Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

Электронная тетрадь

по Основам Защиты Информации

Студент: Полынская Ю.В.

ФИТ 2 курс 2 группа

Преподаватель: Берников В.О.

Минск 2019

# **Практическое занятие №1**

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

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

**Основными национальными интересами в информационной сфере являются:**

* реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;
* формирование и поступательное развитие информационного общества;
* равноправное участие Республики Беларусь в мировых информационных отношениях;
* преобразование информационной индустрии в экспортно-ориентированный сектор экономики;
* эффективное информационное обеспечение государственной политики;
* обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

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

* 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;
* снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента;

**Основные внутренние источники угроз национальной безопасности в информационной сфере:**

* 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.

**Основные внешние источники угроз национальной безопасности в информационной сфере:**

* 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.

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

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.

# **Практическое занятие №2**

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

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

**Задание на выполнение**

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.

Решить задачу разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа в соответствии с вариантом (см. таблицу2.1).

Таблица 2.1 – условия для задачи

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

*Е0* – положительный эффект (экономический, политический, технический и т.д.), создаваемый при нормальном (идеальном) функционировании некоторого информационного объекта.

*E* – эффективность функционирования объекта с учетом воздействия несанкционированного доступа.

*K* – коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объект.

*C* – стоимость средств защиты.

*ΔЕ* – величина, на которую несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования (нарушается нормальная работа, наносится ущерб из-за утечки информации и т.д.).

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».

Эффективность функционирования объекта с учетом воздействия несанкционированного доступа(2.1):

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

Относительная эффективность(2.2):

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

Обозначим снижение эффективности функционирования объекта при наличии средств защиты через ΔЕ3 (2.3), а коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объект – через К, тогда:

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

Найдём эффективность функционирования(2.4):

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

Найдём относительную эффективность функционирования(2.5):

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

Если эффективность функционирования объекта имеет стоимостное выражение (доход, прибыль и т.д.), то UΣ (суммарный ущерб объекту из-за затрат на установку средств защиты) непосредственно изменяет эффективность(2.6):

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

Таким образом, для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа имеет вид(2.7):

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

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.

**Вывод**: при решении поставленной задачи была вычислена относительная эффективность функционирования (0,99), так как она стремится к максимуму, можно утверждать, что все вычисления произведены правильно, и эффективность является целесообразной.

# **Практическое занятие №3**

## **Тема «Разработка информационной безопасности бизнес-компании»**

Цель: Разработать проект политики информационной безопасности бизнес-компании МобиРем.

**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.

Информационные ресурсы в современном обществе являются наиболее значимыми, но при этом, очень уязвимыми т.к. механизм их распространения становится все более гибким и количество возможностей их передачи растет. В связи с этим информационная безопасность — одно из важнейших условий функционирования любой структуры.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Беларуси. Поэтому решение вопроса об разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации. Вследствие этого, в дополнение к требованиям и рекомендациям стандартов, Конституции, законам и иным руководящим документам приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике методики международных стандартов, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации предприятия.

**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.

Ниже представлена организационная структура МобиРем (рис.1):

Структура управление компанией построена именно таким образом с целью обеспечения максимальной сегментации отделов и недопущения утечки данных сотрудникам, не имеющим прямого к ним отношения. Данная схема способствует обеспечению корректной работы внутри компании, защиты ее интересов, при этом соблюдая интересы клиентов, обеспечивая право на защищенность личных данных.

Проработка структуры демонстрирует четкую сегментацию на отделы, которые взаимодействуют между собой только через исполнительного директора и владельца бизнеса. Таким образом нагрузка на двух людей увеличивается, но зато обеспечивается максимальная защищенность персональных данных.

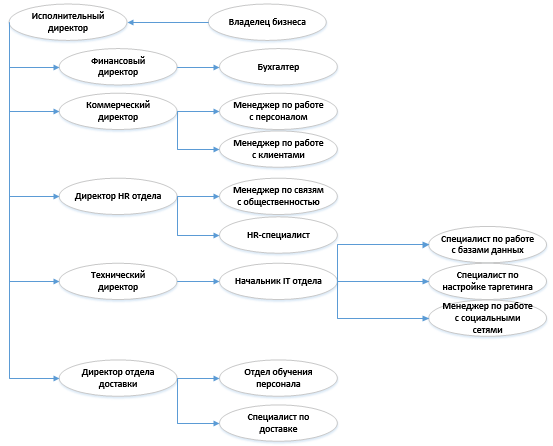


Рисунок 3.1 – Организационная структура бизнес-компании Мобирем

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. Оценка 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.

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 lipko-stadko.by 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 МобиРем 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 использования;
  + 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 в офис и на склад предметов, способных нанести ущерб.
  + Угроза доступа в эксплуатационный отдел, могут быть нарушены эксплуатационные планы.
  + Угроза доступа в ИТ-отделе.

**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.

При разработке политики безопасности можно была использована следующую модель (рис. 3.2), основанная на адаптации Общих Критериев (ISO 15408) и проведении анализа риска (ISO 17799).

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.

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.

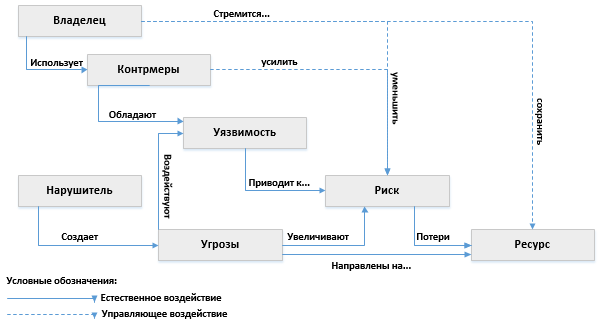


Рисунок 3.2. – модель построения корпоративной системы защиты информации.

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.

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.

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

* + вооруженная офисов компании;
  + четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
  + обязательная экстренная связь офиса с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
  + строгий подбор сотрудников с привлечением, при необходимости, без данных милиции;
  + защита главных серверов компании 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 в офисе наглядного отображения плана по работе во время чрезвычайных ситуаций.

Так же, эффективной мерой по защите является проведение тестовых экспериментов по атаке на фирму: наем специализированных людей, которые проведут атаку на сетевые ресурсы компании и выявят пробелы в защите. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.

**Выводы**

Приведенные меры по защите информации в торговой сети являются примерными. В реальности, следует провести комплексную оценку с привлечением специализированных людей, которые являются экспертами в вопросах обеспечения информационной безопасности для проведения специальных тестов и экспериментов.

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

* + вооруженная офисов компании;
  + четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
  + обязательная экстренная связь офиса с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
  + строгий подбор сотрудников с привлечением, при необходимости, без данных милиции;
  + защита главных серверов компании 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 в офисе 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.

# **Практическое занятие №4**

**Тема «Настройка Брандмауэра Windows»**

Цель: Овладение навыками настройки и использования Брандмауэра Windows.

Первым этапом необходимо включить брандмауэр

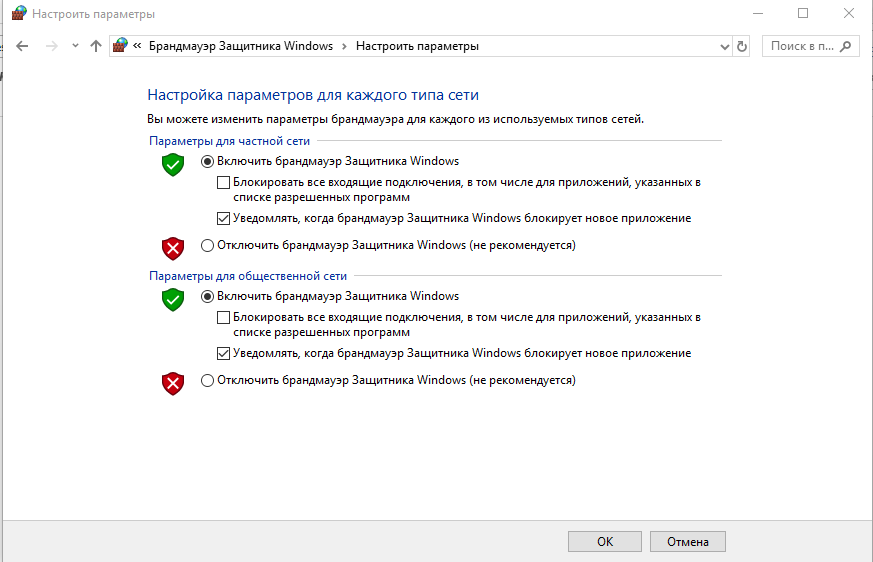


Рисунок 4.1 – Включение Брандмауэра.

Настройка правил для входящих подключений:

1. В открывшемся окне Брэндмауэра выбираем в левой панели правила для входящих подключений, затем во вкладке меню «Действие» выбираем «Создать правило», либо нажимаем «Создать правило» в правой панели.

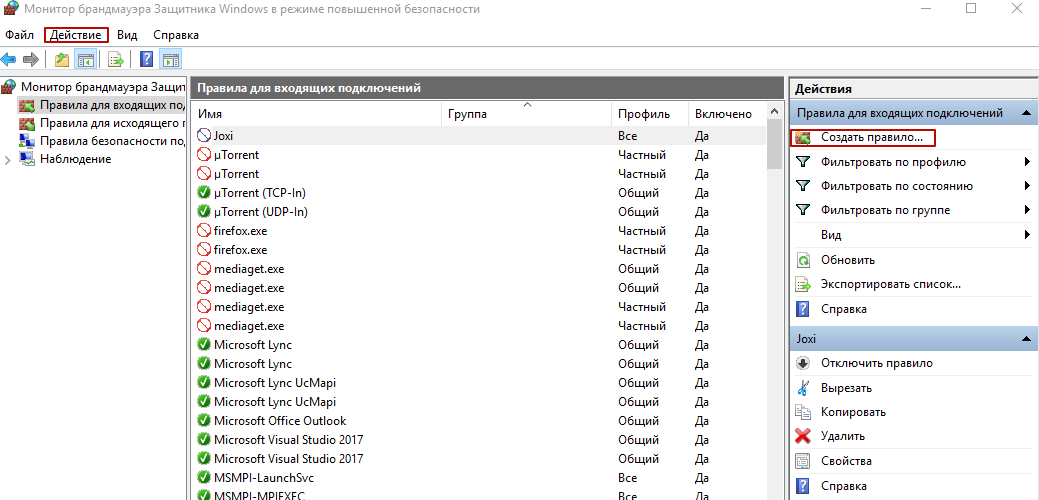


Рисунок 4.2 – Создание правила.

2. В открывшемся мастере создания правила выбираем «Для программы»

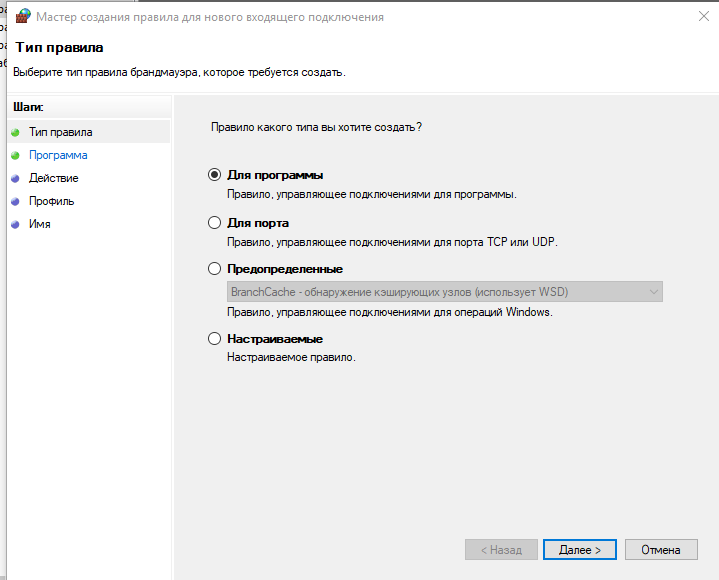


Рисунок 4.3 – Тип правила

3. Далее указываю её путь, через папку в которой она установлена.

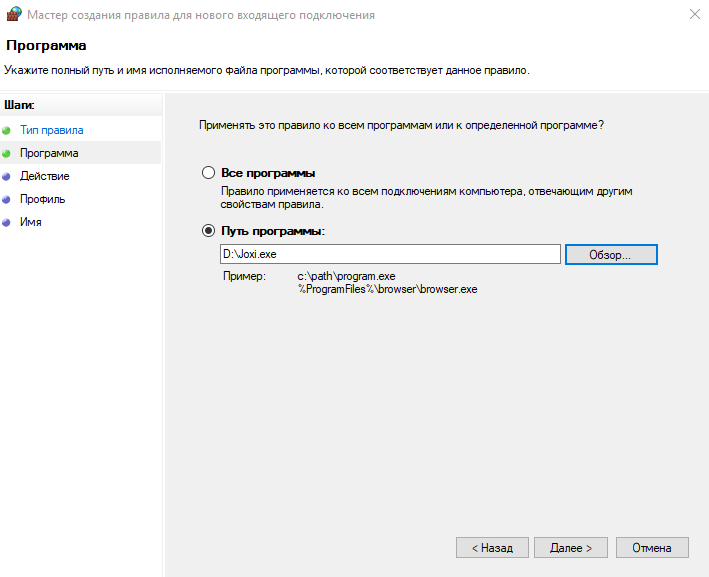


Рисунок 4.4 – Путь к программе

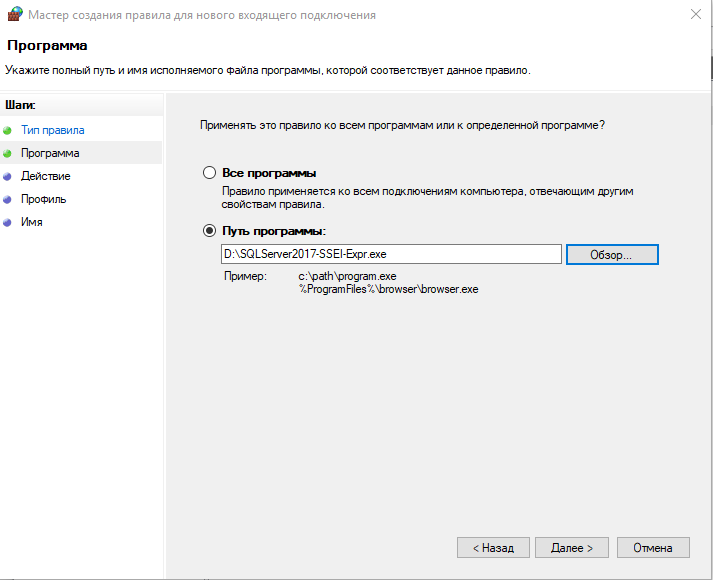


Рисунок 4.5 – Путь к программе

4. Далее я указала какое именно действие хочу применить. В данном случае “блокировать подключение”.

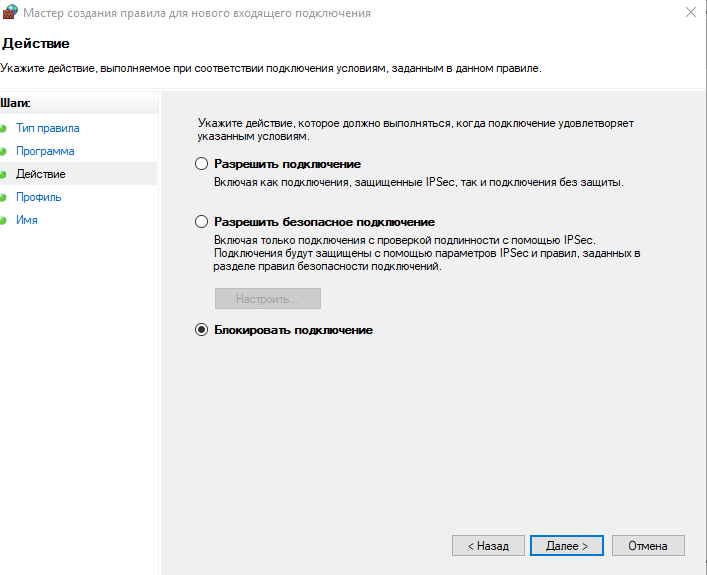


Рисунок 4.6 – Вид подключения

В данном – “разрешить подключение”.

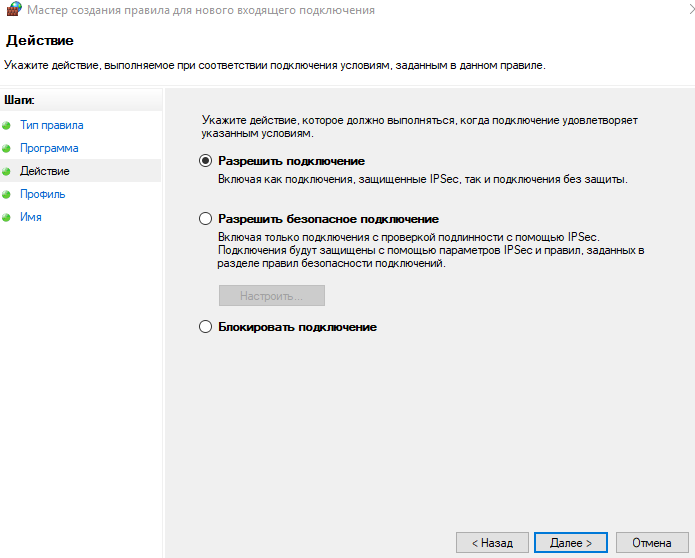


Рисунок 4.7 – Вид подключения

5. Далее указываю имя задаваемого подключения.

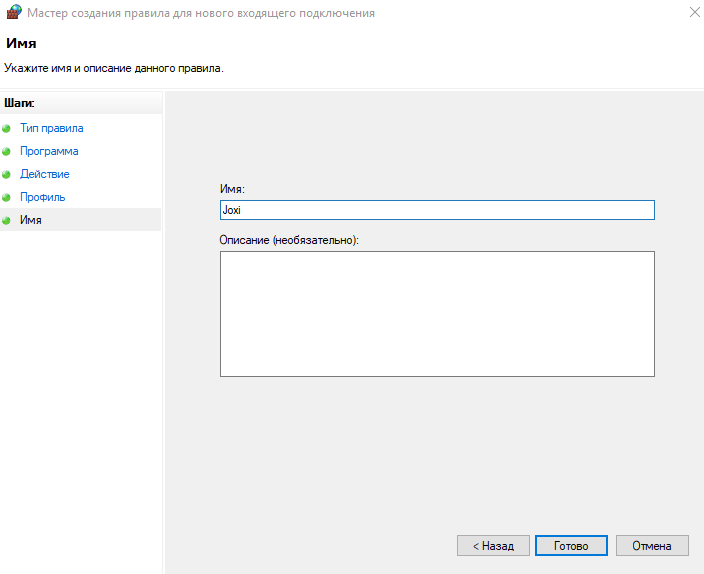


Рисунок 4.8 – Имя и описание программы

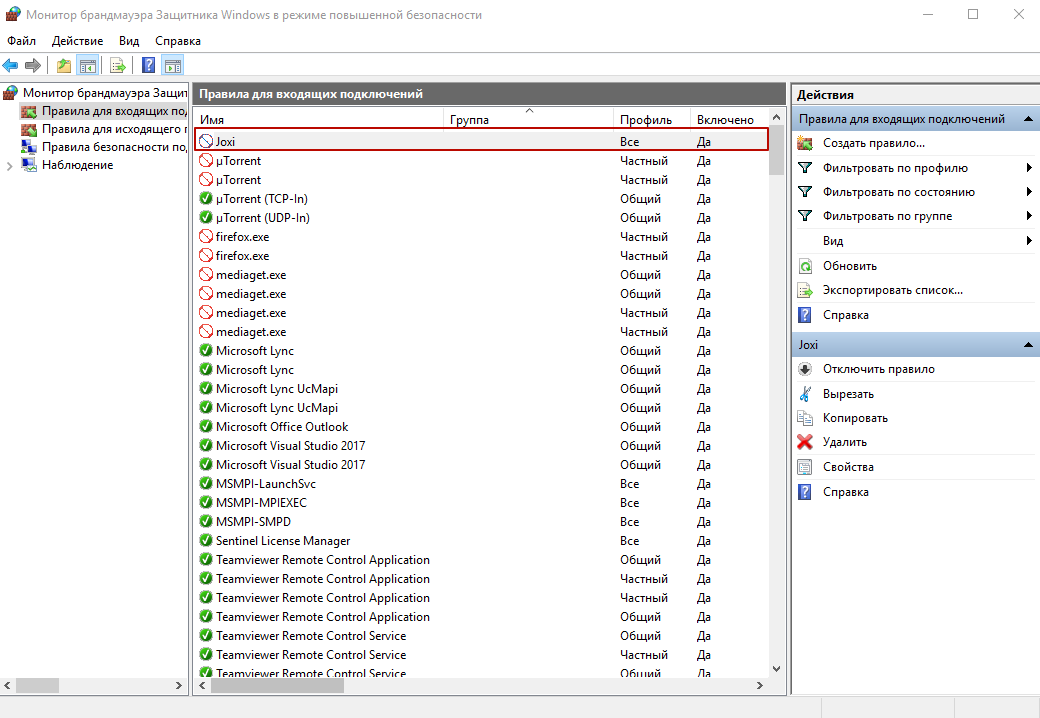
Результат: подключенный нами правила, добавлены к существующим 

Рисунок 4.9 – Правила для входящих подключений

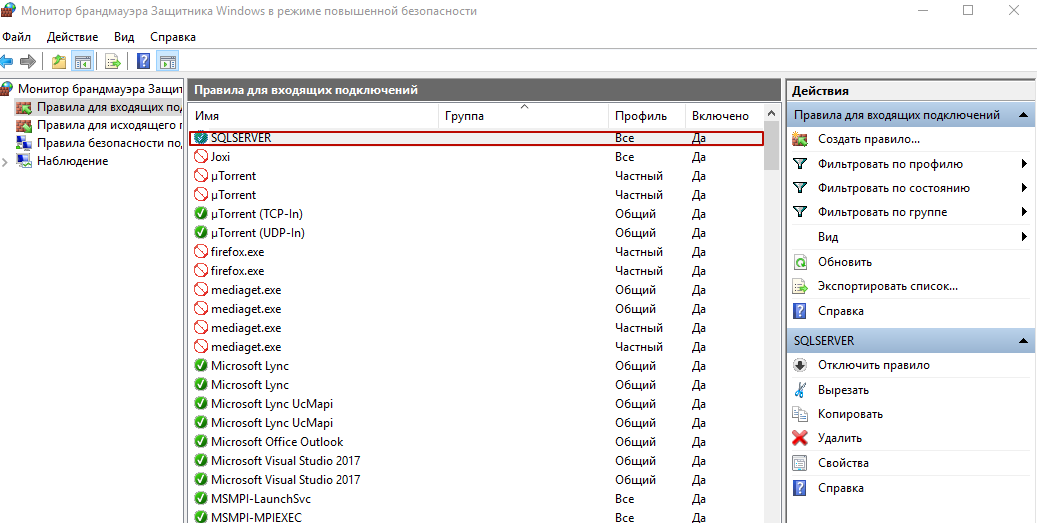


Рисунок 4.10 – Правила для входящих подключений

Так же 2-м щелчком по правой клавише мыши мы можем вызвать свойства для созданных нами правил

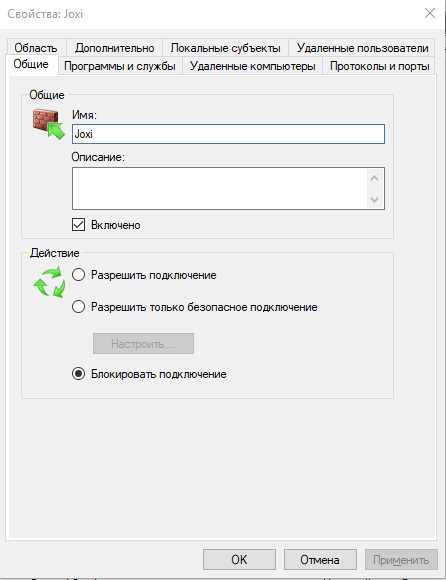


Рисунок 4.11 – Свойства созданного правила

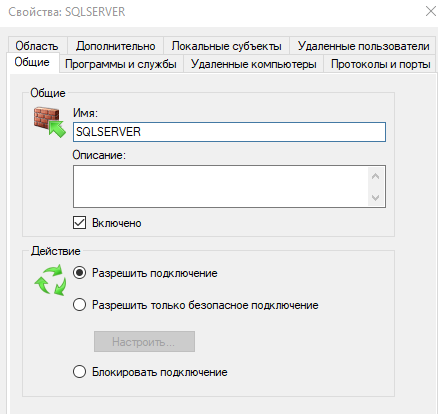


Рисунок 4. 12 – Свойства созданного правила

2.Правила для исходящих подключений ничем не отличаются от входящих. Единственное отличие - в открывшемся окне Брэндмауэра выбираем в левой панели правила для исходящих подключений

В открывшемся мастере создания правила выбираем «Для программы» Далее указываю её путь, через папку в которой она установлена

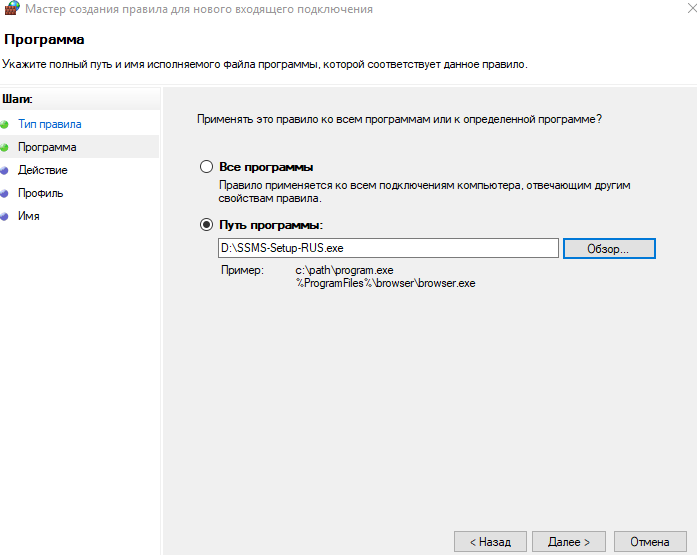


Рисунок 4. 13 – Путь программы

Указываю её путь, через папку в которой она установлена

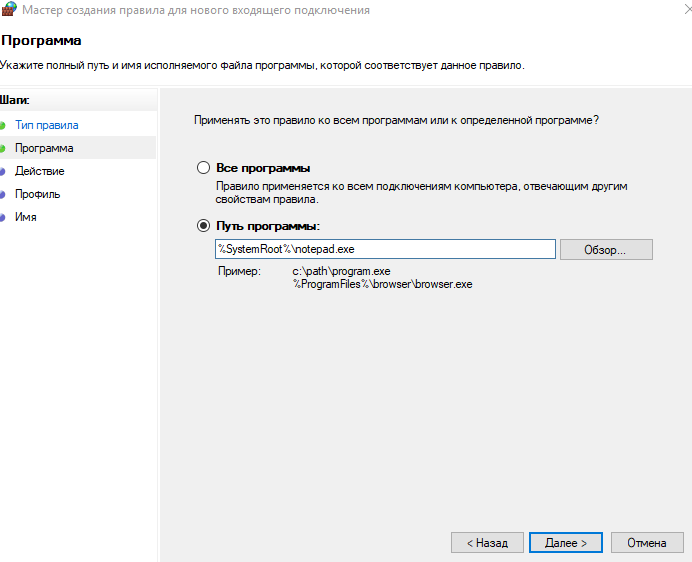


Рисунок 4. 14 – Путь программы

Далее я указала какое именно действие хочу применить. В данном случае “блокировать подключение”.

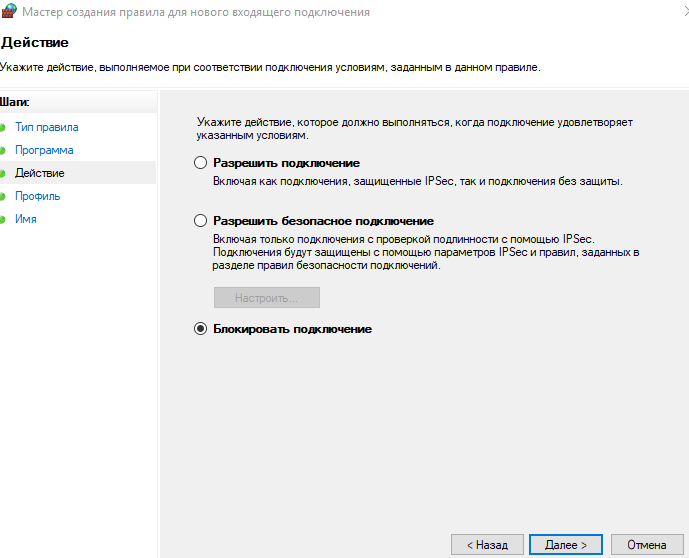


Рисунок 4.15 – Вид подключения

В данном – “разрешить подключение”.

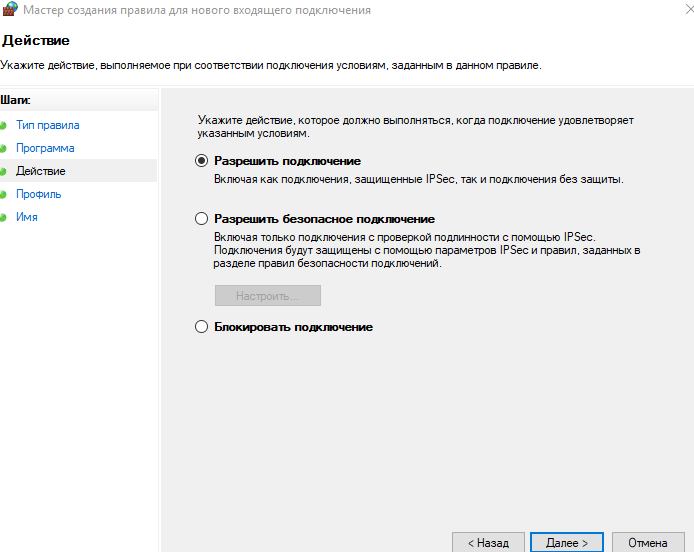


Рисунок 4.16 – Вид подключения

Далее указываю имя задаваемого подключения

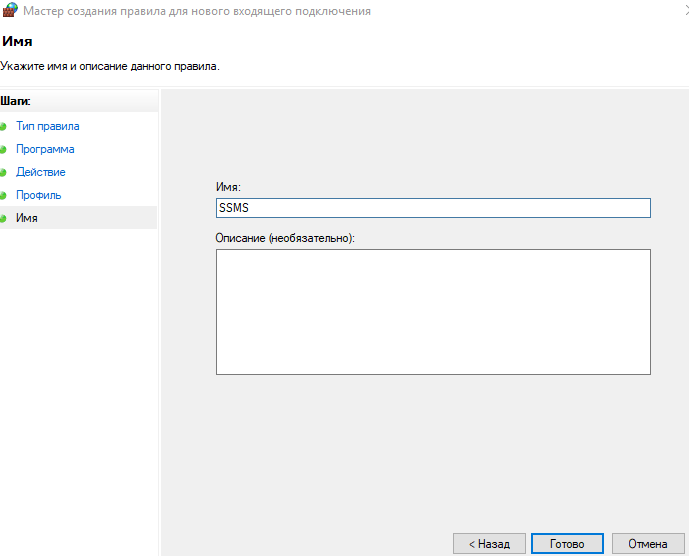


Рисунок 4.17 – Имя и описание программы

Указываю имя задаваемого подключения

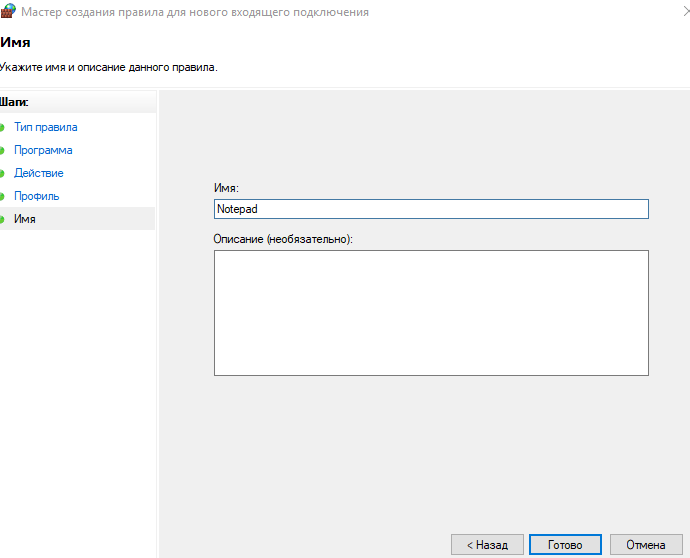


Рисунок 4.18 – Имя и описание программы

Так же 2-м щелчком по правой клавише мыши мы можем вызвать свойства для созданных нами правил

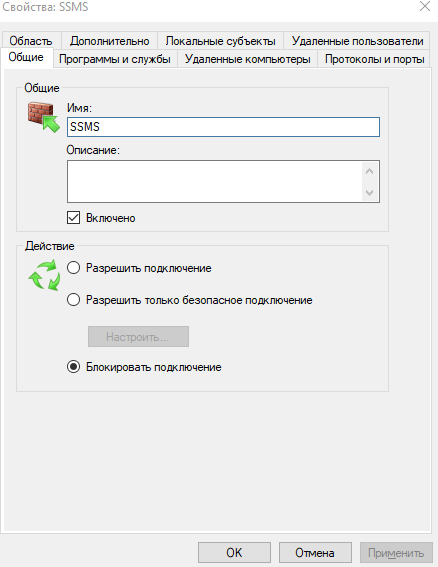


Рисунок 4.19 – Свойства созданного правила

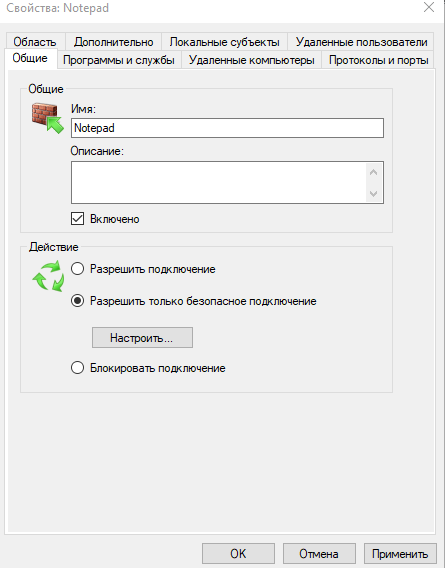


Рисунок 4.20 – Свойства созданного правила

**3. Вернуть настройки Брандмауэра в исходное состояниe**

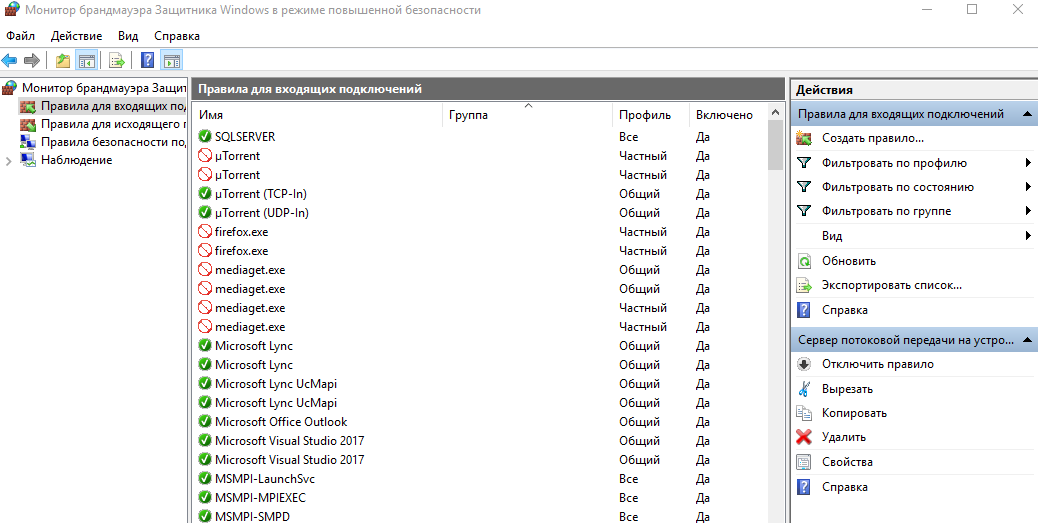


Рисунок 4.21 – Правила для подключений в исходном состоянии

Диспетчер проверки драйверов-verifier

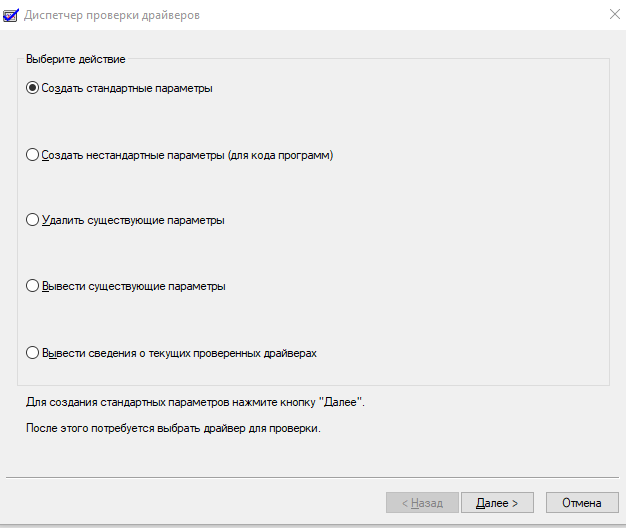


Рисунок 4.22 – Диспетчер проверки драйверов

Настройка системы-msconfig

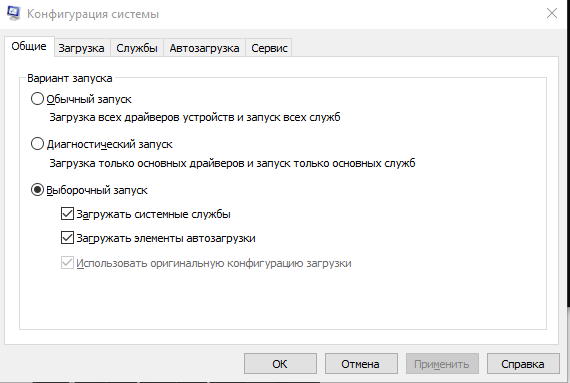


Рисунок 4.23 – Конфигурация системы

Просмотр событий-eventvwr.msc

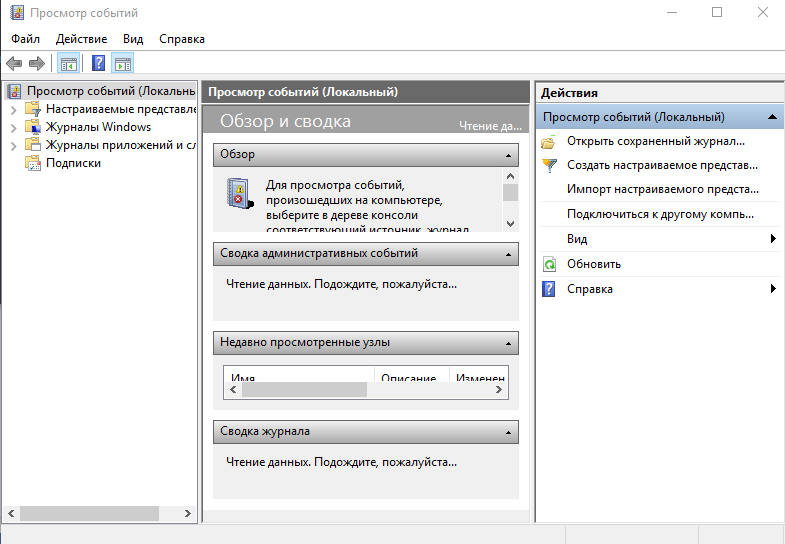


Рисунок 4.24 – Просмотр событий

Управление компьютером-compmgmt.msc

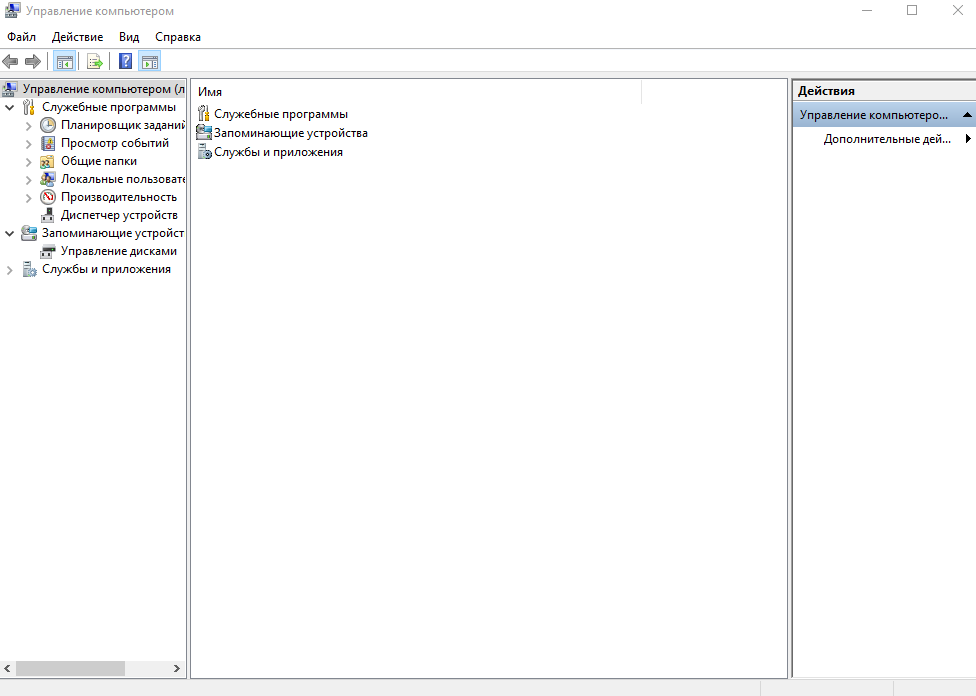


Рисунок 4.26 – Управление компьютером

Вывод: в случаи нарушения политики безопасности компьютера, брандмауэр блокирует входные и выходные потоки данных, проходящие через интернет или сеть.

# **Практическое занятие №5**

**Тема «Настройка антивирусов»**

Цель: Овладение навыками настройки и использования различных антивирусов.

**Ход работы:**

Открыла программу ESET NOD32 Smart Security. Открыла дополнительные настройки, нажав клавишу F5 на клавиатуре – Персональный файервол. Открылось окно расширенной настройки. В расположенном справа раскрывающемся меню Режим фильтрации выбрала нужный режим фильтрации.

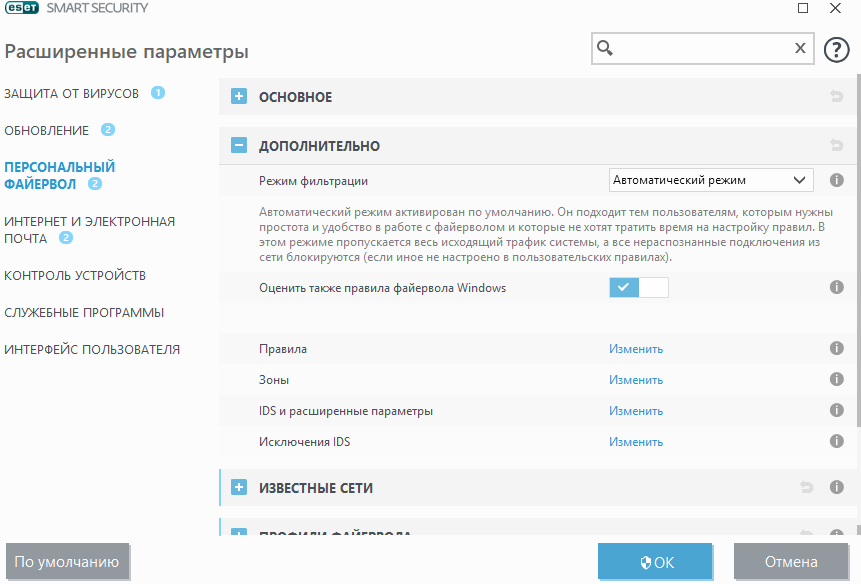


Рисунок 5.1 – Режим фильтрации

**Автоматический режим**

В автоматическом режиме сетевое взаимодействие автоматически контролируется параметрами, определенными пользователем.

**Интерактивный режим**

В интерактивном режиме сетевое взаимодействие анализируется в соответствии с заранее определенными правилами.

**Режим на основе политик**

В режиме на основе политик сетевое взаимодействие анализируется в соответствии с правилами, определенными администратором.

**Автоматический режим с исключениями**

Данный режим позволяет настроить вручную правила.

**Режим обучения**

Автоматическое создание и сохранение правил, предназначен для первоначальной настройки персонального брандмауэра.

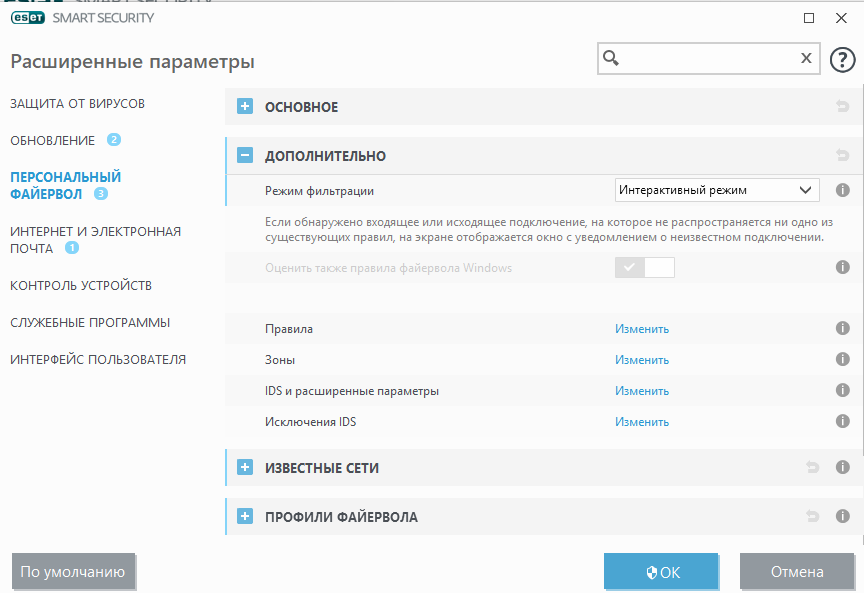


Рисунок 5.2 – Режим фильтрации

Оффлайн обновление NOD32 – обновление сигнатур угроз из локальной папки

Открыла главное окно NOD32. Нажала F5 для управления настройками NOD32 и выбрала пункт Обновление.

Обновление без подключения к сети Интернет возможно только для пользователей версии4.2

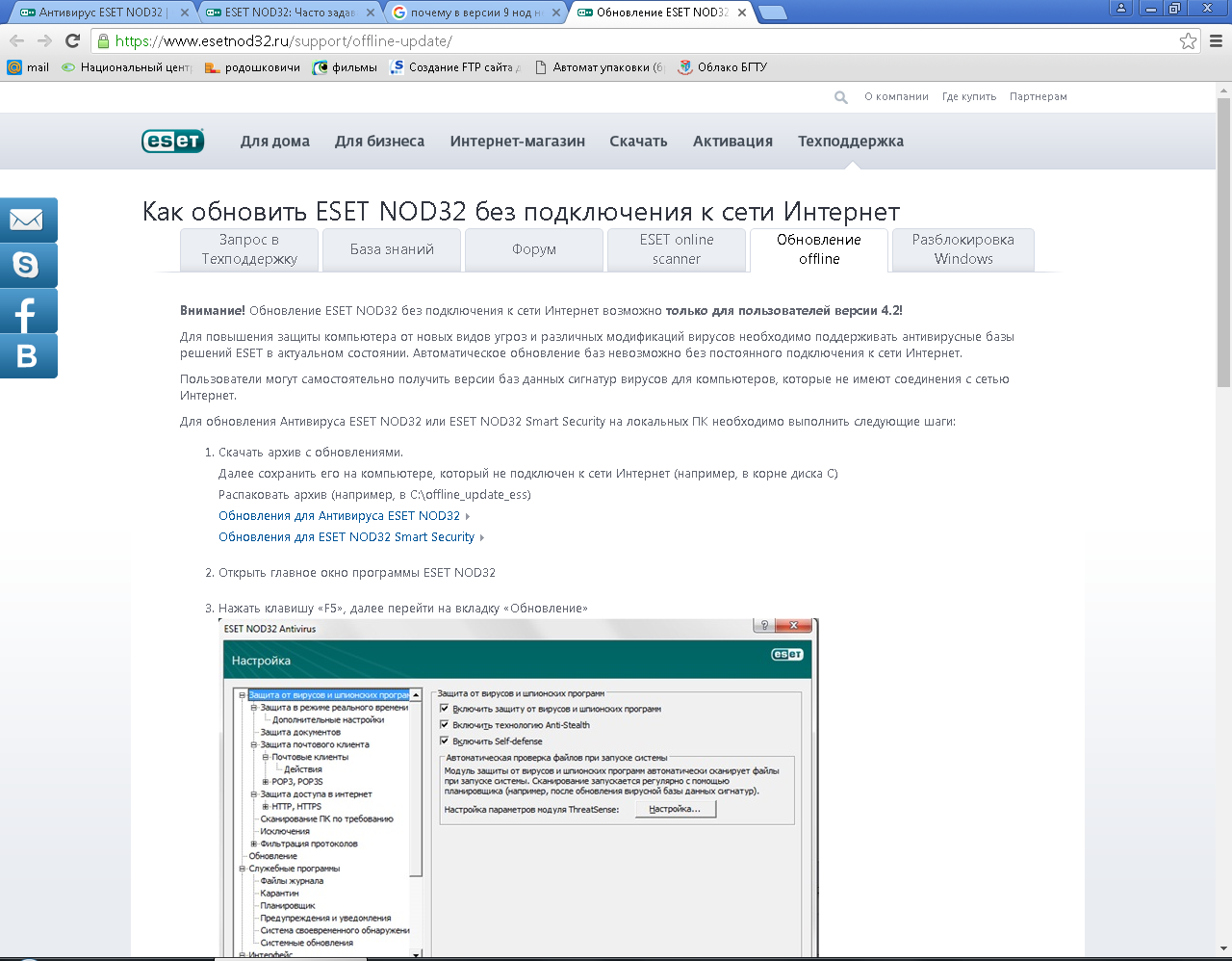


Рисунок 5.3 – Оффлайн обновление

В настройках обновления:

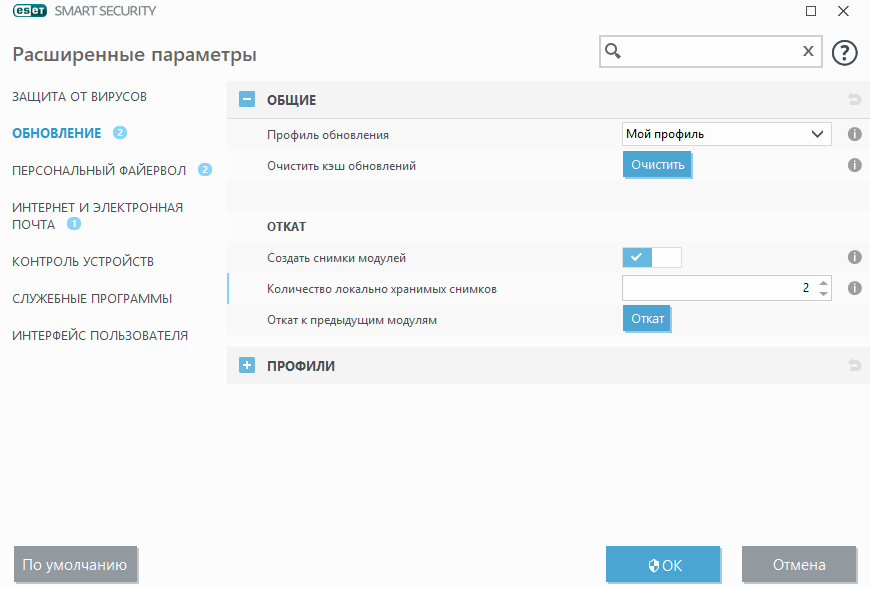


Рисунок 5.4 – Общие сведения

В обновлении смотрим раздел Основное.

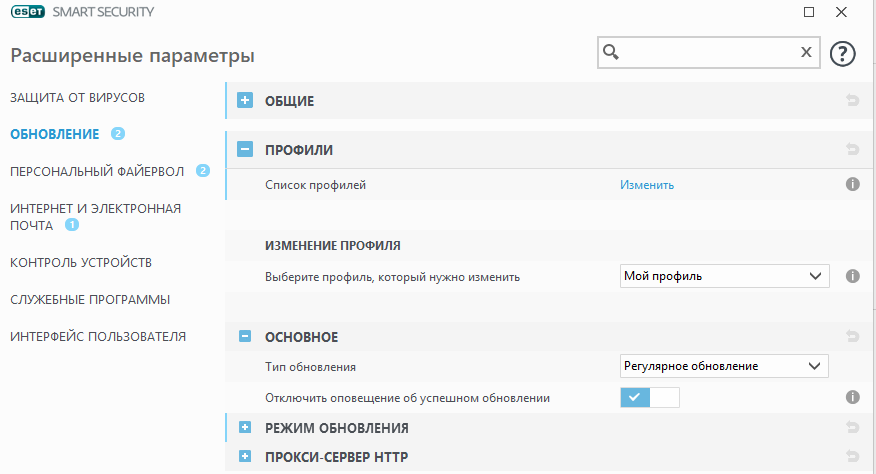
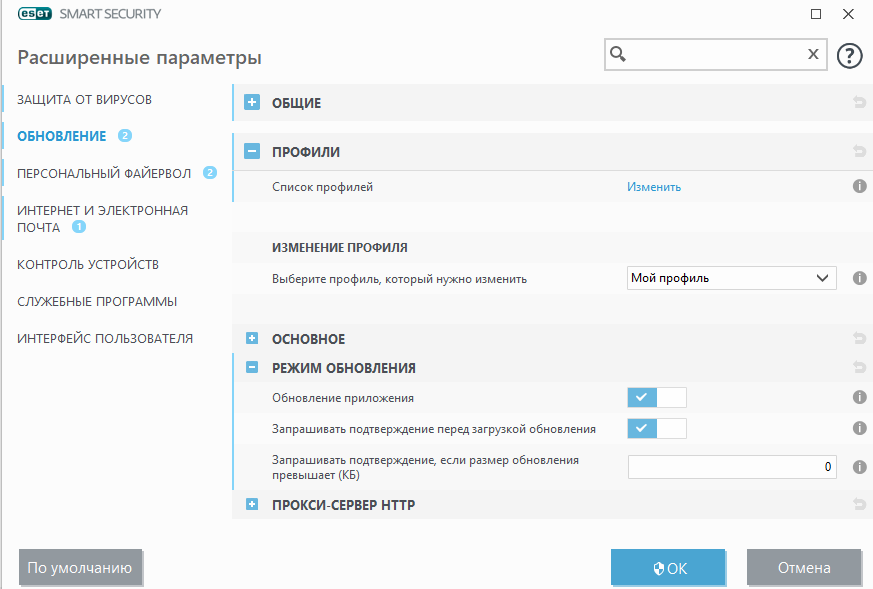
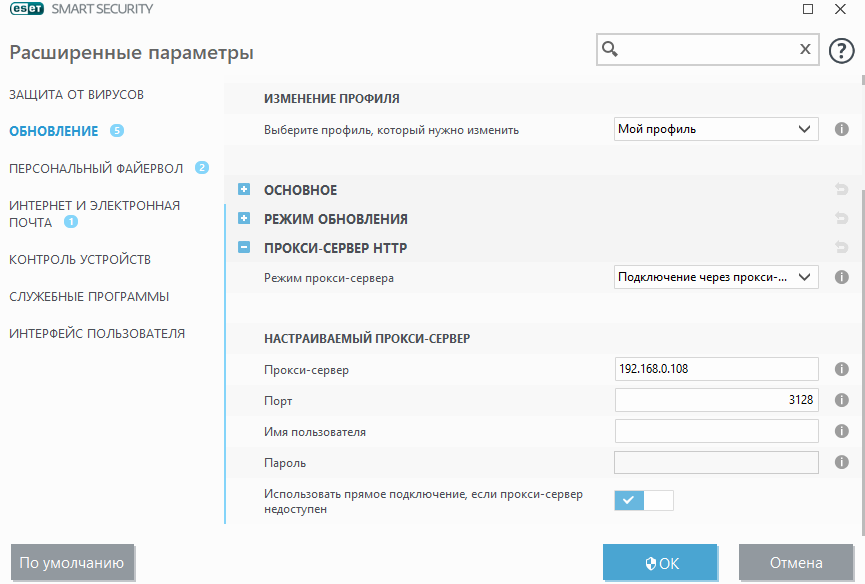


Рисунок 5.5 – Профили и основное

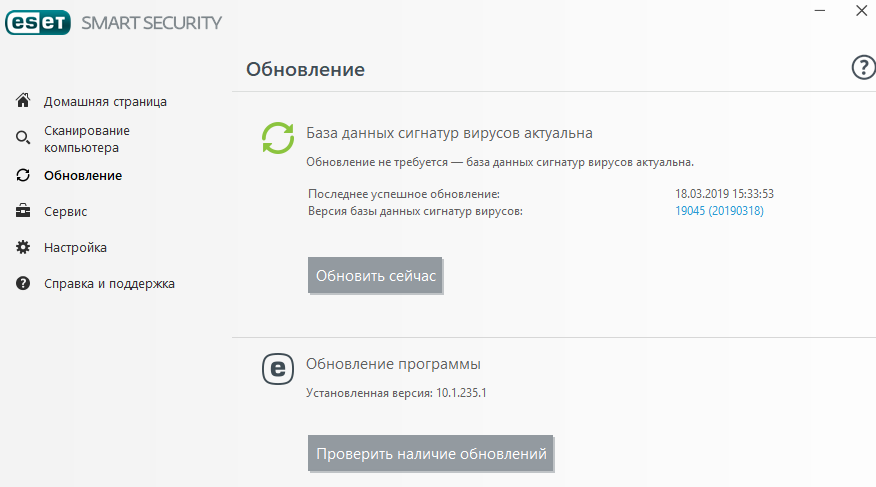
В обновлении смотрим раздел Режим обновления.

Рисунок 5.6 – Режимы обновления

В обновлении смотрим раздел Прокси сервер.

 Рисунок 5.7 – Прокси сервер

Обновление:

 Рисунок 5.8 – Обновление

Сервис:

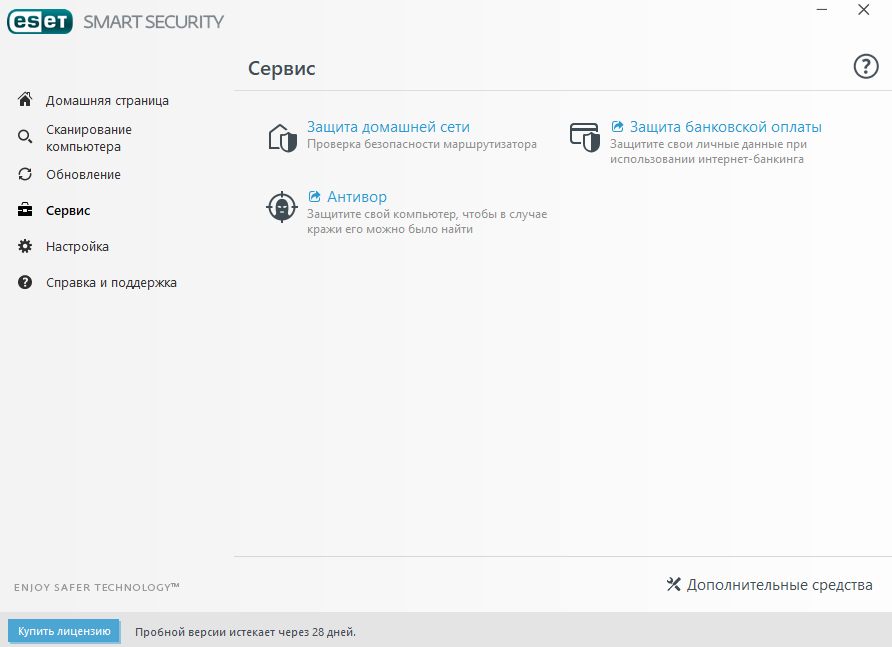


Рисунок 5.9 – Сервис

Вывод: изучила режимы работы файервола ESET NOD32 Smart Security. Обновила систему и изучила разделы данного файервола.

# **Практическое занятие №6**

**Тема «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.

С задачей подбора программного обеспечения для криптографической защиты данных сталкивается каждый, кто всерьез задумывается о безопасности своей конфиденциальной информации. И в этом нет абсолютно ничего удивительного - шифрование на сегодняшний день является одним из самых надежных способов предотвратить несанкционированный доступ к важным документам, базам данных, фотографиям и любым другим файлам.

Говоря о криптографических утилитах, нельзя не упомянуть и про бесплатное программное обеспечение. Ведь сегодня практически во всех областях есть достойные продукты, распространяющиеся совершенно свободно. И защита информации не является исключением из этого правила.

Проблема заключается в том, что для грамотного выбора необходимо понимать все аспекты работы криптографических продуктов. Этапы работы с утилитой True Crypt.

1. После установки программы, запускаем её и нажимаем на кнопку Create Volume. Выбираем место для создания раздела (может быть в файле, в разделе диска либо внутри дискового устройства).

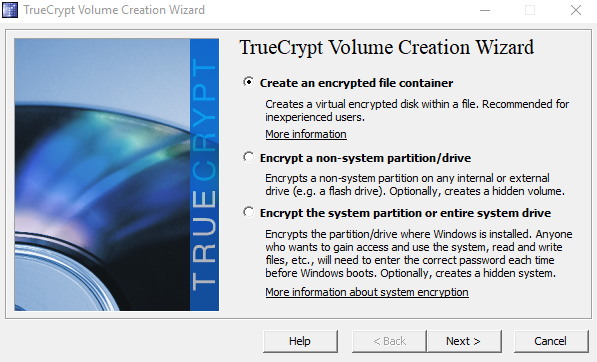


Рисунок 6.1 – Create Volume для создания раздела

1. Определение раздела: обычный или скрытый.

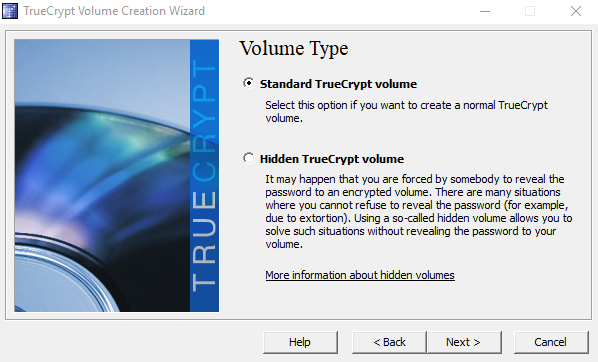


Рисунок 6.2 – Тип раздела

1. На следующем этапе выбираем место для создания раздела.

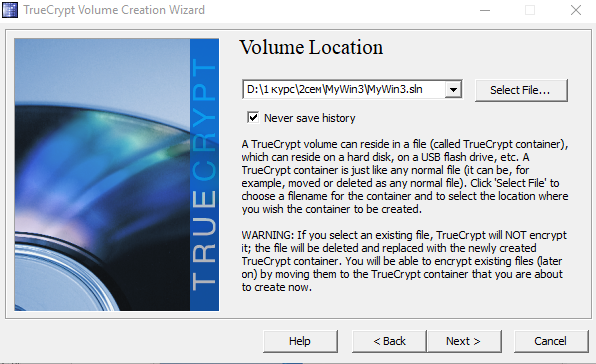


Рисунок 6.3 – Путь к разделу

1. Далее выбираем алгоритм для шифрования, а так же хеш – алгоритма предназначенного для раздела



Рисунок 6.4 – Алгоритм шифрования

1. Указываем предполагаемы размер контейнера (2 Мб, но можно и др.).

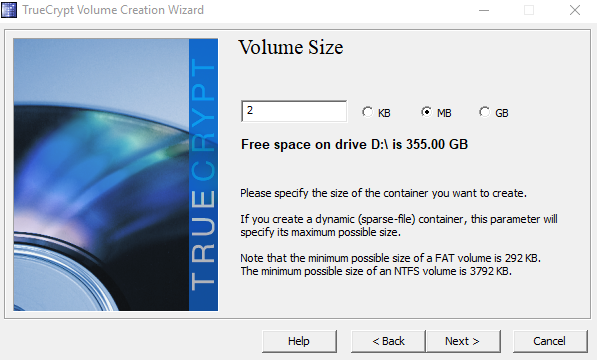


Рисунок 6.5 – Размер раздела

1. Ввод пароля и его подтверждение (пароль 123).



Рисунок 6.6 – Пароль для раздела

1. В этом окне следует двигать мышкой быстро и секунд 30. Это нужно для увеличения криптографических свойств ключей. Жмем Format и ждем завершения процесса создания раздела.

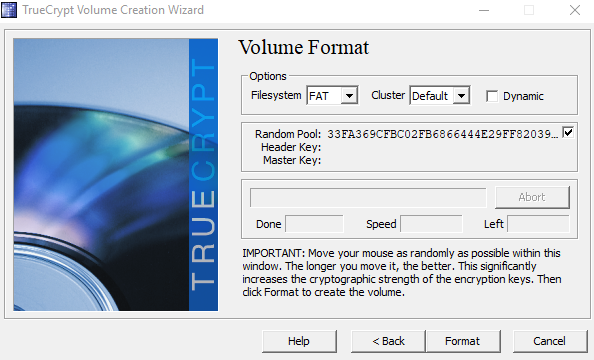


Рисунок 6.7 – Криптографический ключ

По окончанию видим:

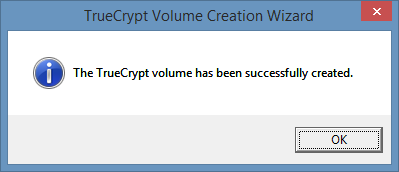


Рисунок 6.8 – Создан ключ

Жмем в окне Exit и выходим. Возвращаемся к главному окну.

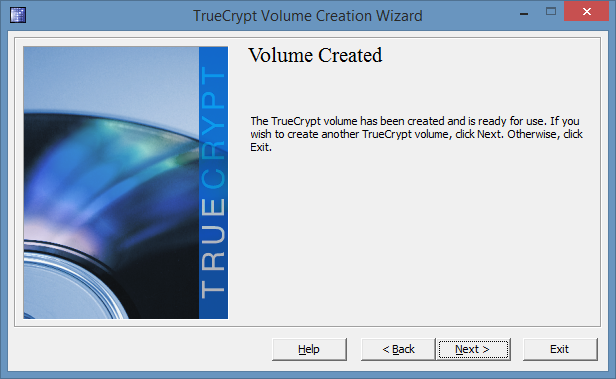


Рисунок 6.9 – Возвращаемся в меню

1. Выбираем букву, она будет названием диска к которому примонтируется контейнер.

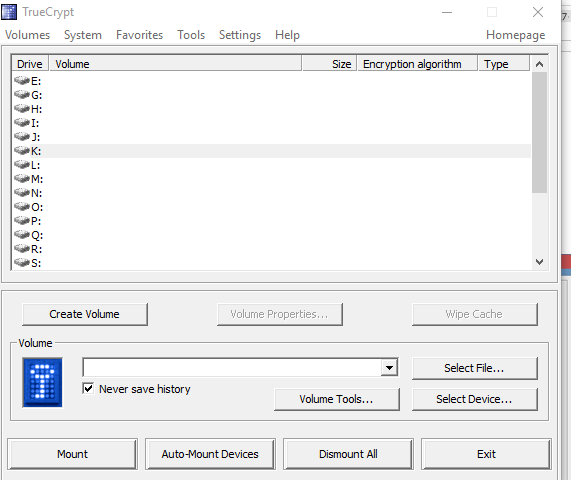


Рисунок 6.10 – Диски для контейнеров

1. Жмем Select File, и видим открывшееся окно, в котором выбираем файл.

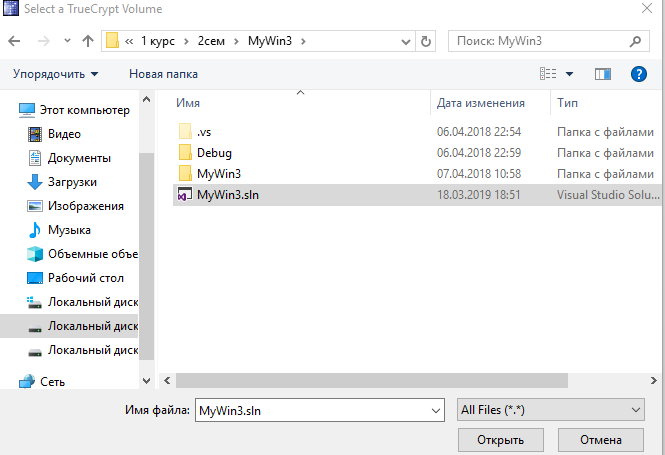


Рисунок 6.11 – Выбираем файл

1. В первоначальном окне жмем Mount. Появляется окно, запрашивающее пароль. Вводим пароль(123).

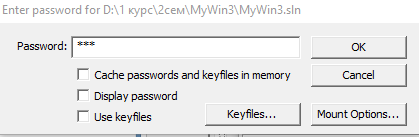


Рисунок 6.12 – Вводим пароль

1. Происходит монтировка на выбранный диск.

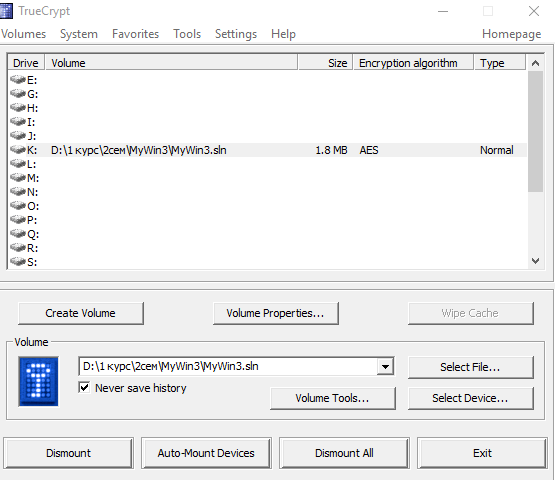


Рисунок 6.13 – Файл помещен в контейнер

1. Зайдя в раздел через Мой компьютер, можно увидеть тот самый диск, созданный ранее.

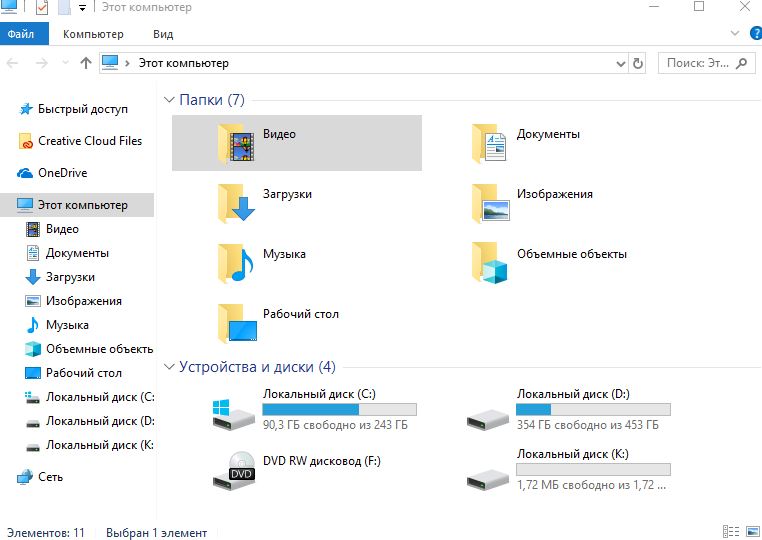


Рисунок 6.14 – Созданный раннее диск

13. Для закрытия и отказе в доступе к данным следует выбрать этот раздел и нажать кнопку Dismount.

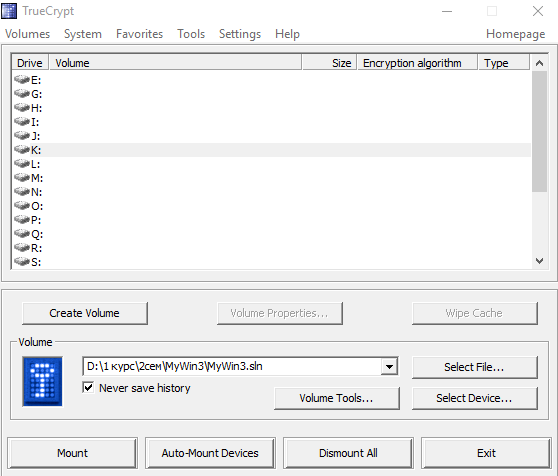


Рисунок 6.15 – Очищенный контейнер

Вывод: изучила программу для криптографической защиты информации при передаче и хранении. Рассмотрела в теории несколько видов криптографических программ и узнала какую лучше использовать для корпоративных клиентов, а что для домашнего использования. Из-за разницы в функционале большинство бесплатных программ не подойдут для использования в корпорациях, в частности, из-за возможности многопользовательской работы и использования более надежных алгоритмов шифрования.

# **Практическое занятие №7**

**Тема «Криптографическая защита информации»**

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

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

Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа.

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

Шифрованием называют процесс преобразования открытых данных в зашифрованные или зашифрованных данных в открытые по определенным правилам с применением ключей.

Классификация алгоритмов шифрования

1. Симметричные

1.1. Потоковые:

* + - с одноразовым или бесконечным ключом
    - с конечным ключом;
    - на основе генератора псевдослучайных чисел.

1.2. Блочные:

1.2.1. Шифры перестановки

1.2.2. Шифры замены:

* + - моноалфавитные;
    - полиалфавитные;

2. Асимметричные:

* + - Диффи-Хеллман
    - Райвест-Шамир-Адлeман
    - Эль-Гамаль.

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

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.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу.

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.

1. Реализуем пример генерации секретного ключа методом Диффи-Хеллмана:
   1. В качестве p и g взять два любых простых числа.
   2. Секретный ключ 1-го человека должен быть: номер варианта + 8.

|  |  |
| --- | --- |
| 1-й человек | 2-й человек |
| 1) открытое простое число p= 5; | 2) открытое простое число p= 5; |
| открытое простое число g= 2; | открытое простое число g= 2; |
| секретный ключ a=15+8=23; | секретный ключ b=7; |
| открытый ключ A = 223 mod 5= 3; | открытый ключ B = 27 mod 5 = 3; |
| секретный ключ s= 323 mod 5= 2; | cекретный ключ s = 37 mod 5=2; |
| S=2 | S=2 |

Таблица 7.1 – Генерация секретного ключа методом Диффи-Хеллмана

1. Зашифровать сообщение «хочузачетавтоматом» с использованием шифра Цезаря и полученного секретного ключа.



Рисунок 7.1 – Русский алфавит

Ключ 2: “чрщхйвщжфвдфровфро ”

Вывод: я изучила симметричный алгоритм шифрования «шифр Цезаря», и ассиметричный алгоритм «Диффи-Хелмана».

# **Практическое занятие №8**

**Тема «Криптографическая защита информации»**

Цель: Овладение навыками работы с известными криптографическими алгоритмами.

Ход работы:

1) Математические результаты, которые положены в основу этого алгоритма.

**Определение 1**. Сравнением целых чисел a и b будем называть соотношение между ними вида a = b + mk, означающее, что их разность (a – b) делится на заданное положительное число m, называемое модулем сравнения. При этом а называется вычетом числа b по модулю m.

**Определение 2**. Говорят, что два целых числа a и b сравнимы между собой и обозначают этот факт через a = b (mod m), если a и b имеют одинаковые остатки при делении на m.

Приведем некоторые очевидные свойства сравнений.

Пусть a = b (mod m) и с = d (mod m). Тогда:

1) *a (+-) c = b (+-) d (mod m),*

2) *a\*c (+-) b\*d (mod m).*

**Теорема 1.** (Малая теорема Ферма). Если p – простое число, то (x в степени (p – 1)) = 1 (mod p) для любого х, простого относи-тельно p, и (x в степени p) = х (mod p) для любого х.

**Определение 3.** Функцией Эйлеpа Ф(n) называется число положительных целых, меньших n и простых относительно числа n.

**Теорема 2.** Если n = pq, (p и q – отличные друг от друга простые числа), то Ф(n) = (p – 1)(q – 1).

**Теорема 3.** Если n = pq, (p и q – отличные друг от друга простые числа) и х – простое относительно p и q, то (x в степени Ф(n)) = 1 (mod n).

**В реальных системах RSA реализуется следующим образом:**

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.

Реализация примера шифрования сообщения:

Условие: Сообщение: DAA, p = 59, q = 43

1. n = p \* q =2537;
2. φ(n) = (p - 1) \* (q - 1) = 58 \*42 = 2436;
3. e = 5. Открытый ключ шифра – (e, n) – (5, 2537);
4. d = (k \* 2436 + 1) /5 = 1949, k = 4;
5. D-C = Te mod n = 45 mod 2537 = 92;
6. A-C = Te mod n = 15 mod 2537 = 2389;
7. Зашифрованное сообщение – 92 2389 2389;
8. Расшифровка происходит с помощью закрытого ключа – (d, n) по формуле T = Cd mod n;
9. T = 921949 mod 2537 = 4;
10. T = 23891949 mod 2537 = 1;
11. Расшифрованное сообщение – DAA

# **Практическое занятие №9**

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

**Цель:** Изучить основные положения авторского права и смежных прав.

1. **На какие объекты 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.).

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

Личные неимущественные права:

* признаваться автором произведения (право авторства);
* использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом либо без обозначения имени, т.е. анонимно (право на имя);
* обнародовать или разрешать обнародовать произведение в любой форме (право на обнародование), включая право на отзыв;
* право на защиту произведения, включая его название, от всякого рода искажении или любого иного посягательства, способных нанести ущерб чести и достоинству автора (право на защиту репутации автора).

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

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

* воспроизведение произведения;
* распространение оригинала или экземпляров произведения посредством продажи или иной передачи права собственности;
* прокат оригиналов или экземпляров компьютерных программ, баз данных, аудиовизуальных произведений, нотных текстов музыкальных произведений и произведений, воплощенных в фонограммах;
* импорт экземпляров произведения;
* публичный показ оригинала или экземпляра произведения;
* публичное исполнение произведения;
* передачу произведения в эфир;
* иное сообщение произведения для всеобщего сведения;
* перевод произведения на другой язык;
* переделку или иную переработку произведения.

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

Авторское право на составные произведения:

* Автору сборника и других составных произведений (составителю) принадлежит авторское право на осуществленные им подбор и распоряжение материалов как результат творческого труда (составительство).
* Составитель пользуется авторским правом при условии соблюдения им прав авторов каждого из произведений, включенных в составное.
* Авторы произведений, включенных в составное произведение, вправе использовать свои произведения независимо от составного произведения, если иное не предусмотрено авторским договором.
* Авторское право составителя не препятствует другим лицам осуществлять самостоятельный подбор и расположение тех же материалов для создания своих составных произведений.
* Лицу, выпускающему в свет энциклопедии, энциклопедические словари, периодические и продолжающиеся сборники научных трудов, газеты, журналы и другие периодические издания, принадлежат исключительные права на использование таких изданий в целом. Это лицо вправе при любом использовании таких изданий указывать свое наименование или требовать такого указания.

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

Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно. Имущественные права действуют в течение всей жизни автора (соавторов) и 50 лет после его (последнего соавтора) смерти. Переход авторского права по наследству, кроме прав авторства, на имя и на защиту репутации автора без ограничения срока.

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

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

1. **Что такое авторский договор?**

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.

1. **Наиболее распространенные виды авторских договоров?**

Наиболее распространенные виды авторского договора:

* изобретательский,
* постановочный,
* сценарный,
* художественного заказа,

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

1. **Основные составляющие авторского договора?**

Авторский договор должен предусматривать способы использования произведения (конкретные права, передаваемые по данному договору); срок, на который передается право, и территорию, на которую распространяется действие этого права на указанный срок; размер вознаграждения и (или) порядок определения размера вознаграждения за каждый способ использования произведения, порядок и сроки его выплаты, а также другие условия, которые стороны сочтут необходимыми.

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

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

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

Вознаграждение определяется в авторском договоре в виде процента от дохода за соответствующий способ использования произведения, или в виде твердо зафиксированной суммы, или иным образом. При этом ставки авторского вознаграждения не могут быть ниже минимальных ставок, устанавливаемых СМ РБ. Если в авторском договоре об издании или ином воспроизведении произведения вознаграждение определяется в виде твердо зафиксированной суммы, то в договоре должен быть установлен максимальный тираж экземпляров произведения.

**Практическое занятие №10**

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

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

1. **Основные составляющие описания изобретения?**

-область техники, к которой относится изобретение;

-уровень техники;

-сущность изобретения;

-перечень фигур чертежей, если они прилагаются с кратким указанием на то, что изображено на каждой из них. Если представлены иные материалы, поясняющие сущность изобретения, то перечисляют их;

-сведения, подтверждающие возможность осуществления изобретения.

1. **Правила оформления описания изобретения?**

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

1. **Какие основные пункты должна содержать заявка на изобретение?**

Заявка должна содержать документы:

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

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

Заявка подается в трех экземплярах и должна содержать:

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

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

На изобретение:

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

Заявка на выдачу патента:

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

Заявка на полезную модель:

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

Патент на полезную модель действует в течение пяти лет, считая с даты подачи заявки в патентный орган.

1. **На какие ОПС выдаются патенты?**

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

1. **На какие ОПС выдаются свидетельства?**

Топологии интегральной микросхемы.

# **Практическое занятие №11**

**Тема «Патентные исследования»**

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

**Задание для выполнения.**

**Задание 1**

Изучить виды, содержание и порядок проведения патентных исследований.

**Задание 2**

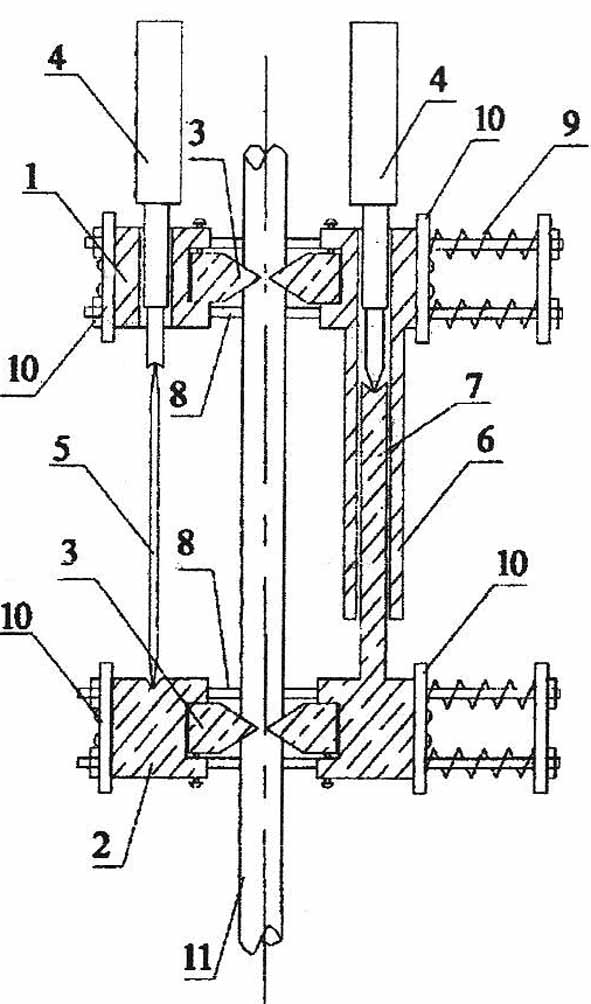
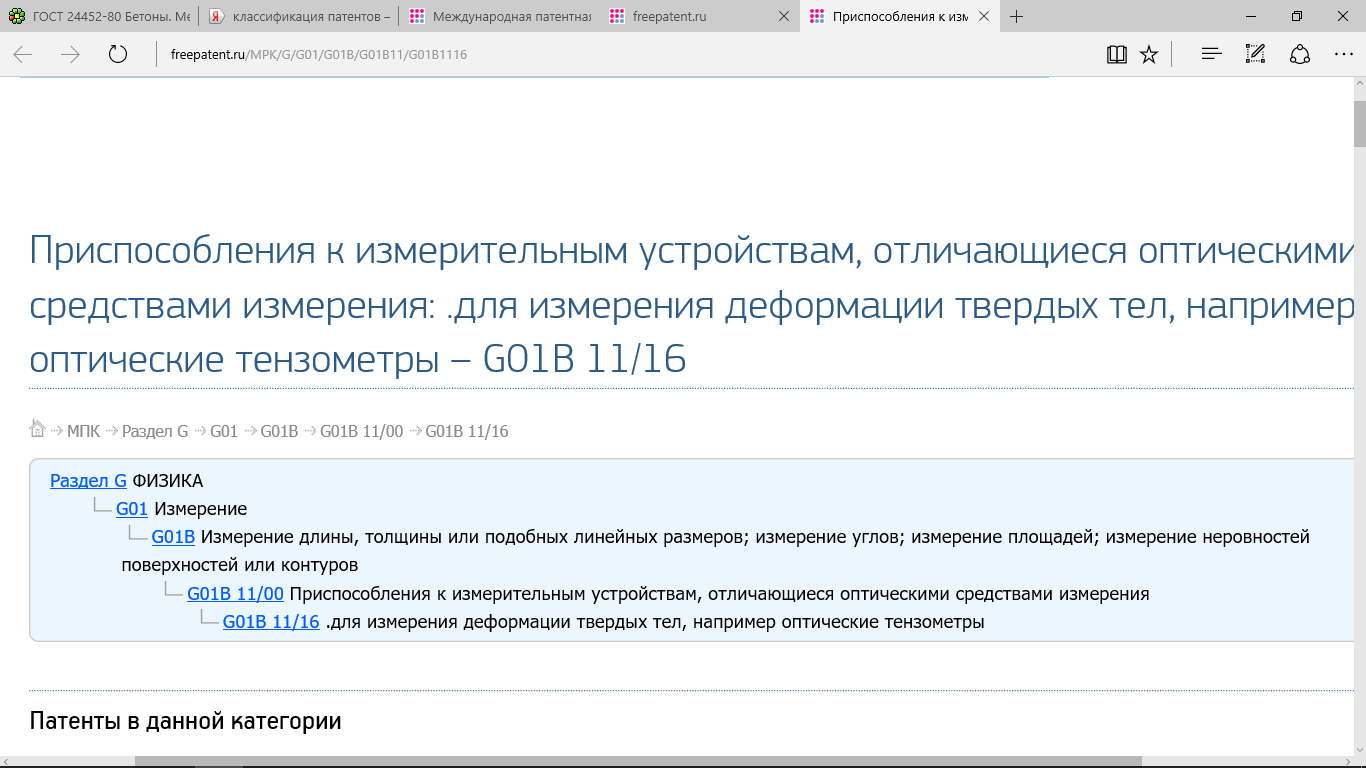


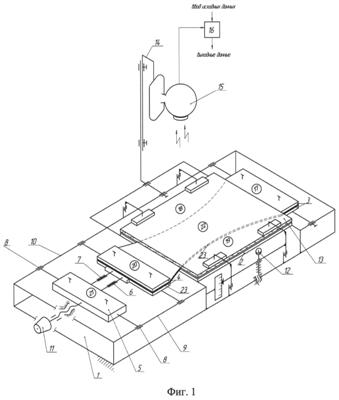
Рисунок 6 – Разработана конструкция приспособления (устройства) для измерения продольных деформаций изделий при их испытании на растяжение, отличающееся особенностями конструктивного расположения элементов

Изобретение относится к измерительной технике. Целью изобретения является повышение информативности путем определения формы поперечного сечения образца. Это устройство, содержащее рамку с установленными на ней индикаторами с измерительными штангами, вторую рамку с опорными площадками, предназначенными для взаимодействия с измерительными штангами, узлы крепления рамок на образце, отличающееся тем, что, с целью повьшения точности, каждый узел крепления рамок выполнен в виде разрезной втулки, жестко закрепленной в рамке, пустотелого стержня, расположенного внутри разрезной втулки с возможностью перемещения вдоль ее оси, профилированного упора, один конец которого предназначен для установки на образец , а другой размещен в пустотелом стержне с возможностью перемещения относительно него, и установленных в пустотелом стержне последователь (Л но с вторым концом профилированного упора пружины и регулировочного винта.

Следовательно, поиск аналогово нужно производить в данной группе:



Проведенный патентный поиск по указанному классу, выявил следующие аналогичные по конструктивному выполнению патенты и полезные модели, приведенные на рисунках 2 –3 :

[](http://www.freepatent.ru/images/patents/505/2507479/2507479.jpg)

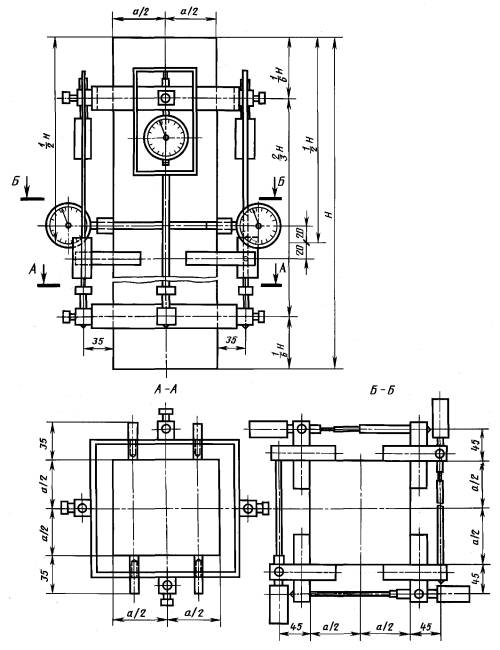
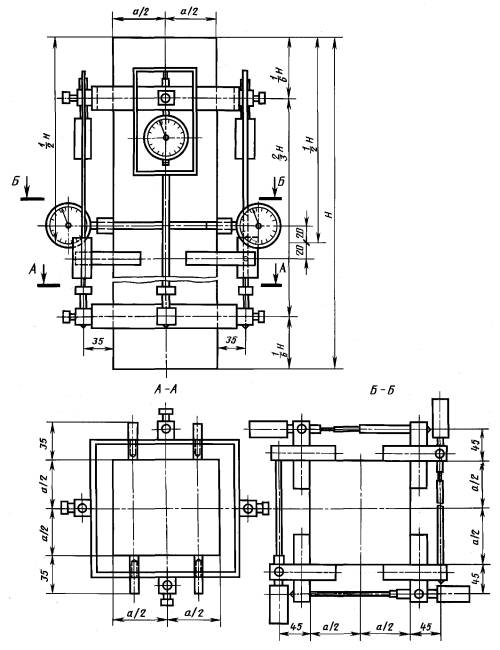
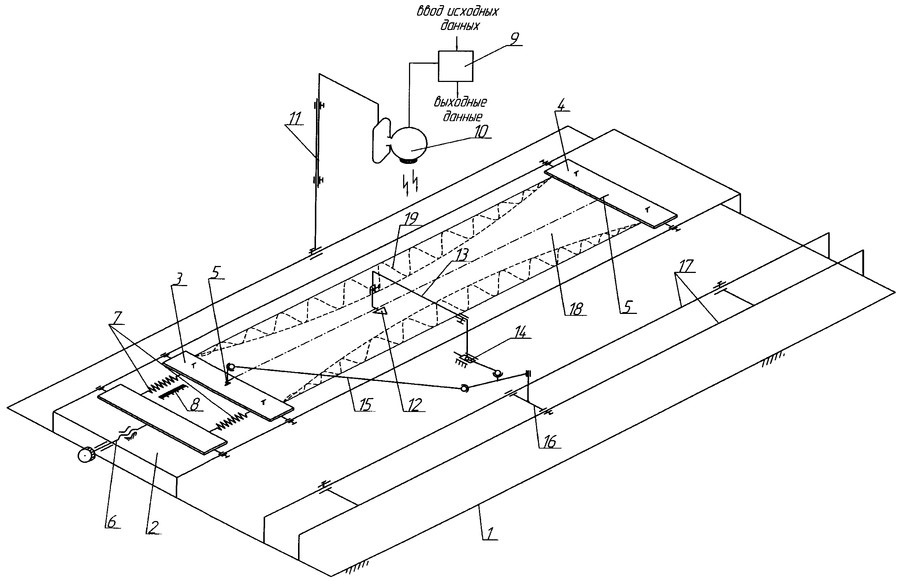


Рисунок 1– оптоэлектронное устройство для исследования деформационных характеристик волокнистых систем. Патент: 2507479

Автор: Железняков Александр Семенович, Шеромова Ирина Александровна, Старкова Галина Петровна, Королева Людмила Анатольевна



.

Рисунок 2– устройство для измерения продольной и поперечной деформации легкодеформируемых трикотажных полотен. Патент: № 2499257

Автор: Старкова Галина Петровна, Подшивалова Анна Викторовна

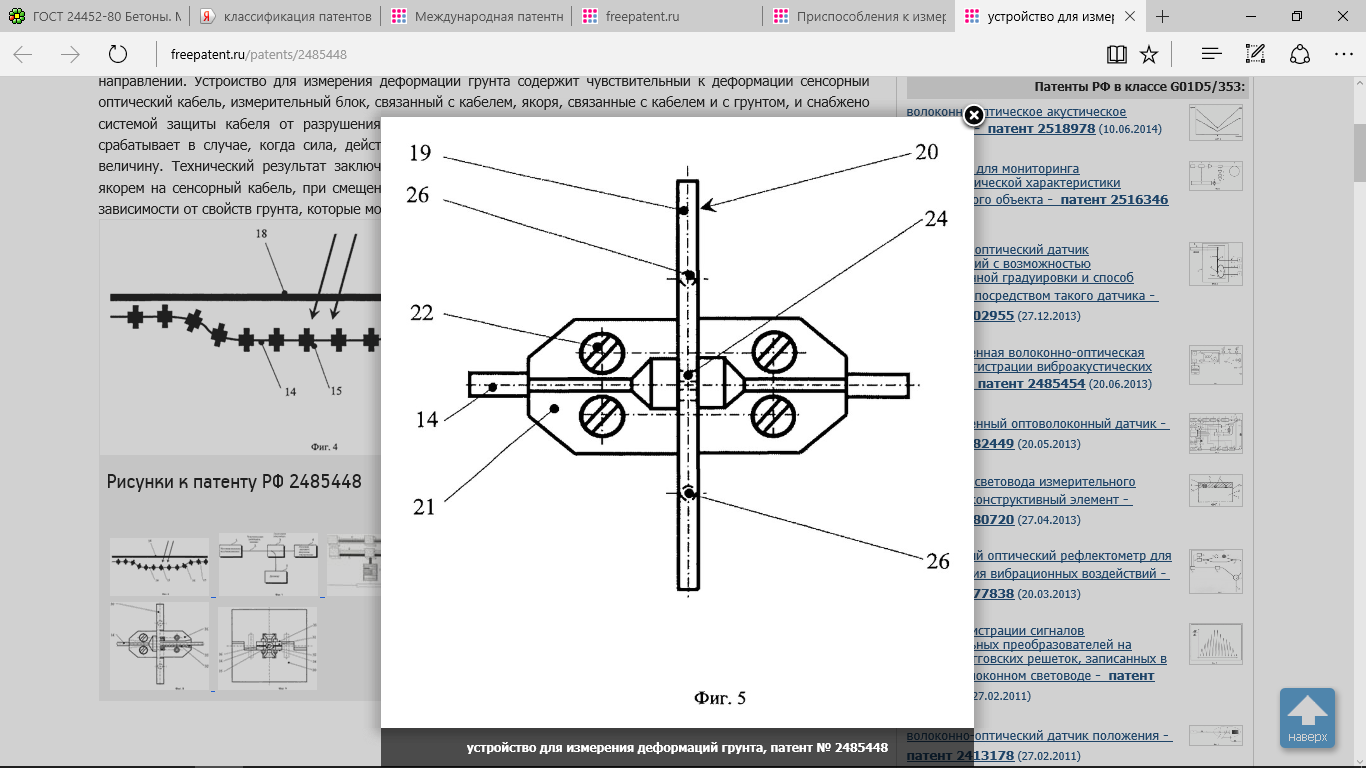


Рисунок 3­– устройство для измерения деформаций грунта.Патент: № 2485448

Автор: Наумов Александр Николаевич, Гречанов Александр Владимирович

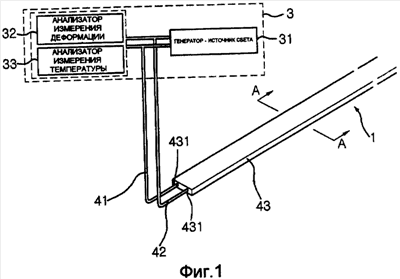
[](http://www.freepatent.ru/images/patents/71/2391625/2391625.jpg)

Рисунок 4– устройство и датчик для измерения деформации подземной трубы. Патент: 2391625

Автор: ЧАНГ Китае (KR)

Все данные по обнаруженным патентам-аналогам сводятся в соответствующую таблицу.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Предмет поиска (объект исследования, его составные части) | Страна выдачи, вид и номер охранного документа. Классификационный индекс | Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвенционный приоритет, дата публикации | Название изобретения (полезной модели, промышленного образца) | Сведения о действии охран-ного документа или причина его аннулирования (только для анализа патентной чистоты) |
| Устройства измерения деформации,  измерения  деформационных характеристик | Патент РФ  №2507479  МПК  G01B | Железняков Александр Семенович, Шеромова Ирина Александровна, Старкова Галина Петровна, Королева Людмила Анатольевна  подача заявки:2012-10-08  публикация патента:  20.02.2014 | оптоэлектронное устройство для исследования деформационных характеристик волокнистых систем | Действует |
| Патент РФ  № 2499257  МПК  G01B | Старкова Галина Петровна, Подшивалова Анна Викторовна  подача заявки:2012-06-01  публикация патента:  20.11.2013 | устройство для измерения продольной и поперечной деформации легкодеформируемых трикотажных полотен. | Действует |
| Патент РФ  № 2485448  МПК  G01B | Наумов Александр Николаевич,Гречанов Александр Владимирович  подача заявки:2013-04-03  публикация патента:  27.09.2014 | устройство для измерения деформаций грунта | Действует |
| Патент Китай  №2391625  МПК  G01B | Чанг ЭмДжи  подача заявки:2006-12-22  публикация патента:  10.06.2010 | устройство и датчик для измерения деформации подземной трубы | Действует |

Дальнейший анализ сущности обнаруженной патентной информации, выполняемой специалистами, позволяет определить наличие существенных отличий и возможность получения патента на изобретение или полезную модель.

# **Практическое занятие №12**

**Тема «Патентный поиск»**

Цель: освоить навыки проведения патентного поиска по заданной тематике. Провести патентный поиск по теме «Компьютерное программное средство для ситуационного управления виртуальным производственным комплексом».

По патентному поиску были обнаружены следующие варианты:

Название программы для ЭВМ: Среда управления виртуальными машинами

|  |  |
| --- | --- |
| Номер регистрации (свидетельства):[**2013661663**](http://www1.fips.ru/fips_servl/fips_servlet?DB=EVM&DocNumber=2013661663&TypeFile=html)  Дата регистрации: **12.12.2013**  Номер и дата поступления заявки:**2013619813 29.10.2013**  Дата публикации: [**20.01.2014**](http://195.208.85.205/Archive2/EVM/2014/2014.01.20/DOC/RUNW/000/002/013/661/663/document.pdf)  **Действует** | Авторы: **Гусарова Наталия Федоровна(RU)  Добренко Наталья Викторовна (RU)  Иванов Роман Владимирович (RU)  Решетников Виталий Витальевич (RU)**  Правообладатель: **федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (RU)**  Программа для ЭВМ создана по государственному контракту  государственный заказчик: **Министерство образования и науки РФ (RU)** |

**Реферат:**

Программа предназначена для поддержки решения образовательных задач и представляет собой web-сервис, позволяющий управлять виртуальными машинами в сети независимо от типа виртуальной машины и платформы виртуализации. Функционал программы: интерфейс регистрации серверов виртуализации; интерфейс регистрации пользователя; интерфейс взаимодействия с виртуальной машиной в составе; выбор виртуальной машины из списка; удаленные запуск/остановка/управление виртуальной машины через консоль доступа; клонирование виртуальной машины; создание новой виртуальной машины с управлением параметрами.

**Тип реализующей ЭВМ:** IBM PC-совмест. ПК

**Язык программирования:** С#

**Вид и версия операционной системы:** Windows Server 2008 R2

**Объем программы для ЭВМ:** 12,7 Мб

Название программы для ЭВМ: Программный комплекс «Система планирования (программный модуль «Расписание») и контроля (программный модуль «Диспетчерская») пассажирских перевозок» (ПК СПК ПП)

|  |  |
| --- | --- |
| Номер регистрации (свидетельства):[**2015619755**](http://www1.fips.ru/fips_servl/fips_servlet?DB=EVM&DocNumber=2015619755&TypeFile=html)  Дата регистрации: **14.09.2015**  Номер и дата поступления заявки:**2015616502 16.07.2015**  Дата публикации: [**20.10.2015**](http://195.208.85.205/Archive2/EVM/2015/2015.10.20/DOC/RUNW/000/002/015/619/755/document.pdf)  Контактные реквизиты:  **ips@ittrans.ru** | Правообладатель: **Общество с ограниченной ответственностью «Инвест Проект Сеть» (RU)** |

**Реферат:**

Программа является клиент-серверным приложением, предназначена для планирования и контроля исполнения пассажирских перевозок. Областью применения программы являются процессы управления перевозками многофилиальными хозяйствующими субъектами транспортной отрасли. Программа включает в себя взаимодействующие программные модули (ПМ): ПМ «Расписание», ПМ «Диспетчерская». Функциональные возможности: ПМ «Расписание»: автоматизированная разработка маршрутных расписаний с возможностью их корректировки на основе исходных данных о пассажиропотоках, паспортах маршрутов, пробегах с ведением истории их изменений, формирование отчетов по планируемым эксплуатационным показателям маршрутов и предприятиям; ПМ «Диспетчерская»: ввод, хранение и обработка информации, характеризующей фактическую работу подвижного состава с детализацией до каждого выхода: выпуск на линию, переключения, задержки движения, увеличенные интервалы, браки, формирование требуемой отчетности. Хранение и обработка данных реализована на СУБД "Oracle".

**Тип реализующей ЭВМ:** IBM РС - совмест. ПК, Apple Macintosh

**Язык программирования:** С++, Java, Perl

**Вид и версия операционной системы:** Windows, Linux, MacOS

**Объем программы для ЭВМ:** 95 Мб

Название программы для ЭВМ: Программный комплекс «Система контроля автомойки»

|  |  |
| --- | --- |
| Номер регистрации (свидетельства):[**2013612267**](http://www1.fips.ru/fips_servl/fips_servlet?DB=EVM&DocNumber=2013612267&TypeFile=html)  Дата регистрации: **20.02.2013**  Номер и дата поступления заявки:**2012661647 27.12.2012**  Дата публикации: [**20.03.2013**](http://195.208.85.205/Archive2/EVM/2013/201301/DOC/RUNW/000/002/013/612/267/document.pdf)  **Действует** | Авторы: **Не указаны**  Правообладатель: **Синицын Сергей Александрович (RU)** |

**Реферат:**

Программа предназначена для дистанционного осуществления функций контроля за деятельностью предприятия, такого как автомойка, с одновременным управлением технологическими процессами. Программа используется администратором автомойки для приема заказов от клиентов, ввода информации в базу данных системы, а также логически управляет включением/выключением набора оборудования через контроллеры на основании информации, полученной от набора датчиков. Программа осуществляет функции контроля и учета количества обслуживаемого транспорта, видов и количества оказанных услуг, потраченного времени на оказание данных услуг, учета расходных материалов. Удаленный доступ к управлению программой находится у владельца автомоечного комплекса. Позволяет дистанционно управлять принадлежащим ему предприятием, получать всевозможные виды отчетов, изменять параметры и регламенты логического управления оборудованием. Программный комплекс позволяет разделить виды услуг на несколько категорий, например, мойка, кафе, магазин, шиномонтаж.

**Язык программирования:** Java, SQL, XML, ActionScript

**Объем программы для ЭВМ:** 4 Мб

Название программы для ЭВМ: Тренажер на базе модели деятельности дирекции инновационного развития промышленного предприятия

|  |  |
| --- | --- |
| Номер регистрации (свидетельства):[**2013612882**](http://www1.fips.ru/fips_servl/fips_servlet?DB=EVM&DocNumber=2013612882&TypeFile=html)  Дата регистрации: **15.03.2013**  **Действует**  Номер и дата поступления заявки:**2013610348 22.01.2013**  Дата публикации: [**20.06.2013**](http://195.208.85.205/Archive2/EVM/2013/201302/DOC/RUNW/000/002/013/612/882/document.pdf)  Контактные реквизиты: [**t.pracapovich@rane.ru**](mailto:t.pracapovich@rane.ru)  **Действует** | Правообладатель: **Российская Федерация, от имени которой выступает Министерство промышленности и торговли Российской Федерации (RU)** |

**Реферат:**

Программа предназначена для применения в образовании и позволяет комплексно в краткий срок и в удаленном режиме освоить необходимый образовательный материал. Пользователи принимают решения по управлению виртуальным предприятием в аспекте инноваций и технологий. Программа рассчитывает состояние предприятия в соответствии с принятыми решениями, а также заложенным сценарием и предоставляет участникам управленческую отчётность. Программа обеспечивает пользователю следующие возможности: доступ пользователей к упорядоченной и систематизированной управленческой отчетности; доступ пользователей к принятию управленческих решений: формы ввода данных; настройка программы - регистрация и управление участниками, общая настройка системы, запуск учебных сессий.

**Язык программирования:** РНР 5.3

**Объем программы для ЭВМ:** 703 Кб

# **Практическое занятие №13**

**Тема «Регистрация компьютерных программ в Национальном центре интеллектуальной собственности»**

Цель: Овладеть навыками подготовки документации для регистрации компьютерных программ.

|  |  |
| --- | --- |
| В Национальный центр  интеллектуальной собственности  220034, г. Минск, ул. Козлова, 20 | дата поступления и рег. № (присваивается при необходимости): |
|  |

**ЗАЯВКА**

**на оказание услуг по регистрации компьютерной программы**

|  |  |  |
| --- | --- | --- |
| 1. Заявитель   /ФИО физического лица, полное наименование юридического лица/ | Полынская Юлия Викторовна | |
| просит Национальный центр интеллектуальной собственности оказать услуги по регистрации компьютерной программы в соответствии с нижеприведенными данными | | |
| 1. Вид услуг   /отметить знаком «Х» нужное/ | Х | Стандартная регистрационная процедура (заявитель является автором) |
|  | Стандартная регистрационная процедура (заявитель не является автором) |
|  | Ускоренная регистрационная процедура  (заявитель является автором) |
|  | Ускоренная регистрационная процедура  (заявитель не является автором) |
| Х | Оформление дополнительного экземпляра свидетельства |
| Х | Оформление дополнительного экземпляра свидетельства на английском языке |
|  | Оформление изменений в отношении ранее зарегистрированной компьютерной программы |
| 1. Название компьютерной программы | Электронный журнал для ВУЗа/BSTU journal | |
| 1. Год создания компьютерной программы | 2019 | |
| 1. Авторы компьютерной программы   /ФИО автора(ов), дата (число/месяц/год) рождения/ | Полынская Юлия Викторовна, 27.02.2000 | |
| 1. Правообладатель компьютерной программы   /ФИО физического лица, полное наименование юридического лица/ | Полынская Юлия Викторовна | |
| 1. Основание принадлежности исключительного права на компьютерную программу   /отметить знаком «Х» нужное/ | Х | Создание компьютерной программы |
|  | Переход исключительного права в порядке служебного произведения |
|  | Приобретение исключительного права по договору |
|  | Правопреемство (в т.ч. наследование) в отношении исключительного права |
| 1. Данные для заключения договора на оказание услуг по регистрации компьютерной программы   /полный (юридический) адрес, банковские реквизиты Заявителя; для организаций – лицо (ФИО и должность), уполномоченное на заключение договора (ссылка на документ); данные о лице, уполномоченном на ведение дел по договору - ФИО контактные данные – тел., эл. почта/ |  | |
| 1. Перечень прилагаемых материалов (с указанием носителя, кол-ва листов и т.д.)   /**обязательно** – экземпляр компьютерной программы, описание компьютерной программы, документы (заверенные копии), подтверждающие принадлежность исключительного права, при подаче Заявки через представителя – документ, подтверждающий полномочия представителя, **дополнительно** – на усмотрение заявителя/ |  | |
| Заявитель подтверждает свое понимание того, что регистрация компьютерной программы, о проведении которой просит Заявитель: 1) не является основанием или условием возникновения и осуществления авторского права на компьютерную программу, 2) осуществляется по инициативе Заявителя на основании предоставляемых им сведений (материалов), 3) в случае предоставления Заявителем для целей регистрации компьютерной программы недостоверных данных НЦИС или ассоциируемые с ним лица не могут рассматриваться ответственными за произведенную регистрацию компьютерной программы | | |
| 1. Дата Заявки и подпись Заявителя   /дата оформления заявки, подпись Заявителя либо уполномоченного представителя, ФИО, должность, печать – при наличии/ |  | |

ПЕРЕЧЕНЬ СВЕДЕНИЙ (МАТЕРИАЛОВ),

представление которых необходимо для целей оказания услуг по регистрации компьютерных программ

|  |  |
| --- | --- |
| Вид сведений (материалов) | Примечания (форма представления, конкретные данные, которые должны содержаться в материалах и т.д.) |
| 1. Экземпляр компьютерной программы | Представляется на материальном носителе (компакт-диске) в формате, предполагающем возможность тестового запуска компьютерной программы в целях обеспечения практической возможности подтвердить факт существования компьютерной программы и ее функциональность (работоспособность). На экземпляре компьютерной программы (на материальном носителе либо в составе результатов функционирования компьютерной программы, доступных для восприятия) должно содержаться указание автора(ов), правообладателя(ей), года создания компьютерной программы |
| 2. Описание компьютерной  программы | Документ произвольной формы (предпочтительно – объемом до 5 страниц), в котором раскрывается назначение, область применения и функциональные возможности компьютерной программы, перечень файлов, в которых представлена компьютерная программа и их размер, язык программирования, операционная система, технические требования для работы с компьютерной программой и другие сведения, относящиеся к назначению и функционированию компьютерной программы |
| 3. Документы (их заверенные копии, заверение может быть осуществлено самостоятельно Заявителем), подтверждающие принадлежность исключительного права на компьютерную программу | Применимо к случаям регистрации компьютерных программ Заявителями, не являющимися авторами таких компьютерных программ.  1) В случае перехода исключительного права в порядке служебного произведения должны быть подтверждены обстоятельства: наличие трудовых отношений между автором(ами) и правообладателем компьютерной программы; создание компьютерной программы по заданию нанимателя или в порядке выполнения обязанностей, обусловленных трудовым договором 2) В случае приобретения исключительного права по договору должны быть подтверждены обстоятельства: наличие договора(ов), определяющего(их) переход исключительного права на компьютерную программу от автора(ов) к правообладателю; 3) в случае приобретения исключительного права в порядке правопреемства (в т.ч. наследования) должны быть подтверждены обстоятельства: правопреемство действующего правообладателя в отношении исключительного права на компьютерную программу от лица, принадлежность которому исключительного права на данную компьютерную программу надлежащим образом подтверждена. |
| Общее требование к материалам:  1)должны предоставляться в форме/способом, позволяющей необходимым образом подтвердить происхождение материалов (их соответствующей части) от конкретного заинтересованного лица и, по возможности, предотвращающей возможность их несанкционированной корректировки (например, в отношении текстовых материалов - наличие подписи уполномоченного лица и печати Заявителя на каждом листе и т.п.; в отношении компакт-дисков – нанесение соответствующих надписей на поверхность носителя средствами, исключающими/затрудняющими внесение корректировок)  2) форма представления материалов должна соответствовать интересам их автоматизированной обработки (оцифровки – для документов) и унифицированного хранения: текстовые материалы (а также изображения экранных форм и т.д.) – исполнены на листах бумаги формата А4 машинным (печатным) способом; компакт-диски – формат CD или DVD (односторонний), формат/способ записи данных должен позволять тестовый запуск компьютерной программы (в целях подтверждения факта ее существования и функциональности) с помощью обычного (не специализированного) оборудования. | |