики разрешения споров, впоследствии распространяются и на другие авторские договоры.

Постановочный договор заключается тогда, когда основным способом использования произведения является его публичное исполнение. Его предметом могут быть драматические произведения, музыка или либретто оперы, балета, оперетты, музыка к драматическому спектаклю и т.п., которые используются театрально-зрелищными организациями (театрами, филармониями, цирками, концертными организациями и т.д.) путем постановки на сцене. В настоящее время постановочный договор должен заключаться пользователями в отношении как необнародованных, так и обнародованных произведений.

Сценарный договор - это договор, который регламентирует отношения, связанные с использованием текста, по которому снимается кинофильм, телефильм, делается радио- или телепередача, проводится массово-зрелищное мероприятие и т.д. Сценарный договор близок к постановочному договору, из рамок которого он постепенно выделился в самостоятельный вид. Их основное различие заключается в том, что литературный сценарий в отличие, например, от драматического произведения используется не в своем неизменном виде, а служит основой для создания более приближенного к нуждам кинематографа, телевидения или радио режиссерского сценария, по которому, собственно, и ставится фильм или делается передача. В этом смысле сценарный договор предполагает, что произведение (сценарий) может быть использовано в измененном виде.

Договор о депонировании рукописи регулирует условия и порядок обнародования и последующего использования произведения, которое помещается на хранение в специальный информационный орган.Договор художественного заказа опосредует отношения, связанные с созданием произведений изобразительного искусства в целях их публичной демонстрации .Владельцы произведений (материальных носителей) вправе распоряжаться ими по своему усмотрению, но при условии уважения авторских прав создателей авторских произведений.

Договор об использовании в промышленности произведений декоративно-прикладного искусства имеет своей задачей урегулирование вопросов, возникающих в связи с тиражированием в промышленности оригинальных произведений декоративно-прикладного искусства. Он заключается лишь с внештатными художниками предприятий, произведения которых принимаются к использованию. Авторы получают вознаграждение как за сам факт создания произведения, принятого к использованию, так и за последующее тиражирование в зависимости от объема использования.

Содержание авторского договора:

* авторский договор на передачу исключительных прав, разрешающий использование произведения определенным способом и в установленных пределах только лицу, которому эти права передаются;
* авторский договор на передачу неисключительных прав, разрешающий использование произведения и другим лицам, в том числе самому обладателю исключительных прав, заключившему авторский договор.

Авторский договор заключается в письменной форме и, по желанию сторон, может быть заверен нотариально. Договор может быть изменен, прекращен или расторгнут также только письменно. В каждом отдельном случае издатель и автор выбирают и согласуют оригинальный текст авторского договора. Следует отметить, что авторский договор не обязательно представляет собой единый документ. Он может включать и различного рода дополнительные соглашения. Авторское право предусматривает возможность заключения еще одного вида договора - авторского договора заказа. По договору заказа автор обязуется создать произведение в соответствии с условиями договора и передать его заказчику. Особенность авторского договора заказа состоит в том, что заказчик обязан в счет обусловленного договором вознаграждения выплатить автору аванс. Размер, порядок и сроки выплаты аванса устанавливаются в договоре по соглашению сторон.

В соответствии с законом, авторский договор должен предусматривать следующие обязательные положения:

* способы использования произведения (конкретные права, передаваемые по данному договору);
* срок и территории, на которые передается право;
* размер вознаграждения и (или) порядок определения размера вознаграждения за каждый способ использования произведения, порядок и сроки его выплаты.

**Вывод:** Изучил основные положения авторского права и смежных прав.

# Практическое занятие №10

**Криптографическая защита информации**

**Цель:** Овладение навыков работы с известными криптографическими алгоритмами.

Каждый пользователь выбирает два больших простых числа p и q, и в соответствии с описанным выше алгоритмом выбирает два простых числа e и d; как результат умножения первых двух чисел устанавливается n. После этого {e, n} образует открытый ключ, а {d, n} – секретный (хотя можно взять и наоборот).

Открытый ключ публикуется и доступен каждому, кто желает послать владельцу ключа сообщение, которое зашифровывается указанным алгоритмом. После шифрования, сообщение невозможно дешифровать с помощью открытого ключа. Владелец же секретного ключа без труда может pасшифpовать принятое сообщение.

Процедура создания ключей RSA заключается в следующем.

Выбирается два простых числа ***p*** и ***q***, например ***p = 7*** и ***q = 13***

Вычисляется произведение ***n = p\*q***, в нашем примере ***n = 7\*13 = 91***

Вычисляется функция Эйлера ***φ(n)***

***φ(n) = (p-1)\*(q-1)***

В нашем примере ***φ(n) = (7-1)\*(13-1) = 72***. Функция Эйлера определяет количество целых положительных чисел, не превосходящих ***n*** и взаимно простых с ***n***.

Целые числа называются взаимно простыми, если они не имеют никаких общих делителей, кроме 1.

Выбирается произвольное целое ***e***: ***0 < e < n*** взаимно простое с значением функции Эйлера ***φ(n)***. В нашем примере возьмём ***e = 5***. Пара чисел ***(e, n)*** объявляется открытым ключом шифра. В нашем примере ***(e, n) = (5, 91)***

Вычисляется целое число ***d***  (обратное число по модулю от е) из соотношения

***(d\*e) mod φ(n) = 1***.

Операция ***mod*** вычисляет остаток от целочисленного деления двух чисел.

Это соотношение означает, что результатом деления произведения чисел ***e*** и ***d*** на значение функции Эйлера должно быть число 1. Поэтому ***d*** можно рассчитать по формуле

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

придавая ***k*** последовательно значения 1, 2, 3,.. до тех пор, пока не будет получено целое число ***d***.

***Подсказка*.** Подбор ***k*** удобнее проводить в табличном процессоре Excel.

Найдём ***d*** в рассматриваемом примере:

http://altaev-aa.narod.ru/security/images/im8.png

при ***k = 1***, ***d*** – не целое, при ***k = 2***, ***d = 29***. Пара чисел ***(d, n)*** будет закрытым ключом шифра. В нашем примере ***(d, n) = (29, 91)***.

RSA-шифрование сообщения ***T*** выполняется с помощью открытого ключа получателя ***(e, n)*** по формуле

http://altaev-aa.narod.ru/security/images/im9.png,

где ***Ti*** и ***Ci*** числовые эквиваленты символов исходного и зашифрованного сообщений.

Реализовать пример шифрования сообщения в соответствии с вариантом, исходные данные которого представлены в таблице 9.

*Таблица 9 – “Исходные данные”*

|  |  |  |  |
| --- | --- | --- | --- |
| № варианта | Сообщение | p | Q |
| 4 | DCD | 13 | 97 |

Вычисляем произведение .

Находим функцию Эйлера .

Выбирается произвольное целое ***e***: ***0 <e <n*** взаимно простое с значением функции Эйлера ***φ(n)***. В нашем примере возьмём ***e = 7***. Пара чисел ***(e, n)*** объявляется открытым ключом шифра. В нашем задании ***(e, n) = (7, 1261)***

Вычисляется целое число ***d*** (обратное число по модулю от е) по формуле:

Пара чисел ***(d, n)*** будет закрытым ключом шифра. В нашем задании ***(d, n) = (823, 1261)***.

RSA-шифрование сообщения ***T*** выполняется с помощью открытого ключа получателя ***(e, n)*** по формуле

,

где ***Ti*** и ***Ci*** числовые эквиваленты символов исходного и зашифрованного сообщений (см. табл. 9.2).

*Таблица 9.2 - Числовые эквиваленты английских букв, цифр и символа пробела*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** |
| А | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **24** | **25** | **26** | **27** | **28** | **29** | **30** | **31** | **32** | **33** | **34** | **35** | **36** | **37** |
| X | Y | Z | пробел | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

Зашифруем сообщение «DCD» с помощью открытого ключа (7,1261) (см. табл. 9.3).

*Таблица 9.3 - Вычисление шифрограммы*

|  |  |  |
| --- | --- | --- |
| **Символы исходного сообщения, *Ti*** | **Коды символов *Ti* (табл. 1)** | **Зашифрованные коды символов*Ci*** |
| D | 4 | ***47mod 1261 =1252*** |
| C | 3 | ***37mod 1261 = 926*** |
| D | 4 | ***47mod 1261 =1252*** |

Таким образом, мы исходное сообщение «DCD» представили в виде шифрограммы «1252,926,1252».

Расшифровка RSA-закодированного сообщения ***T*** выполняется с помощью закрытого ключа получателя ***(d, n)*** по формуле

Восстановим исходное сообщение, применив закрытый ключ ***(d, n) = (823, 1261)*** той же пары (см. табл. 9.4).

*Таблица 9.4 - Восстановление сообщения*

|  |  |  |
| --- | --- | --- |
| **Зашифрованные коды символов *Ci*** | **Дешифрованные коды символов *Ti*** | **Символы исходного сообщения, *Ti*** |
| 1252 | ***1252823mod 1261 = 4*** | D |
| 926 | ***926823mod 1261 = 3*** | C |
| 1252 | ***1252823mod 1261 = 4*** | D |

Таким образом, мы восстановили исходное сообщение «DCD».

**Вывод**: Овладели навыками работы с известными криптографическими алгоритмами, зашифровали и расшифровали сообщение с помощью алгоритма RSA.

### Практическое занятие №11

**Составление и оформление заявок на объекты промышленной собственности**

Цель: Овладеть навыками составления и оформления заявок на объекты промышленной собственности

На данном практическом занятии рассматриваются следующие вопросы:

* Основные составляющие описания изобретения?
* Правила оформления описания изобретения?
* Какие основные пункты должна содержать заявка на изобретение?
* Основные документы, необходимые для подачи заявки на изобретения?
* Отличия заявок на охранные документы различных объектов промышленной собственности?
* На какие ОПС выдаются патенты?
* На какие ОПС выдаются свидетельства?

Одной из наиболее распространенных коммерчески значимых форм правовой охраны является патент, который обеспечивает патентообладателю исключительное (монопольное) право на использование объекта промышленной собственности и запрещает всем третьим лицам их использование в коммерческих целях без разрешения патентообладателя. Являясь одновременно правовым, техническим и информационным документом, патент выступает не только в качестве формы правовой охраны от несанкционированного использования, но и своеобразным экономическим стимулом для инвестиций в научные исследования и промышленность.

Составление и оформление заявок на объекты промышленной собственности (изобретение, полезную модель, промышленный образец, товарный знак и др.).

Алгоритм патентования:

* отбор изобретений для патентования;
* подготовка заявок на выдачу патентов;
* подача заявок в соответствующие патентные ведомства;
* ведение переписки с патентными ведомствами в процессе проведения экспертизы по заявкам на патенты;
* ведение переписки по патентным спорам с административными и судебными органами;
* получение патентов;
* оплата пошлин за юридически значимые действия;
* поддержание в силе заявок на патенты и собственно патентов.

Описание изобретения наряду с формулой изобретения и графическими материалами (если они необходимы) является основным документом на выдачу патента. Оно представляет собой технико-правовой документ и должно полностью раскрывать техническую сущность изобретения, а также содержать достаточную информацию для дальнейшей разработки объекта изобретения. Кроме того, описание изобретения должно давать точное и ясное представление о новизне, изобретательском уровне и промышленной применимости изобретения.

Описание начинается с названия изобретения и указания индекса или индексов рубрики действующей редакции международной патентной классификации, к которой относится заявляемое изобретение и содержит следующие разделы:

* 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. 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. При этом оценка новизны и изобретательского уровня осуществляется в сравнении с уровнем техники для определения, которого проводится информационный поиск. Источники с общедоступной информацией об изобретении раскрытые автором прямо или косвенно не включаются, если раскрытие осуществлено не позднее 12 месяцев до даты подачи заявки в патентный орган.

В разделе «Уровень техники» приводятся сведения об аналогах и прототипах.

Аналог изобретения – это известное до даты приоритета средство того же назначения, совокупность признаков которого сходна с совокупностью существующих признаков изобретения.

Приоритет изобретения устанавливается по дате поступления в патентный орган надлежащим образом оформленной заявки. Если в процесс экспертизы установлено, что идентичное изобретение имеет одну и туже дату приоритета, то патент может быть выдан, но заявке, но которой доказана более ранняя дата ее отправки в патентный орган.

За прототип изобретения принимается аналог наиболее близкий, но совокупности признаков. К приводимым сведениям о каждом из аналогов, в то числе о прототипе относятся библиографические данные источника информации, в котором он раскрыт, признаки аналога с указанием тех из них, которые совпадают с существенными признаками заявляемого изобретения, а также указание причин, препятствующих получению требуемого технического результата. Если аналогов несколько, то последним описывается прототип.

Заявка на изобретение 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.

Вместе с заявкой или не позднее 2-х месяцев с даты ее подачи в одном экземпляре предоставляется документ, подтверждающий уплату пошлины в установленном размере или освобождение от уплаты, либо наличие оснований для уменьшения ее размера.

Заявление о выдаче патента оформляется на русском языке. Остальные документы на белорусском, русском или другом языке.

В заявлении о выдаче патента указываются сведения о названии изобретения, заявителях и авторах, дате подачи заявки, адресе для переписки, перечня прилагаемых документов и др. Заявление представляется по установленной НЦИС форме.

Описание изобретения наряду с формулой изобретения и графическими материалами (если они необходимы) является основным документом на выдачу патента. Оно представляет собой технико-правовой документ и должно полностью раскрывать техническую сущность изобретения, а также содержать достаточную информацию для дальнейшей разработки объекта изобретения. Кроме того, описание изобретения должно давать точное и ясное представление о новизне, изобретательском уровне и промышленной применимости изобретения.

Вместе с заявкой или не позднее 2-х месяцев с даты ее подачи в одном экземпляре предоставляется

* документ, подтверждающий уплату пошлины в установленном размере или освобождение от уплаты, либо наличие оснований для уменьшения ее размера;
* доверенность, при подаче заявки через патентного поверенного;
* заверенная копия первой заявки, в случае подачи заявки в соответствии с Парижской конвенцией по охране промышленной собственности (конвенционная заявка).

При экспертизе заявки на полезную модель проверка соответствия заявленной полезной модели условиям патентоспособности не осуществляется.

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.

Охранный документ (патент, свидетельство) – это выдаваемый патентным органом от имени государства документ, который удостоверяет авторство, приоритет на объект промышленной собственности и исключительное право на его использование. Приоритет - первенство, чаше всего, определяемое датой подачи заявки на ОПС. Конвенционный приоритет обозначает, что заявка, поданная в одной стране-участнице конвенции, обладает во всех других странах приоритетом в течение года, исчисляемого с момента подачи заявки в первой стране. Одной из наиболее распространенных коммерчески значимых форм правовой охраны является патент, который обеспечивает патентообладателю исключительное (монопольное) право на использование объекта промышленной собственности и запрещает всем третьим лицам их использование в коммерческих целях без разрешения патентообладателя. Являясь одновременно правовым, техническим и информационным документом, патент выступает не только в качестве формы правовой охраны от несанкционированного использования, но и своеобразным экономическим стимулом для инвестиций в научные исследования и промышленность.

ОПС патенты выдаются на: устройства, изделия, способы, вещества, биотехнические продукты, применение устройства, способа, вещества, биотехнического продукта по определенному положению.

* устройство (например, машина, прибор, инструмент, деталь и др.);
* способ (например, способ изготовления изделий, нанесения покрытий, способ лечения и др.);
* вещество (сплав, смесь, раствор, химическое соединение и др.);   
  биотехнологический продукт;
* применение устройства, способа, вещества, биотехнологического продукта по определенному назначению.

ОПС свидетельства выдаются на: открытия, научные теории, математические методы, изобретения, противоречащие принципам гуманности и морали.

Свидетельство выдается на товарный знак, на географические указания на 10 лет с последующим продлением на неопределенное количество раз по 10 лет.

Вывод: овладел навыками составления и оформления заявок на объекты промышленной собственности.

**Практическое занятие №11**

**Тема «Патентные исследования»**

Цель: Изучить виды, содержание и порядок проведения патентных исследований.

**Теоретическое введение**

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 КЛАССИФИКАЦМЯ (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).

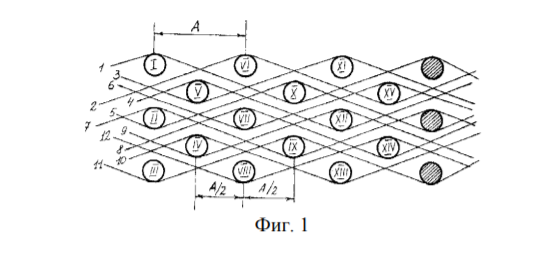
**МПК**, кроме того, является:

* 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.

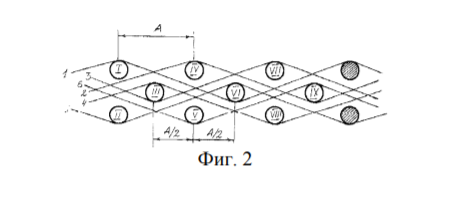
**МПК** охватывает все области знаний, объекты которых могут подлежать защите охранными документами. Иерархическая структура МПК выражается в разбивке всех областей знаний на несколько классификационных уровней. В нисходящем порядке эти уровни иерархии соответствуют разделам, классам, подклассам, основным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

Информационная база - *Афiцыйны бюлетэнь «Вынаходствы, карысныя мадэлi, прамысловыя узоры» Нацыянальнага цэнтра iнтэлектуальная уласнасцi Рэспублiкi Беларусь, каталог МПК .*[http://www.belgospatent.org.by](http://www.belgospatent.org.by/)

Проведенный патентный поиск по указанному классу, выявил следующие аналогичные по конструктивному выполнению патенты и полезные модели, приведенные на рисунках.

 Многослойная ткань, состоящая по меньшей мере из двух систем основных нитей и уточных нитей и выполненная саржевым переплетением, причем соединение соседних основных систем выполнено переплетением каждых двух противолежащих основных нитей с общей уточной нитью для каждой пары основных нитей, при этом в соединении соседних основных систем последовательно участвует каждая нить этих систем, отличающаяся тем, что соотношение плотности основных и уточных нитей в ткани равно (1,1-1,3):1. 2. Ткань по п. 1, отличающаяся тем, что каждая основная система связывает две соседние системы уточных нитей. 3. Ткань по п. 1 или 2, отличающаяся тем, что каждая последующая уточная система нитей смещена относительно предыдущей уточной системы на величину, равную половине расстояния между двумя нитями в уточной системе.

Изобретение относится к области текстильных тканых материалов, предназначенных для использования при изготовлении теплоизоляционных и конструкционных композиционных материалов. Известна многослойная ткань, состоящая по крайней мере из двух систем основных нитей и уточных нитей и выполнена саржевым переплетением, причем соединение соседних основных систем выполнено переплетением каждых двух противолежащих основных нитей с общей уточной нитью для каждой пары основных нитей, при этом в соединении соседних основных систем последовательно участвует каждая основная нить этих систем (Европейская заявка № 20038, кл. D 03D 11/00, 1980).

 Недостатком указанной ткани является потеря прочности в продольном направлении ткани из-за наличия изогнутости нитей основных систем. Нити уточных систем, переплетающиеся с нитями основных систем, изогнуты более чем в два раза по сравнению с нитями уточных систем, не переплетающихся с нитями основных систем, вследствие чего при растяжении ткани нити разных уточных систем работают неодновременно, снижая прочность ткани по утку. Задача настоящего изобретения заключается в повышении физико-механических показателей за счет создания равнопрочного тканого материала. Эта задача решается за счет того, что в многослойной ткани, состоящей по меньшей мере из двух систем основных нитей и уточных нитей и выполненной саржевым переплетением, причем соединение соседних основных систем выполнено переплетением каждых двух противолежащих основных нитей с общей уточной нитью для каждой пары основных нитей, соотношение плотности основных и уточных нитей в ткани равно (1,1-1,3):1.

Также каждая основная система связывает две соседние системы уточных нитей. При этом каждая последующая система уточных нитей смещена относительно предыдущей на величину, равную половине расстояния между двумя нитями в уточной системе. Технический результат достигается за счет уменьшения межнитевого пространства, что дает увеличение прочности на 10-30 %.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Таблица 1 – Патентная документация | | | | |
| 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) |
| Ткань, многослойная ткань | Патент РБ  № 6275  МПК D03D. | Финникова З.И., Еровенкова В.И.,Сергеев В.Т.  Заявка а20000878 от 2000.05.29,опубл. 0.06.2004  ОБ № 3, 2004. | «Многослойная ткань» | Действует |
| Патент РБ  № 11484  МПК D03D , H05B. | Витебский государственный технологический университет  Заявка a20070196 от 2007.02.26,опубл. 30.10.2008  ОБ № 1, 2006. | «Многослойный электропроводящий материал» | Действует |
| Патент РБ  № 1200U  МПК D03D. | Елисеева Р.И., Транковский В.П., Кущенко Л.Н.  Заявка u20030272 от 2003.06.16, опубл. 30.12.2003  ОБ № 3, 2000. | «Кремнеземная ткань» | Действует |
| Патент РБ  № 6170  МПК D03D. | Открытое акционерное общество «Гродно Химволокно».  Заявка u19990271 от 1999.03.25, опубл. 30.06.2004  ОБ № 3, 1991. | «Полиэфирная кордная ткань для каркаса радиальных шин» | Действует |

### Практическое занятие №13

**Патентный поиск**

Цель: освоить навыки проведения патентного поиска по заданной тематике

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.

Национальный центр интеллектуальной собственности [http://www.belgospatent.org.by](http://www.belgospatent.org.by/)

Российское агентство но патентам и товарным знакам (Роспатент) предоставляет доступ к патентным материалам на страницах своего сайта:

http://www1.fips.ru/wps/wcm/connect/content\_ru/ru/inform\_resources/inform\_retrieval\_system

Евразийские патенты – http://www.eapo.org

Бесплатный поиск по патентам США возможно проводить с 1790 г по сайту компании United States Patent and Trademark Office [http://www.uspto.gov](http://www.uspto.gov/patft/)

Европейский патентный офис [http://www.epo.org](http://www.epo.org/)

Патентное бюро Японии. Поиск по серверу Японского патентного ведомства (ЯПВ) необходимо начинать со страницы [www.jpo.go.jp](http://www.jpo.go.jp)

Российские патенты www.fips.ru/

Задание для выполнения: Интернет-сервис аутентификации

|  |  |
| --- | --- |
| **Классы МПК:** | [G06F 15/173 (2006.01)](http://www1.fips.ru/publication-web/classification/mpk?view=detail&edition=2018&symbol=G06F) ,[H04B 7/00 (2006.01)](http://www1.fips.ru/publication-web/classification/mpk?view=detail&edition=2018&symbol=H04B)  АУТЕНТИФИКАЦИЯ В СИСТЕМЕ СВЯЗИ |
| **Автор(ы):** | ХСУ Рэймонд Т. |
| **Патентообладатель(и):** | КВЭЛКОММ ИНКОРПОРЕЙТЕД (US) |
| **Приоритеты:** | подача заявки: 20.06.2003  публикация патента: 31.12.2003 |

G:\ИНСТИТУТ\лабы\2 курс\ОЗИ\00000001.tif Изобретение относится к аутентификации в системе связи. Предложены способ и устройство для обеспечения шифрования речи при сотовой аутентификации в формате расширяемого протокола аутентификации. Техническим результатом является обеспечение обычного формата для аутентификации и настройки. 8 н. и 3 з.п. ф-лы, 8 ил.

|  |  |
| --- | --- |
| **Классы МПК:** | G06F 19/00, G06F 17/60, G07F 19/00 Система проведения безналичного расчета |
| **Автор(ы):** | Тюменцев Павел Дмитриевич |
| **Патентообладатель(и):** | Тюменцев Павел Дмитриевич |
| **Приоритеты:** | подача заявки: 2002-11-29  публикация патента: 30-06-2003 |

Система для проведения безналичного расчета, включающая взаимодействующие посредством сети связи, по меньшей мере, одно персональное мобильное средство связи покупателя, средство для генерирования запроса на обслуживание, центр идентификации первичного кода абонента мобильной сети связи, осуществляющий проверку аутентичности запроса, процессинговый центр банка и процессинговый центр продавца, осуществляющие обработку запроса, отличающаясятем, что дополнительно содержит имитатор личного кода покупателя и идентификатор личного кода покупателя, средство генерирования запроса на обслуживание выполнено в виде устройства ввода информации, связанного с персональным мобильным средством связи покупателя, персональное мобильное средство связи покупателя снабжено средством визуализации личного кода покупателя, а процессинговый центр продавца снабжен соответствующим средством считывания и идентификации личного кода покупателя и выполнен с возможностью обработки запроса на обслуживание покупателя по результатам идентификации первичного кода абонента мобильной сети связи и личного кода покупателя. Система по п. 1, отличающаясятем, что имитатор личного кода покупателя выполнен в виде имитатора штрих-кода, предпочтительно кода EAN-13. Система по любому из пп. 1, 2, отличающаясятем, что имитатор личного кода покупателя размещен в процессинговом центре банка.

Система по любому из пп. 1, 2, отличающаясятем, что имитатор личного кода покупателя размещен в персональном мобильном средстве связи покупателя.

Система по любому из пп. 1, 2, отличающаясятем, что имитатор личного кода покупателя размещен в процессинговом центре банка и в персональном мобильном средстве связи покупателя. Система по любому из пп. 1-5, отличающаясятем, что идентификатор личного кода покупателя размещен в процессинговом центре банка. Система по любому из пп. 1-6, отличающаясятем, что средство визуализации личного кода покупателя выполнено в виде дисплея персонального мобильного средства связи покупателя, выполненного с возможностью воспроизведения текстово-графической информации, предпочтительно штрих-кода.

Система по любому из пп. 1-7, отличающаясятем, что средство считывания и идентификации личного кода покупателя выполнено в виде сканера, выполненного с возможностью считывания и идентификации текстово-графической информации, предпочтительно штрих-кода.

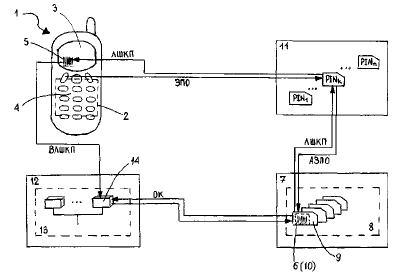


Рисунок 13.2 – Система проведения безналичного расчета

|  |  |
| --- | --- |
| **Классы МПК:** | G07D/00, G06F 17/60  Способ проведения финансовых операций и система для его осуществления |
| **Автор(ы):** | [Бурш Владимир Леонидович](http://bypatents.com/patents/bursh-vladimir-leonidovich), [Колешко Владимир Михайлович](http://bypatents.com/patents/koleshko-vladimir-mihajjlovich), [Карякин Юрий Дмитриевич](http://bypatents.com/patents/karyakin-yurijj-dmitrievich) |
| **Патентообладатель(и):** | [Бурш Владимир Леонидович](http://bypatents.com/patents/bursh-vladimir-leonidovich), [Колешко Владимир Михайлович](http://bypatents.com/patents/koleshko-vladimir-mihajjlovich), [Карякин Юрий Дмитриевич](http://bypatents.com/patents/karyakin-yurijj-dmitrievich) |
| **Приоритеты:** | подача заявки: 1998-07-24  публикация патента: 30-12-2002 |

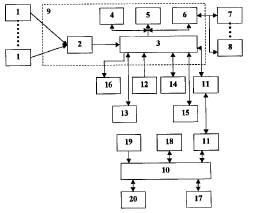
1. Способ проведения финансовых операций, заключающийся в вводе финансовой информации в компьютерную финансовую систему, обработке финансовой информации, ее индексировании, формировании базы данных, формировании транзакций и передаче их в компьютеры финансовых учреждений, отличающийсятем, что одновременно с вводом финансовой информации из нее выделяют часть информации, состав которой определен налоговым органом и преимущественно включает учетный номер налогоплательщика, даты начала и окончания действия сделки, суммы платежей или их эквиваленты, коды финансовых учреждений, номера расчетных счетов, эту часть информации кодируют и подают в компьютерную систему налогового органа, где ее регистрируют, а регистрационный номер используют при формировании транзакций, при этом осуществляют защиту зарегистрированной информации, которую используют налоговым органом для контроля подлинности финансовых документов, причем защиту зарегистрированной информации осуществляют путем формирования ее в виде документа на носителе, на поверхность которого наносят защитную машиночитаемую метку, при этом считывают тонкую структуру поверхности носителя, эту информацию обрабатывают, кодируют и совместно с кодированной информацией, состав которой определен налоговым органом, используют для формирования защитной машиночитаемой метки, причем для контроля подлинности финансового документа считывают защитную машиночитаемую метку с поверхности носителя, сравнивают полученную информацию с эталонным сигналом и по результату сравнения судят о подлинности финансового документа.
2. Способ по п. 1, отличающийсятем, что зарегистрированную кодированную информацию шифруют любым известным способом шифрования для передачи этой части информации субъектам хозяйствования.
3. Способ по п. 1 или 2, отличающийсятем, что при контроле подлинности финансовых документов первоначально считывают и обрабатывают информацию о структуре поверхности носителя, на основе чего формируют эталонный сигнал, с которым сравнивают только ту часть информации, заключенную в защитной машиночитаемой метке, которая относится к структуре поверхности носителя.
4. Система для проведения финансовых операций, включающая терминалы с устройствами ввода и отображения информации и передачи ее в компьютерную финансовую систему, которая содержит системы с устройствами приема информации от множества терминалов, связанные с первым входом процессорного устройства для обработки информации, второй вход-выход которого соединен с запоминающим устройством для хранения информации и программ ее обработки, устройством отображения информации и средством связи с компьютерами финансовых учреждений, отличающаяся тем, что компьютерная финансовая система дополнительно включает устройство считывания тонкой структуры поверхности документа на носителе, выход которого подключен к третьему входу процессорного устройства, и принтер высокого разрешения, выход которого соединен с четвертым входом процессорного устройства, при этом компьютерная финансовая система оснащена комплектом программ для считывания тонкой структуры поверхности носителя, обработки считанной информации и формирования защитной машиночитаемой метки, содержащей информацию о тонкой структуре поверхности носителя и кодированную информацию, состав которой определен налоговым органом и преимущественно включает учетный номер налогоплательщика, даты начала и окончания действия сделки, суммы платежей или их эквиваленты, коды финансовых учреждений, номера расчетных счетов, при этом к пятому входу процессорного устройства через дополнительное оборудование связи подключена компьютерная система налогового органа.
5. Система по п. 4, отличающаясятем, что включает средства хранения зарегистрированной защищенной информации, связанные с компьютерной финансовой системой и компьютерной системой налогового органа.
6. Система по п. 4 или 5, отличающаясятем, что она оснащена программными и/или аппаратными средствами шифрования, которые одновременно подключены к компьютерной финансовой системе и компьютерной системе налогового органа.

Рисунок 13.3 – Способ проведения финансовых операций и система для его осуществления

Вывод: Получил навыки патентного поиска по заданной тематике