Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Электронная тетрадь**

по Основам Защиты Информации

Студент: Лобан В.С.

ФИТ 2 курс 6 группа

Преподаватель: Годун А. В.

Минск 2018

**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:**

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

**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.

**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»**

**Вариант 11**

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

**Теоретическое введение**

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:

|  |  |
| --- | --- |
|  | (1) |

Относительная эффективность:

|  |  |
| --- | --- |
|  | (2) |

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

|  |  |
| --- | --- |
|  | (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:

|  |  |
| --- | --- |
|  | (4) |

где К≥1.

Выражения (1) – (2) примут вид:

|  |  |
| --- | --- |
|  | (5) |

|  |  |
| --- | --- |
|  | (6) |

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

|  |  |
| --- | --- |
|  | (7) |

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

|  |  |
| --- | --- |
|  | (8) |

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

|  |  |
| --- | --- |
|  | (9) |

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

|  |  |
| --- | --- |
|  | (10) |

или

|  |  |
| --- | --- |
|  | (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:

|  |  |
| --- | --- |
|  | (12) |

то:

|  |  |
| --- | --- |
|  | (13) |

В этом случае (11) и (12) принимают вид:

|  |  |
| --- | --- |
|  | (14) |

Или:

|  |  |
| --- | --- |
|  | (15) |

где Cдоп — допустимые расходы на защиту.

**Решение задачи**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E*0 | *E* | *K* | *C* |
| 11 | 19000 | 17000 | 4 | 800 |

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



 – снижение положительного эффекта функционирования.

 – эффективность функционирования объекта при наличии средств защиты.

 – относительная эффективность.

 – относительная эффективность функционирования объекта при наличии средств защиты.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

Вывод: при решении поставленной задачи было вычислено, что коэффициенты ,. Так как коэффициент стремится к максимуму, с уверенностью можно утверждать, что все вычисления произведены правильно, и эффективность является целесообразной.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский Государственный Технологический Университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

Лабораторная работа №3

«Разработка политики информационной безопасности авиакомпании «BELAVIA»»

Выполнил:

студент 2 курса, 6 группы

Лобан В.С.

Проверил:

Годун А. В.

Минск 2018

**ОГЛАВЛЕНИЕ**

[**1.** **Введение.** 11](#_Toc477163564)

[**2.** **Постановка задачи** 12](#_Toc477163565)

[**3.** **Специфика руководства авиакомпании по информационной безопасности** 13](#_Toc477163566)

[**3.1.** **Охраняемые сведения в организации** 13](#_Toc477163567)

[**3.2.** **Демаскирующие признаки охраняемых сведений и технические каналы утечки информации** 13](#_Toc477163568)

[**3.3.** **Оценка возможностей технических разведок и иных источников угроз безопасности информации** 13](#_Toc477163569)

[**3.4.** **Обязанности и права должностных лиц по защите информации** 14](#_Toc477163570)

[**3.5.** **Планирование работ по защите информации и контролю** 14](#_Toc477163571)

[**3.6.** **Контроль состояния защиты информации** 14](#_Toc477163572)

[**3.7.** **Взаимодействие с другими предприятиями** 16](#_Toc477163573)

[**4.** **Политика информационной безопасности авиакомпании** 17](#_Toc477163574)

[**5.** **Меры защиты информации** 18](#_Toc477163575)

[**6.** **Вывод** 20](#_Toc477163576)

[**7.** **Список используемой литературы** 21](#_Toc477163577)

# **Введение**

Политика информационной безопасности – это высокоуровневый документ, который включает в себя принципы и правила, определяющие и ограничивающие определенные виды деятельности объектов и участников системы информационной безопасности, направленные на защиту информационных ресурсов организации.

Как известно, стратегическое планирование позволяет определить основные направления деятельности организации, связав воедино маркетинг, производство и финансы. Долгосрочный стратегический план позволяет компании выстроить все свои бизнес-процессы с учетом микро и макросреды для достижения наилучших финансовых показателей и темпов экономического роста. Важной составляющей в стратегическом планировании является учет требований политики информационной безопасности, которые должны быть краеугольным камнем при определении среднесрочных и долгосрочных целей и задач организации. С ростом компании и пересмотром планов политика также должна пересматриваться. Низкоуровневые документы информационной безопасности необходимо пересматривать в соответствии с реализацией краткосрочных планов.

Политика информационной безопасности неразрывно связана с развитием компании, ее стратегическим планированием, она определяет общие принципы и порядок обеспечения информационной безопасности на предприятии. Политика информационной безопасности тесно интегрируется в работу предприятия на всем этапе его существования. Все решения, предпринимаемые на предприятии, должны учитывать её требования.

Основные этапы разработки политики информационной безопасности следующие:

* исследование текущего состояния информационной среды и информационной безопасности организации;
* анализ полученных сведений по результатам исследования;
* формирование плана работ по разработке политики информационной безопасности;
* разработка политики информационной безопасности организации;

# **Постановка задачи**

В данной работе требуется изучить информационную систему авиакомпании «BELAVIA». Для этого необходимо выделить участки с наиболее важной информацией, уделить внимание изучению различных путей нанесения вреда: уничтожение информации, физическое повреждение носителей информации, программное повреждение информации (вирусы). На основании полученных данных разработать план по выявлению угроз и их устранению.

Конечный документ должен удовлетворять следующим требованиям:

* лаконичность – большой объем документа отпугнет любого пользователя, ваш документ никто никогда не прочитает.
* доступность простому обывателю – конечный пользователь должен понимать, что написано в политике о защите информации.

На рисунке 3.1 изображена структура написания политики информационной безопасности.

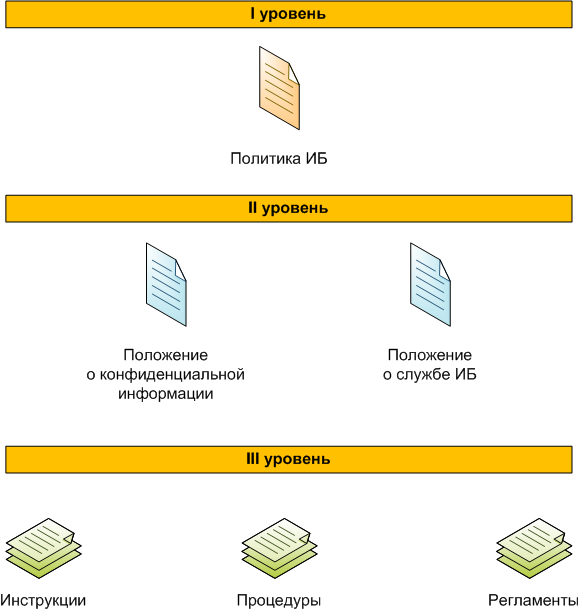


Рисунок 3.1 Структура написания политики информационной безопасности.

На самом деле все очень просто: политика ИБ должна быть документом первого уровня, ее должны расширять и дополнять другие документы (положения и инструкции), которые уже будут описывать что-то конкретное.

# **Специфика руководства авиакомпании по информационной безопасности**

Руководство должно состоять из следующих разделов:

* охраняемые сведения в организации;
* демаскирующие признаки охраняемых сведений и технические каналы утечки информации;
* оценка возможностей технических разведок и других источников угроз безопасности информации;
* организационные и технические мероприятия по защите информации;
* обязанности и права должностных лиц по защите информации;
* планирование работ по защите информации и контролю;
* контроль состояния защиты информации;
* взаимодействие с другими предприятиями (учреждениями, организациями), КГБ.

## **Охраняемые сведения в организации**

В этом разделе указывается конкретная цель, которая должна быть достигнута в результате проведения мероприятий по защите информации (охраняемых сведений) в компании, замысел достижения этой цели и приводится перечень охраняемых сведений (без указания конкретных числовых параметров).

## **Демаскирующие признаки охраняемых сведений и технические каналы утечки информации**

В этом разделе указываются демаскирующие признаки, которые раскрывают охраняемые сведения в авиакомпании, в том числе демаскирующие признаки, возникающие в связи с использованием средств обеспечения ее деятельности. Приводятся возможные технические каналы утечки охраняемых сведений, включая каналы утечки информации в технических средствах ее обработки.

## **Оценка возможностей технических разведок и других источников угроз безопасности информации**

В этом разделе приводится перечень видов и средств технической разведки, источников угроз несанкционированного доступа к информации, которые опасны для данной организации, в том числе со стороны преступных группировок и результаты оценки их возможностей: по обнаружению демаскирующих признаков, раскрывающих охраняемые сведения; по перехвату информации, циркулирующей в технических средствах ее обработки; по перехвату речевой информации из помещений; по получению, разрушению (уничтожению), искажению или блокированию информации в результате несанкционированного доступа к ней.

При оценке используется частная модель угроз для организации, методики оценки возможностей иностранной технической разведки и другие документы по этому вопросу.

В разделе "Организационные и технические мероприятия по защите информации" приводятся:

* организационные и технические мероприятия, обеспечивающие устранение или ослабление (искажение) демаскирующих признаков и закрытие возможных технических каналов утечки охраняемых сведений в организации;
* мероприятия по защите информации об иной создаваемой (применяемой) продукции и технологиях;
* мероприятия по защите информации при постоянном контролируемом и неконтролируемом нахождении иностранных граждан как на территории организации, так и в непосредственной близости от нее;
* мероприятия по защите информации в системах и средствах информатизации и связи.

## **Обязанности и права должностных лиц по защите информации**

В этом разделе определяются должностные лица подразделений авиакомпании, ответственные за разработку, обеспечение и выполнение мероприятий по защите информации, их функциональные обязанности и права, приводится структурная схема взаимодействия подразделений по защите информации с соответствующими основными подразделениями организации.

## **Планирование работ по защите информации и контролю**

В этом разделе указываются руководящие документы для планирования работ по защите информации, требования к содержанию планов, приводится порядок разработки, согласования, утверждения и оформления планов, устанавливается порядок отчетности и контроля за выполнением планов.

## **Контроль состояния защиты информации**

В разделе "Контроль состояния защиты информации" указываются задачи контроля, перечень органов и подразделений, имеющих право проверки состояния защиты информации в организации, привлекаемые силы и средства контроля, порядок привлечения (при необходимости) к этой работе специалистов основных подразделений организации, устанавливаются периодичность и виды контроля, порядок оформления результатов контроля, определяются действия должностных лиц по устранению нарушений норм и требований по защите информации и порядок разработки мероприятий по устранению указанных нарушений.

## **Взаимодействие с другими предприятиями**

В этом разделе указываются порядок взаимодействия в области защиты информации с предприятиями (учреждениями, организациями) при выполнении совместных работ, применяемые совместные организационные и технические мероприятия по защите информации, ответственность, права и обязанности взаимодействующих сторон, а также приводится структурная схема взаимодействия.

# **Политика информационной безопасности авиакомпании**

Пассажир при бронировании сообщает авиакомпании или агенту по продаже перевозок необходимую информацию о маршруте перевозки, дате и времени вылета, необходимом количестве бронируемых мест, классе обслуживания на борту воздушного судна, имеющемся гражданстве, а также информацию о своих персональных данных.  В случае отказа пассажира от предоставления информации, необходимой для бронирования, бронирование не производится. Пассажир при бронировании может сообщить номер телефона или иной способ контакта для его информирования.

Информация личного характера, полученная в формате бумажных регистрационных форм или через сайт компании, используется, среди прочего, для целей регистрирования пользователей, отслеживания политики и статистики, а также в целях, разрешенных пассажиром. Кроме того, BELAVIA использует информацию личного характера для поддержания связи с клиентами иными способами. Информация также используется для того, чтобы проинформировать о внесении существенных изменений в настоящую Политику информационной безопасности. Время от времени пользователям сайта компании предлагается предоставлять информацию в формате опросов или анкет.

BELAVIA нанимает другие компании, которые предоставляют услуги, такие как обработка и доставка информации, размещение информации, доставка содержания и услуг на сайт компании, выполнение статистического анализа. Чтобы эти компании могли предоставлять эти услуги, BELAVIA сообщает им информацию личного характера, однако им будет разрешено получать только ту информацию личного характера, которая необходима им для предоставления услуг. Они обязаны соблюдать конфиденциальность этой информации, и им запрещено использовать ее в иных целях.

Авиакомпания может использовать или раскрывать личные данные потребителя и по иным причинам, в том числе, если мы считаем, что это необходимо в целях выполнения требований закона или решений суда, для защиты прав или собственности компании, защиты личной безопасности пользователей нашего сайта и других соглашений, в целях расследования или принятия мер в отношении незаконной или предполагаемой незаконной деятельности, в связи с корпоративными сделками, такими как разукрупнение, слияние, продажа активов или в маловероятном случае банкротства, или в иных целях в соответствии с вашим согласием. BELAVIA может раскрывать содержание сообщений или писем, однако не будет размещена или опубликована информацию личного характера, а также, за исключением случаев, предусмотренных в настоящей Политике конфиденциальности, такая информация не будет предоставляться оказывающим услуги третьим сторонам без вашего согласия. Информация не будет продана, предоставлена на правах аренды или лизинга, наши списки пользователей с адресами электронной почты третьим сторонам.

# **Меры защиты информации**

Информационная безопасность в сфере гражданской авиации достигается своевременным принятием ряда мер и определенных средств защиты в авиакомпаниях, аэропортах и в компаниях-контрагентов.

* Организационные меры. В первую очередь, защита информации должна начинаться с человека, сотрудника который возьмёт на себя обязанность по обеспечению информационной безопасности в компании. Если компания очень большая, то одним сотрудником не обойтись, и лучше создать отдел хотя бы из 3 человек, один руководитель и два инженера. В любом случае сотрудник или руководитель отдела должен хорошо разбираться в вопросах защиты информации, уровень компетенции сотрудника обязательно отразится на финансовых затратах на защиту информации. Когда сотрудника нашли - он после изучения информационных процессов в компании должен разработать соответствующие организационно-распорядительные документы, подписываются которые главным лицом в компании.
* Физические меры - ограничение физического доступа к защищаемой информации.
* Технические меры - разнообразные средства защиты от НСД, защита информации от утечки по техническим каналам связи, криптографические средства защиты информации, системы защиты от DDOS-атак

Существуют средства защиты информации:

* средства защиты от внешних угроз – антивирусы (Kaspersky AntiVirus for Mail servers, Dr.Web Enterprise Suite и т. д.) средства защиты от DDoS-атак, межсетевые экраны и т. п.;
* средства защиты от внутренних угроз - DLP-системы (InfoWatch, [McAfee DLP](javascript:void(0);)), защита баз данных, системы разделения доступа к информационным ресурсам.
* средства резервирования. Аппаратные и программные средства создания backup (Veeam® Endpoint Backup).

Также существуют не только средства, но и методы (принципы защиты информации):

Препятствование – метод физической защиты информационных систем (ИС), благодаря которому злоумышленники не имеют шанса попасть на охраняемую территорию или к защищаемой информации (к оборудованию, дискам и так далее).

Управление доступом – при этом методе защиты информации регулируется и контролируется эксплуатирование ресурсов компьютерной ИС (компонентов БД, программного обеспечения и аппаратуры). Управление доступом несет множество защитных функций:

* распознавание пользователей, работников и ресурсов системы (всем объектам присваивается персональный идентификационный код);
* аутентификация (установление подлинности) объекта или субъекта согласно представляемого им идентификационному коду;
* инспекция уровня доступа, то есть проверяется согласованность идентификационного кода, даты и времени суток, уровень и вид запрашиваемых ресурсов и операций принятым правилам;
* предоставление доступа и создание условий работы в пределах существующего регламента;
* фиксация (внесение в протокол) запросов к защищаемым ресурсам;

Маскировка – технология охраны данных, ограждающая доступ к ней c помощью криптографии (информация видоизменяется так, что третьи лица без понимания принципа шифровки не имеют возможности ее воспринимать). Этот способ является единственной надежной гарантией защиты данных при передаче их по каналам связи большой протяженности.

# **Вывод**

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.

# **Список используемой литературы**

1 Как обеспечить информационную безопасность в авиакомпаниях [Электронный ресурс] / Все о туризме. Туристическая библиотека. 2017 г. URL: http://tourlib.net/statti\_tourism/suhanov.htm (дата обращения: 28.02.2017).

2. Политика информационной безопасности [Электронный ресурс] / Официальный сайт белорусских авиалиний «BELAVIA». 2017 г. URL: https://belavia.by/policy (дата обращения: 28.02.2017).

3. Меры защиты информации [Электронный ресурс] / Методы защиты информации кратко. 2017 г. URL: http://interesting-information.ru/2015/07/metody-zashhity-informacii-kratko (дата обращения: 28.02.2017).

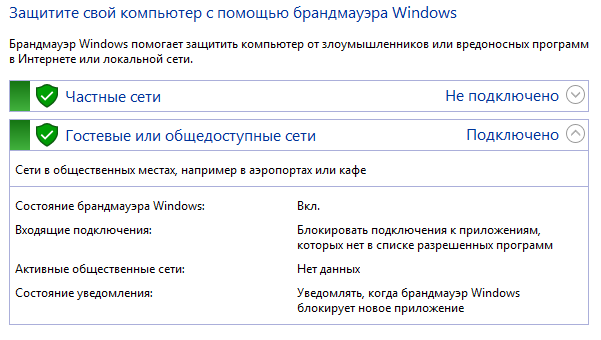
4. Основное содержание руководства по защите информации [Электронный ресурс] / Электронный фонд правовой и нормативно-технической документации. 2017 г. URL: http://docs.cntd.ru/document/902015340 (дата обращения: 28.02.2017).

5. Политика информационной безопасности [Электронный ресурс] / Политика информационной безопасности – опыт разработки и рекомендации. 2017 г. URL: https://habrahabr.ru/post/174489/ (дата обращения: 28.02.2017).

**Практическое занятие №4**

**«Настройка Брандмауэра Windows»** Брандмауэр Windows

Брандмауэр (Межсетевой экран) – это аппаратный или программный комплекс, позволяющий проверять (фильтровать) входные и выходные потоки данных, проходящие через интернет или сеть. В случаи нарушения политики безопасности компьютера, брандмауэр блокирует эти данные. Окно брандмауэра представлено на рисунке 4.1.

Рисунок 4.1 – окно брандмауэра Windows

1. Создание правила для входящих подключений на блокировку подключения

Для настройки входящих и исходящих подключений необходимо выбрать «Дополнительные параметры» (Advanced settings).

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

Далее необходимо указать к исполняемому файлу программы (рис. 4.2).

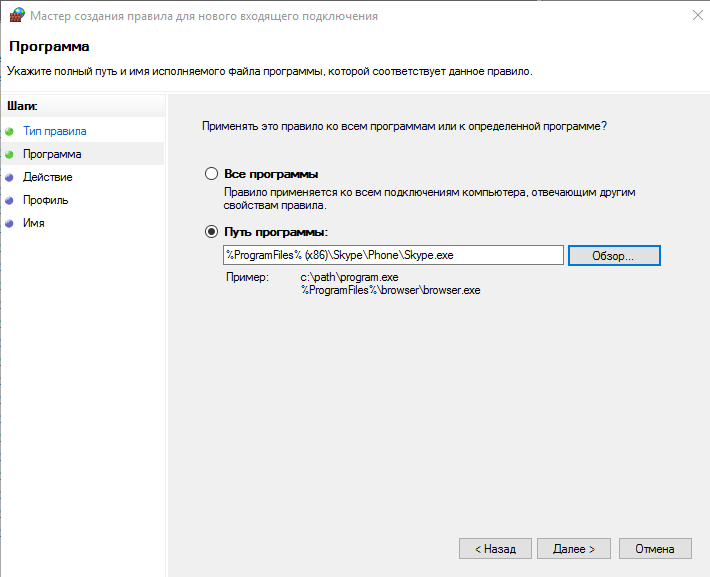


Рисунок 4.2 – Мастер создания правила (путь)

1. Создание правила для входящих подключений на разрешение подключения

Далее указывается, какое именно действие вы хотите применить. В данном случае необходимо блокировать подключение.

В следующем окне указывается необходимое действие (рис. 4.3 ).

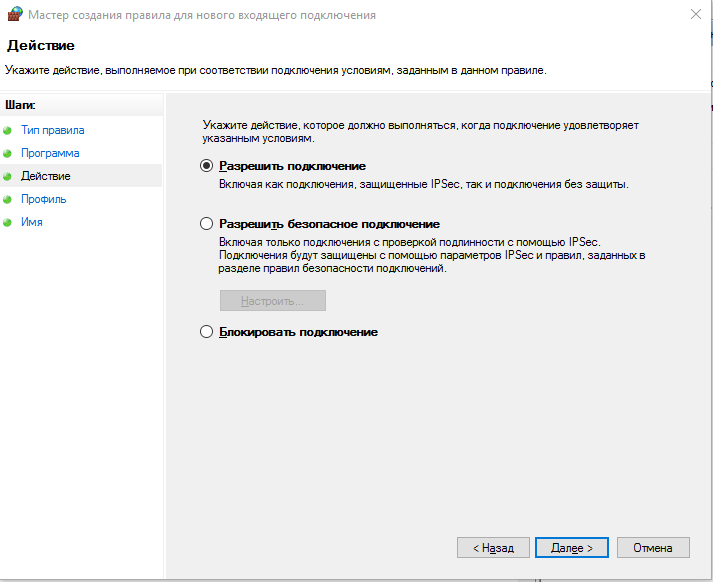


Рисунок 4.3 – разрешение входящего подключения

1. Создание правила для исходящих подключений на блокировку подключения

В следующем окне указывается необходимое действие (рис. 4.4 ).

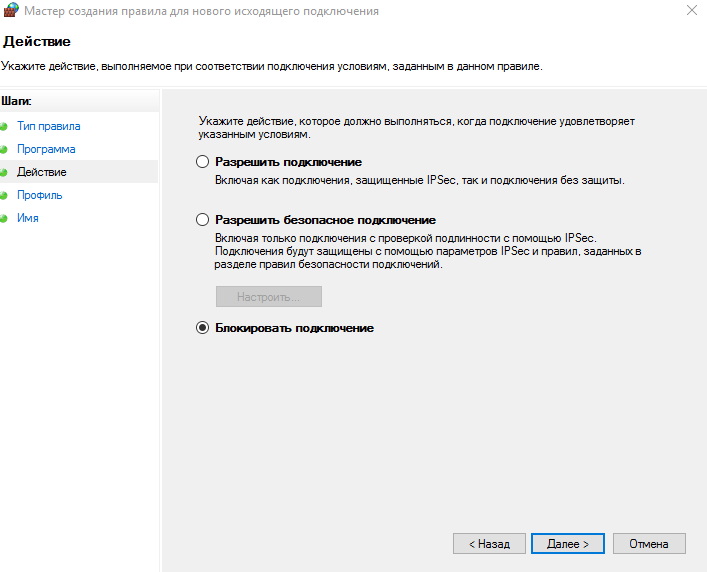


Рисунок 4.4 – блокировка исходящего подключения

1. Создание правила для исходящих подключений на разрешение подключения

В следующем окне указывается необходимое действие (рис. 4.5 ).

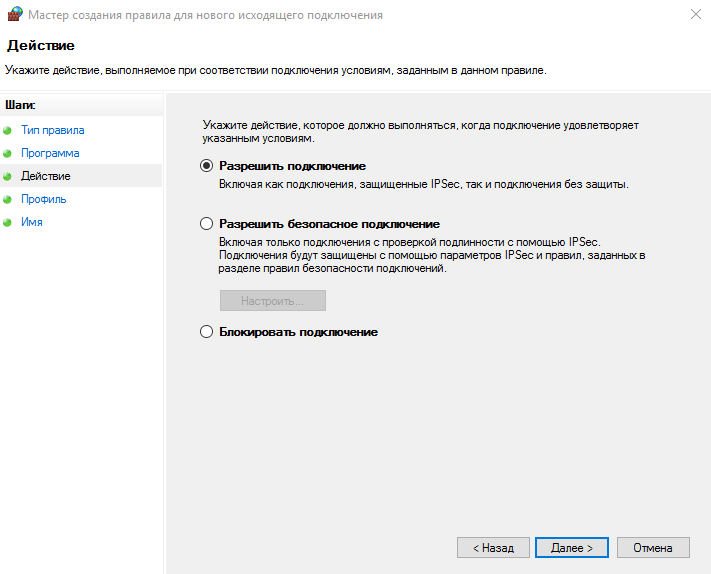
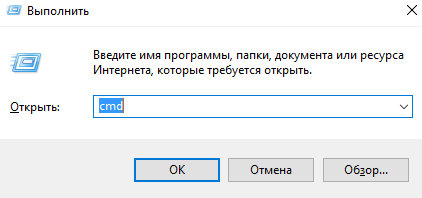


Рисунок 4.5 – разрешение исходящего подключения

1. Меню > Выполнить

Cmd (командная строка) – это текстовый интерфейс, в котором команды отдаются путем ввода текстовых строк с клавиатуры. (рис. 4.6).



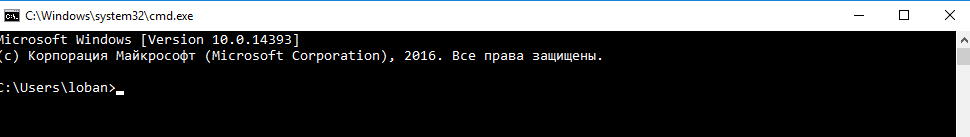


Рисунок 4.6 – Результат работы cmd

MSConfig (Настройка системы)–утилита для управления автозапускаемыми программами и загрузкой Windows.

Начиная с Windows 98, Microsoft поставляет утилиту «MSConfig.exe», предоставляющую интерфейс для управления файлами, запускающимися при загрузке Windows. Она находится в каталоге установки Windows. Её можно запустить из диалогового окна «Выполнить» или через командную строку. В ней нет возможности добавлять новый элемент с именем приложения или документа для автозапуска, но можно отключать, не удаляя, любой пункт из находящихся в списках (рис. 4.7).

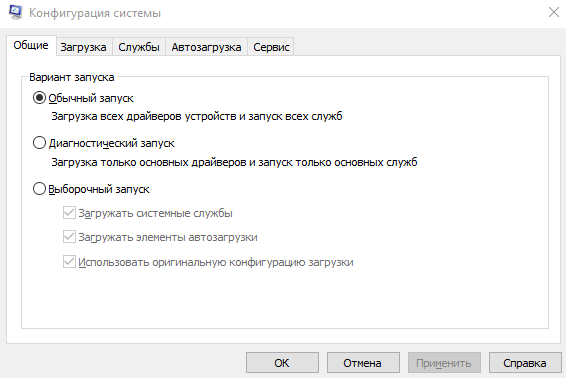


Рисунок 4.7 – Результат работы MSConfig

**Вывод**: в процессе выполнения задания ознакомились с брандмауэром Windows, его функциями и попробовали в действии команды администратора.

**Практическое занятие №5**

**Тема «**Настройка антивирусов**»**

Цель: Овладение навыками настройки и использования различных антивирусов.

**Теоретическое введение**

**Признаки заражения компьютера вредоносными программами.**

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.

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.

**Ход выполнения**

1. **Настроить режим фильтрации файервола антивируса.**

Для настройки режима фильтрации нужно выполнить следующие действия:

1. Открыть программу ESET NOD32 Smart Security, щелкнув по значку программы в области уведомлений Windows или выбрав команды Пуск­ – Все программы – ESET – ESET NOD32 Smart Security.

2. Открыть дополнительные настройки(рис. 5.1), нажав клавишу F5 на клавиатуре – Персональный файервол. Откроется окно расширенной настройки. В расположенном справа раскрывающемся меню **Режим фильтрации** выбрать нужный режим фильтрации и нажать кнопку **OK**.

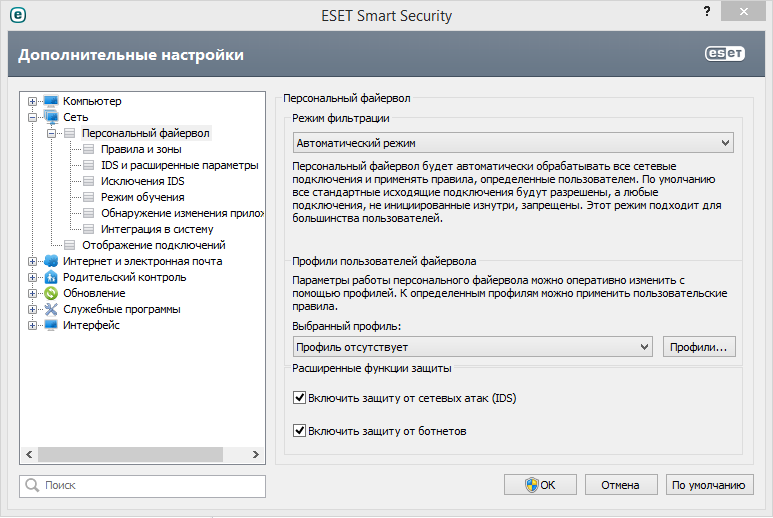


Рисунок 5.1 – Окно выбора режима фильтрации.

1. **Настроить Оффлайн обновление сигнатур угроз из локальной**

**папки**

Для обновления Антивируса ESET NOD32 или ESET NOD32 Smart Security на локальных ПК необходимо выполнить следующие шаги:

1. Открыть главное окно программы ESET NOD32
2. Нажать клавишу «F5»и перейти на вкладку «Обновление» (рис. 5.2)

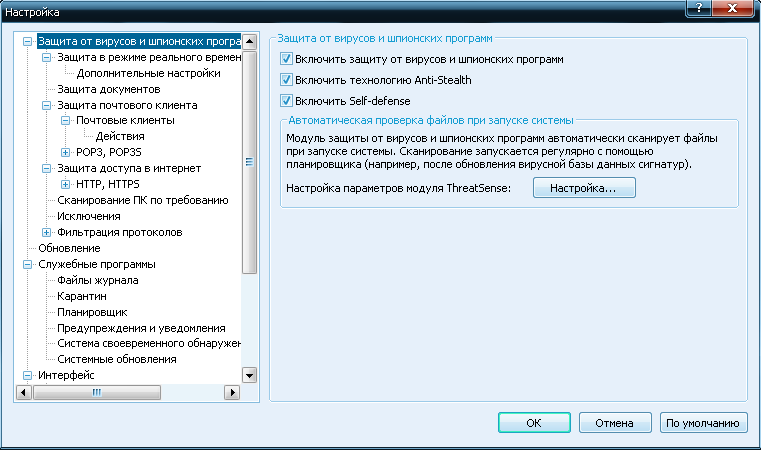


Рисунок 5.2 – Окно настроек

1. В строке «Сервер обновлений» нажать «Изменить» (рис 5.3)

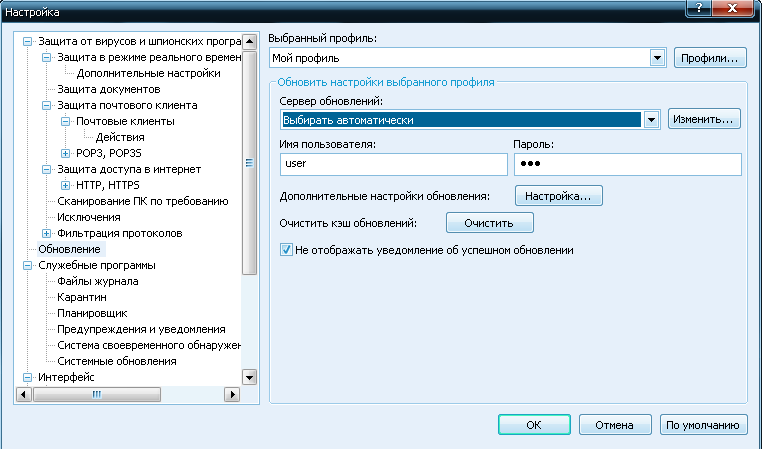


Рисунок 5.3 – вкладка «Обновление» в окне настроек

1. В строке «Серверы обновлений» указать путь к папке с

Обновлениями и далее нажать «Добавить» и «OК» (рис. 5.4)

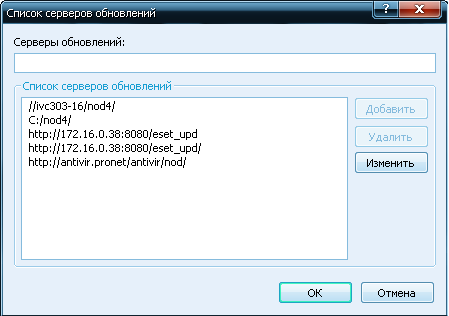


Рисунок 5.4 – окно «Список серверов обновлений»

1. В главном окне программы выбрать «Обновление», далее

«Обновить версию базы данных сигнатур вирусов» (рис. 5.5)

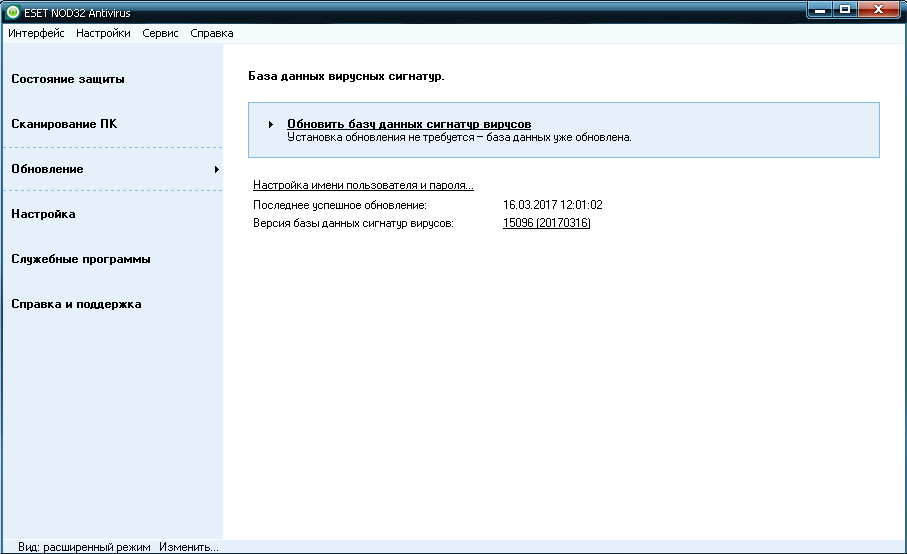


Рисунок 5 – Окно антивируса Eset NOD32.

1. **Настроить Оффлайн обновление сигнатур угроз из локального**

**сервера**

Для настройки оффлайн обновления сигнатур угроз из локального сервера необходимо выполнить все действия из п.2, однако в списке серверов обновлений указать адрес локального сервера (рис 5.6).

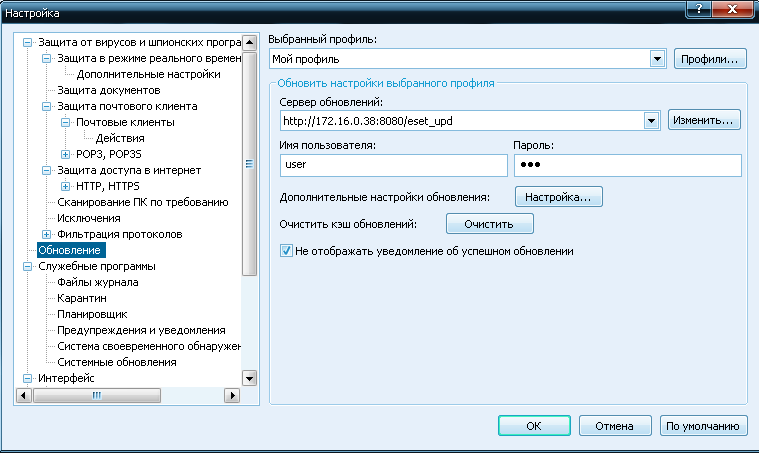


Рисунок 5.6 – Окно обновлений Eset NOD32

**Вывод:** в ходе выполнения практического занятия я изучил навыки настройки и использования различных антивирусов, настройки обновления сигнатур угроз из локального сервера и папки.

**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.

Теоретическое введение

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.

Ход работы

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 – окно создания TrueCrypt раздела

1. Далее вам необходимо определится, какой раздел вы создадите: скрытый или обычный. Руководство покажет создания обычного раздела. Опция уже выставлена. Поэтому нажимаем «Next».

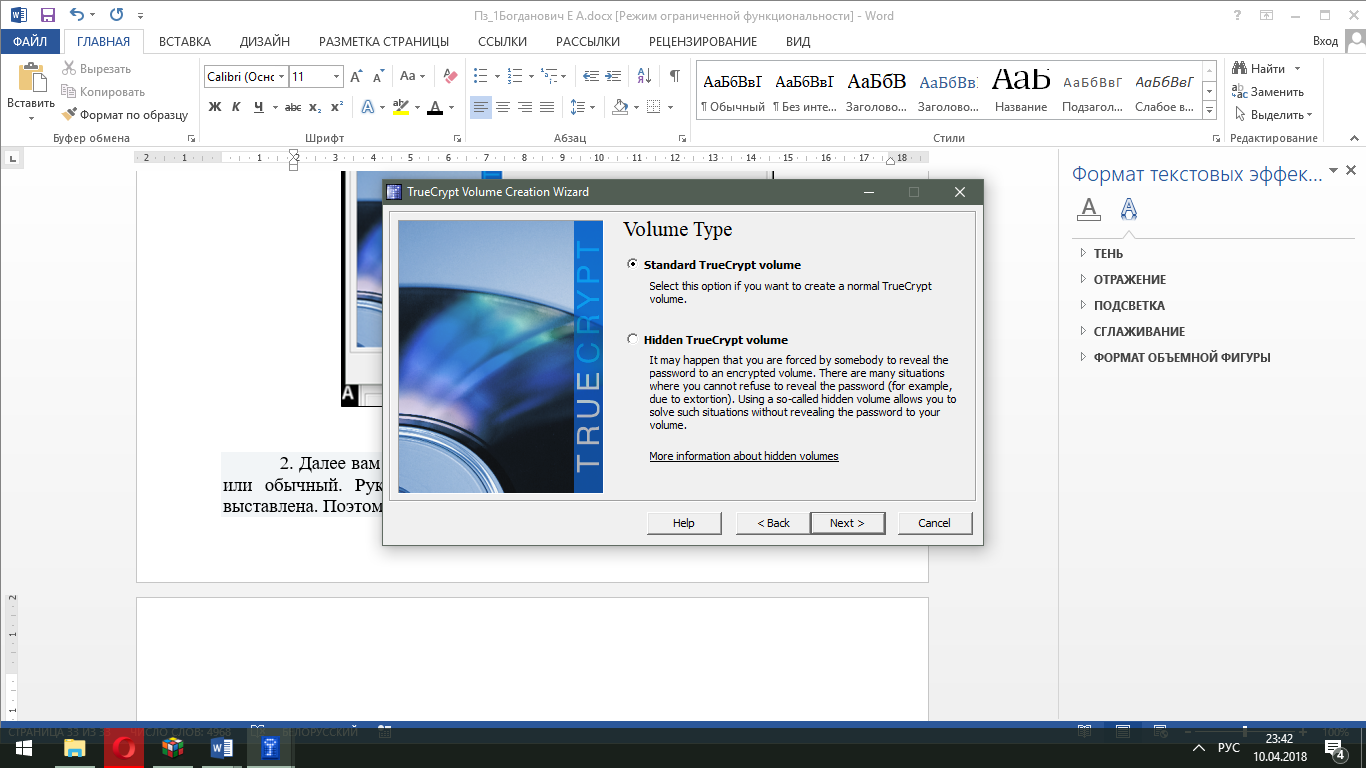


Рисунок 6.2 – определение раздела

1. Данный этап предполагает указание места расположения раздела TrueCrypt. При этом поведение контейнера идентичное с поведением самого обыкновенного файла. Жмем Select File. Открывается окошко для выбора файла.

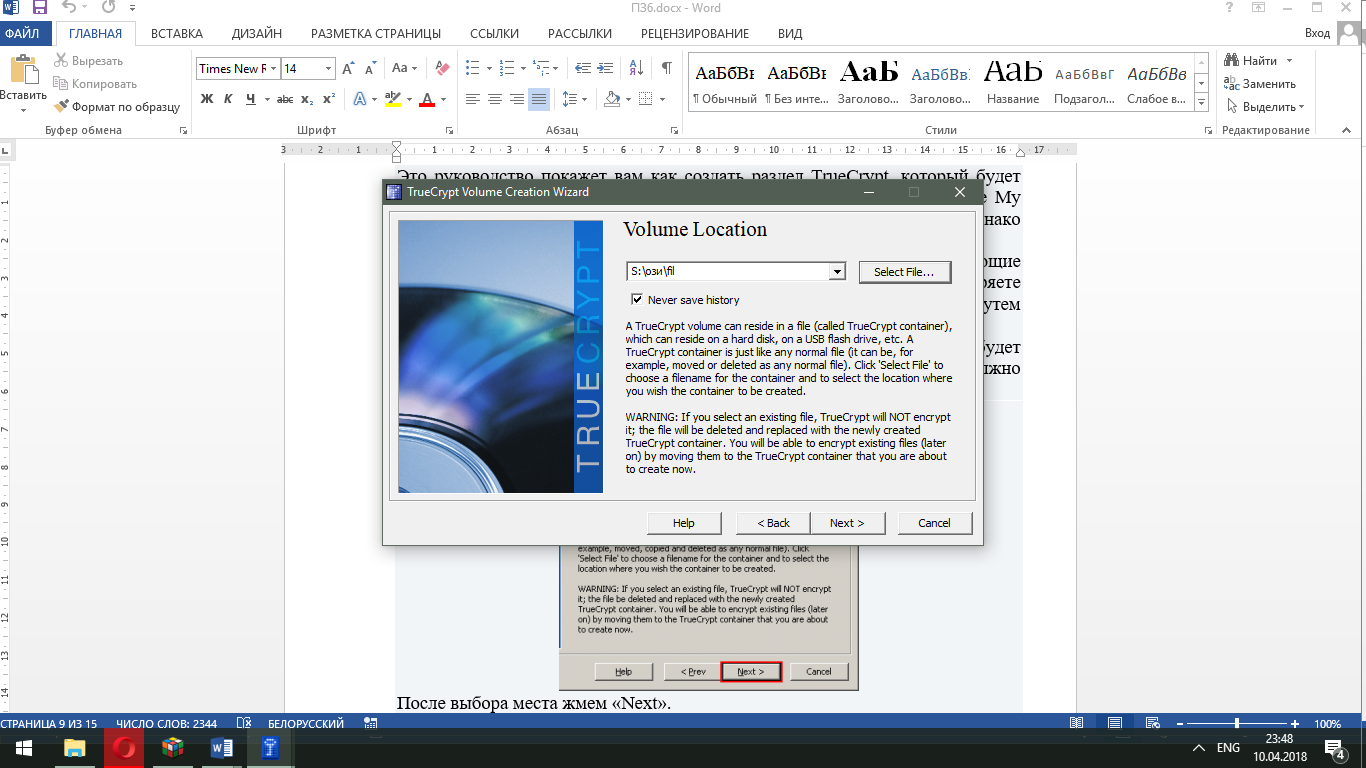


Рисунок 6.3 – размещение раздела

1. В данном разделе нам предлагается сделатиь выбор алгоритма для шифрования, а так же хеш – алгоритма предназначенного для раздела. Выбираем алгоритм AES и жмем  «Next».

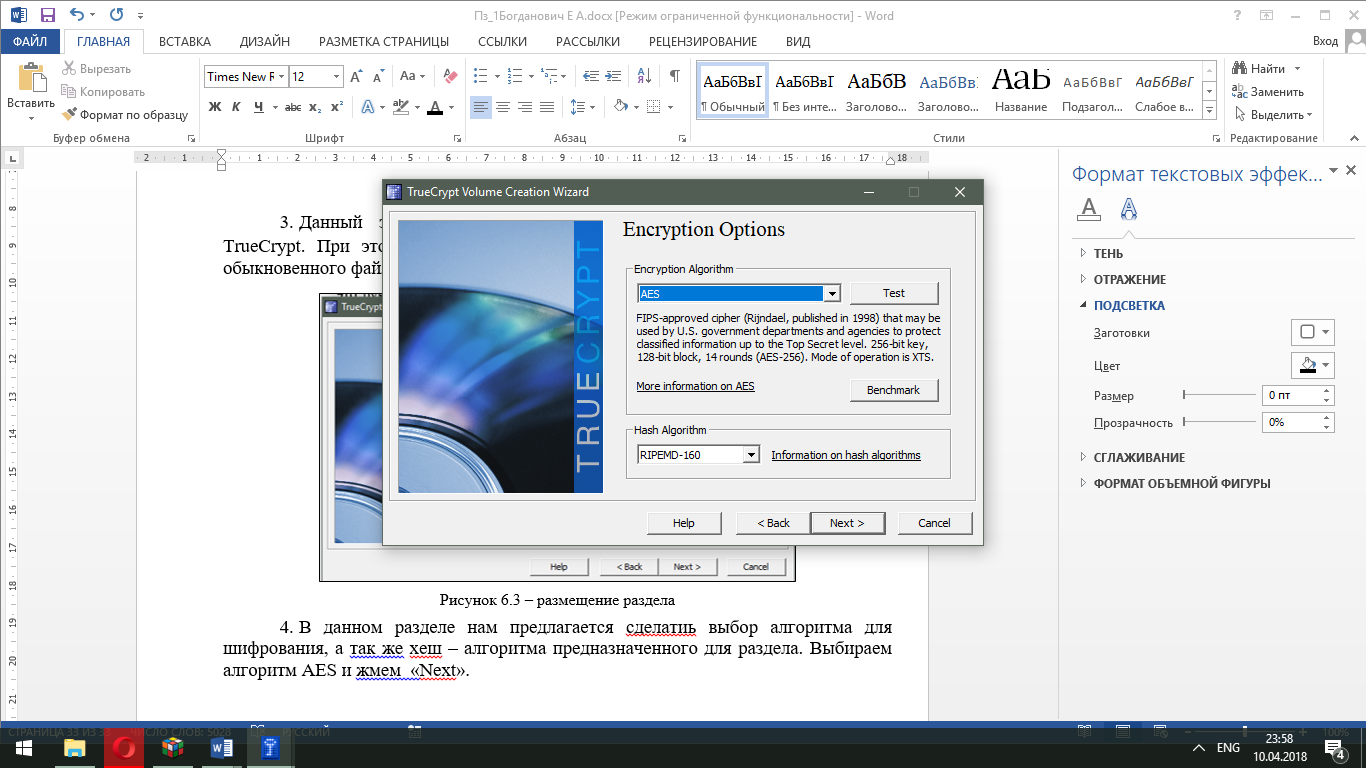


Рисунок 6.4 – алгоритм шифрования

1. Далее в окне мы указываем предполагаемый размер контейнера TrueCrypt в 10 мегабайт. Можно выбрать и другой размер, а затем нажимаем «Next».

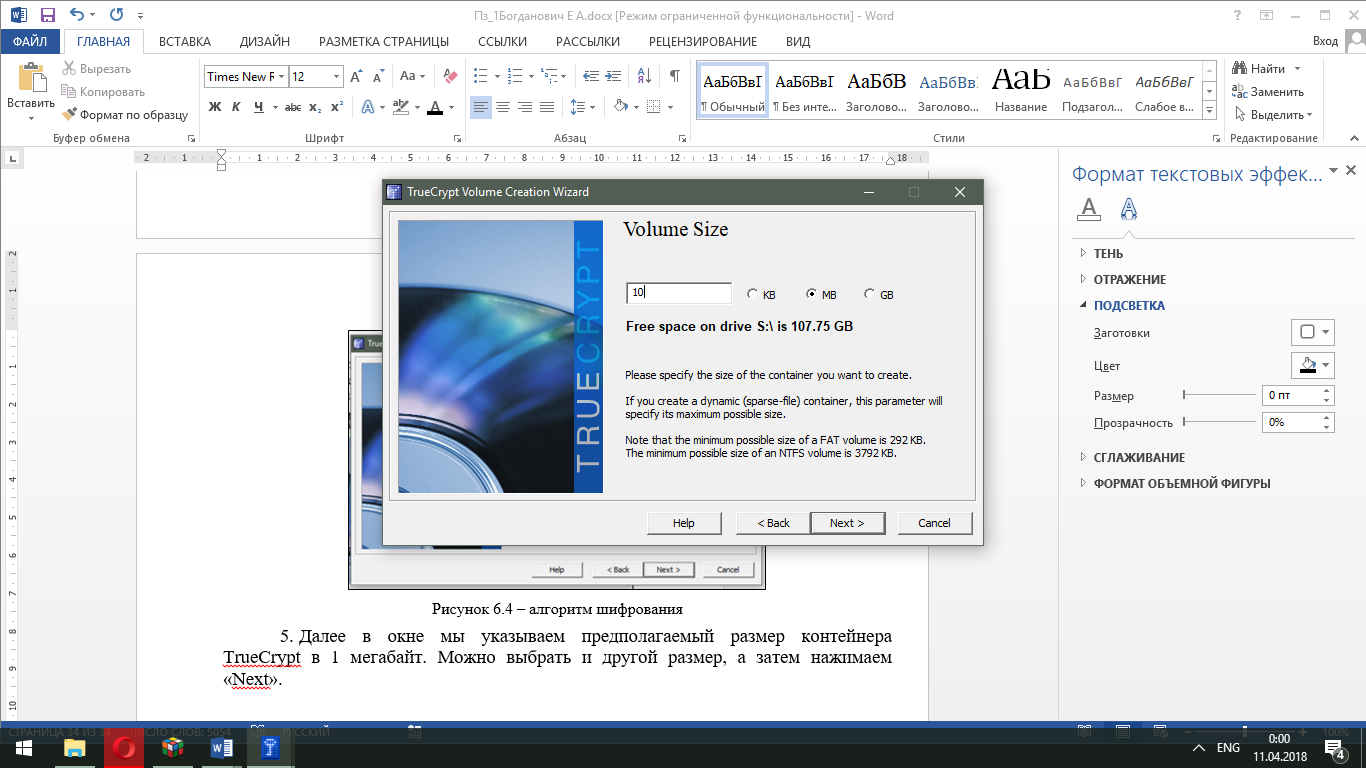


Рисунок 6.5 – размер контейнера

1. Следующий этап самый основной. Тут необходимо определится с паролем для раздела. Стоит ознакомится с информацией, которое дает определение качественного пароля. После того как вы определитесь введите пароль в первое поле, а затем продублируйте его во второе и нажмите «Next».

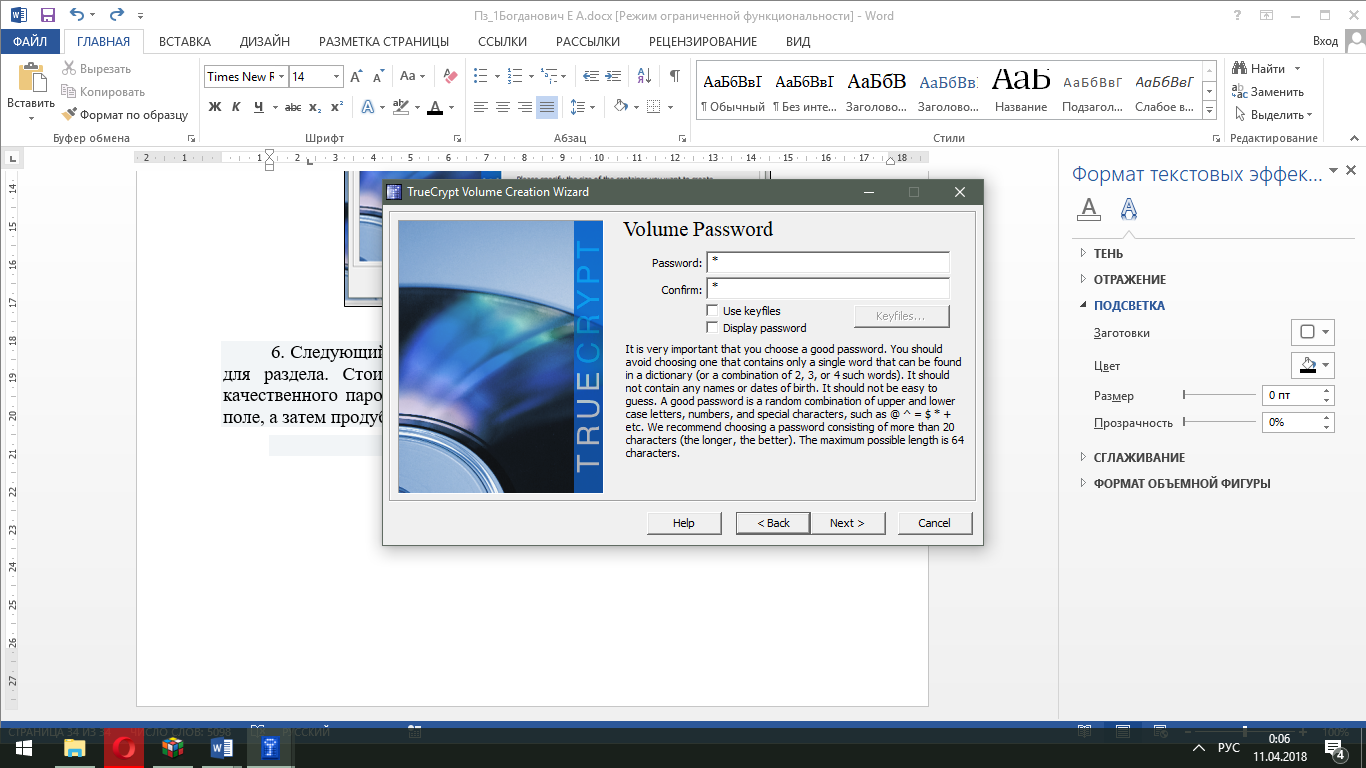


Рисунок 6.6 – настройка пароля

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.

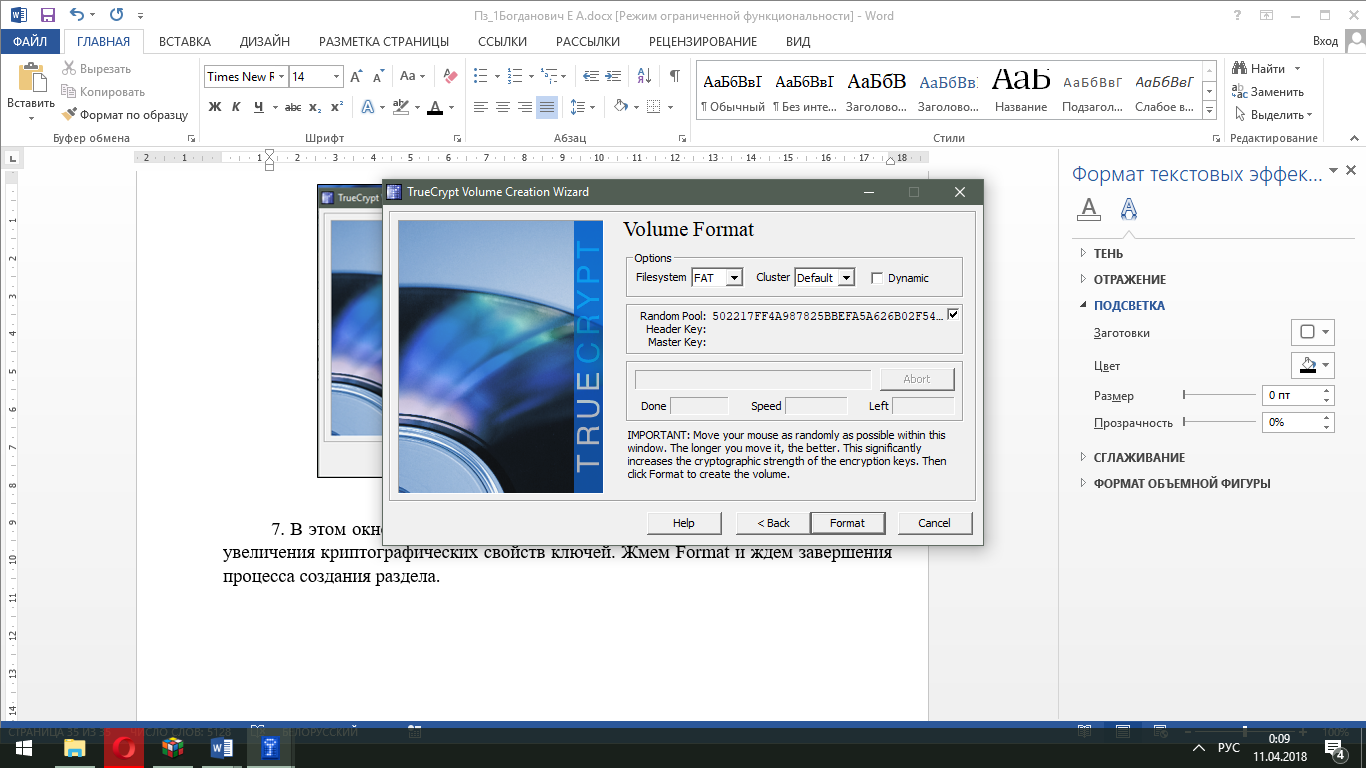


Рисунок 6.7 – создание раздела

1. Выбираем одну из букв представленных в списке, это будет буква диска к которому вы примонтируете ваш контейнер.

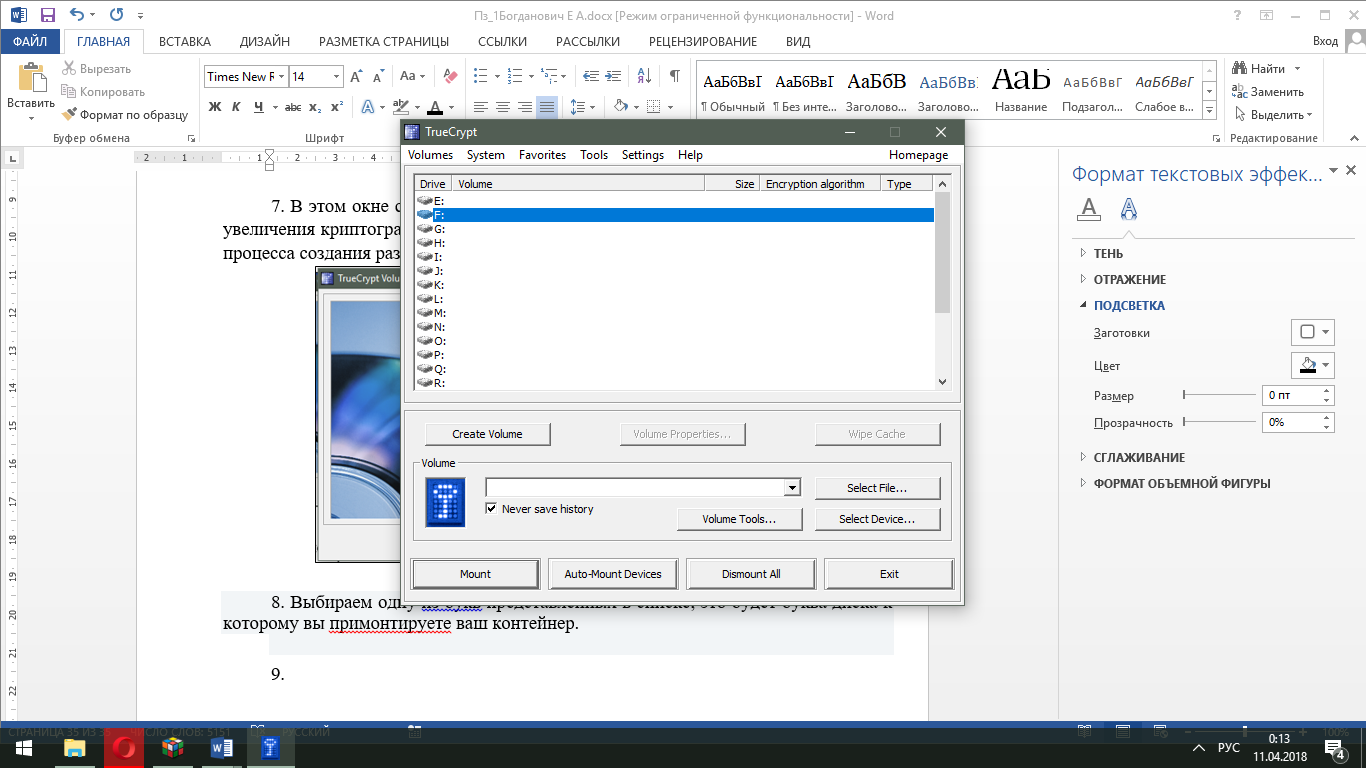


Рисунок 6.8 – буква диска

1. Далее жмем Select File. При этом должна открыться стандартная версия окна в которой  необходимо выбрать файл. В данном окне находим файл, который вы создали с 6 по 11 этап и выбираем его. Жмем  Open, после этого окно должно исчезнуть. В оставшемся окошке TrueCrypt жмем Mount. Появляется окно, которое запрашивает ваш пароль. Вводим пароль, который вы установили на 10 этапе в поле выделенное красным. Жмем «ОК».

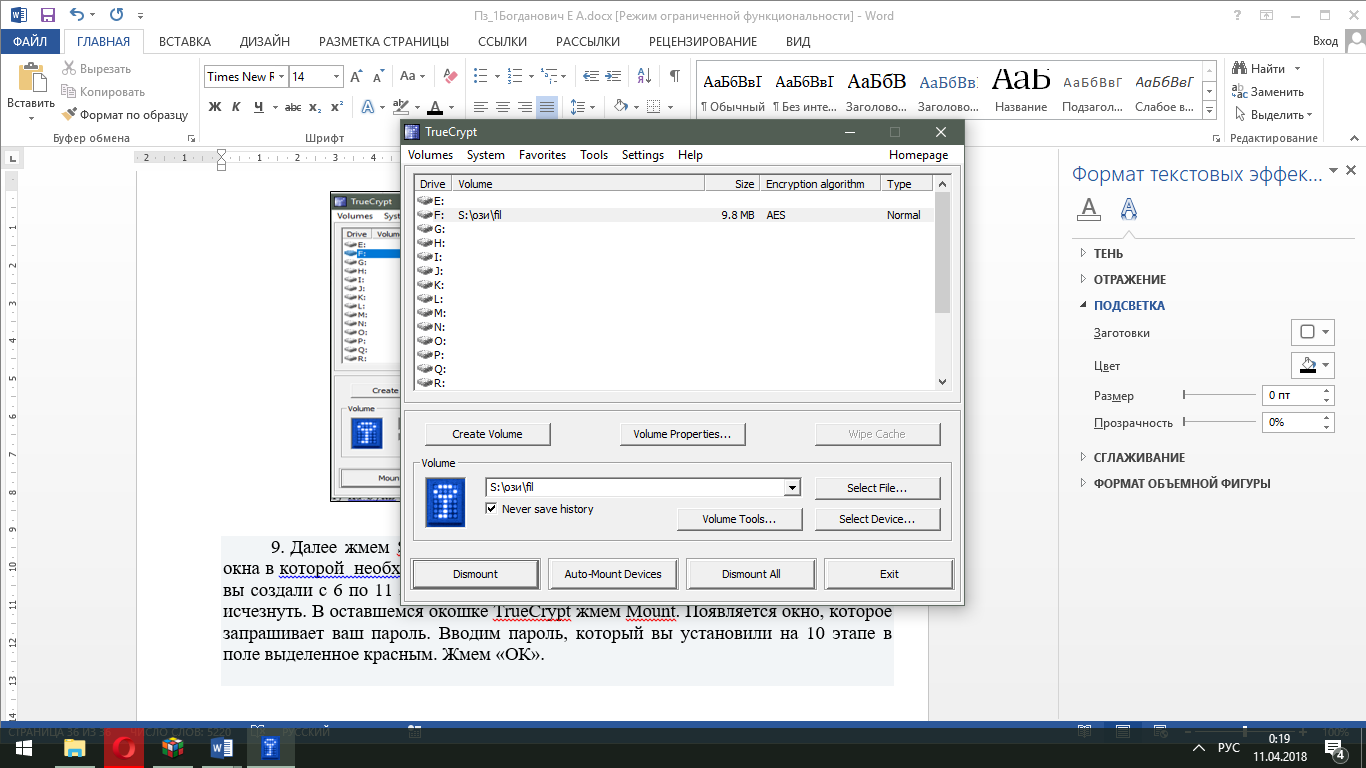


Рисунок 6.9 – монтировка на выбранный раздел

1. Зайдя в раздел через Мой компьютер, можно увидеть тот самый диск, созданный ранее. В данном случае это локальный диск F.

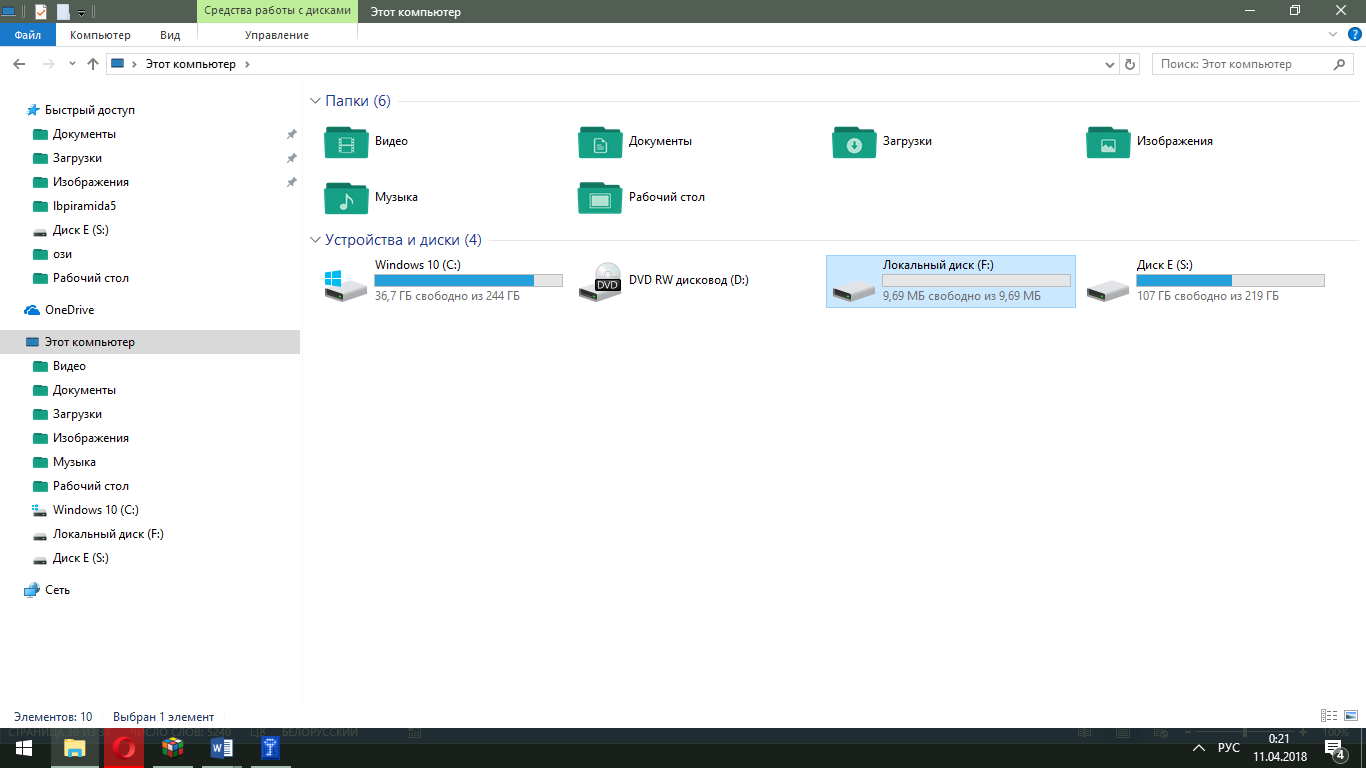


Рисунок 6.10 – созданный диск

Вывод:

Шифрование данных – это метод сокрытия исходного смысла документа или сообщения, которое обеспечивает искажение его первоначального вида. Простыми словами, это способ защиты информации. Такой метод еще называют кодированием, так как с помощью специальных программ или вручную ваш текст переводят в непонятный для постороннего человека код. Сама процедура зависит от последовательности изменения вида данных. Такую последовательность принято называть алгоритмом. Шифрование данных относят к криптографии. Эта наука тщательно изучается мировыми разведывательными организациями, и с каждым днем разгадываются и создаются новые криптографические алгоритмы. Методы шифрования были известны еще в древности, когда римские военачальники передавали с гонцами важные письма в зашифрованном виде. Алгоритмы тогда были примитивными, но успешно запутывали врагов. В отличие от тех времен мы не являемся военачальниками, но врагов имеем. Ими являются мошенники, которые жаждут заполучить важные для нас данные. Вот их-то и следует защитить любым способом.

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

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

**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 (шифр текст). 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 (шифр текст, ciphertext) или зашифрованных данных в открытые по определенным правилам с применением ключей.

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.

1. 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

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

1. Шифры перестановки (transposition, permutation, P-блоки);
2. 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:

1. Получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);
2. Отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;
3. Получатель получает сообщение и расшифровывает его, используя свой секретный ключ.

**Ход работы**

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

1.1.В качестве p и g возьму два любых простых числа.

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

|  |  |
| --- | --- |
| Акакий | Авдотья |
| Открытое простое число p = 113 | Открытое простое число p = 113 |
| Открытое простое число g = 3 | Открытое простое число g = 3 |
| Секретный ключ a = 15+8 = 23 | Секретный ключ b = 58 |
| Открытый ключ A = | Открытый ключ B = |
| Секретный ключ s = | Секретный ключ s = |
| s=61 | s=61 |

Рисунок 7.1. – Пример генерации секретного ключа.

2.Зашифровать сообщение «хочузачетавтоматом» с использование шифра Цезаря и полученного секретного ключа.



Рисунок 7.2. – Алфавит.

Ключ 1: s = 61; «скупдьубоьюкиьоки».

**Вывод:** Овладел основными криптографическими алгоритмами шифрования. Криптография наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности информации. Помимо этого, современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

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

**Теоретическое введение**

Несмотря на достаточно большое число различных систем с открытыми ключами, одной из наиболее популярных остается криптосистема RSA, созданная в 1977 г. и названная в честь ее создателей Рона Ривеста, Адди Шамира и Леонарда Эйдельмана. Они воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, а разложение на множители произведения двух таких чисел – сложно.

**Ход работы**

|  |  |  |  |
| --- | --- | --- | --- |
| Номер варианта | Сообщение | p | q |
| 15 | DAA | 59 | 43 |

1. Выбирается два простых числа ***p*** и ***q***, например ***p = 59*** и ***q = 43.***
2. Вычисляется произведение ***n = p\*q***, в нашем примере ***n = 59\*43 = 2537.***

Вычисляется функция Эйлера ***φ(n)***

***φ(n) = (p-1)\*(q-1)***

В нашем примере ***φ(n) = (59-1)\*(43-1) = 2436***. Функция Эйлера определяет количество целых положительных чисел, не превосходящих ***n*** и взаимно простых с ***n***.

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, 2537)***
2. 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 (d=1949, k=4)***.

Пара чисел ***(d, n)*** будет закрытым ключом шифра. В нашем примере ***(d, n) = (1949, 2537)***.

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

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

**(5,2537)- открытый ключ.**

**Таблица 2. *Вычисление шифрограммы***

|  |  |  |
| --- | --- | --- |
| **Символы исходного сообщения, *Ti*** | **Коды символов *Ti*(табл. 1)** | **Зашифрованные коды символов*Ci*** |
| D | 68 | ***685mod 2537 = 1701*** |
| А | 65 | ***655mod 2537 = 1286*** |
| A | 65 | ***655mod 2537 = 1286*** |

Рассмотрим пример восстановления исходного сообщения.

***(d, n) = (1949, 2537)-закрытый ключ***.

**Таблица 3. *Восстановление сообщения***

|  |  |  |
| --- | --- | --- |
| **Зашифрованные коды символов *Ci*** | **Дешифрованные коды символов *Ti*(табл. 4.1)** | **Символы исходного сообщения,*Ti*** |
| 1701 | ***17011949mod 2537 = 68*** | D |
| 1286 | ***12861949mod 2537 = 65*** | A |
| 1286 | ***12861949mod 2537 = 65*** | A |

**Вывод:** Несмотря на достаточно большое число различных систем с открытыми ключами, одной из наиболее популярных остается криптосистема RSA. 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 расшифровать принятое сообщение. Овладел навыками работы с криптосистемой RSA.

**Практическое занятие №9**

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

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

**Теоретическое введение**

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.).

Общие положения относятся равным образом и к авторским, и к смежным правам. Они регулируют отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), постановок, исполнений, фонограмм, передач организаций эфирного и кабельного вещания (смежные права).

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

Источниками регулирования авторского права являются как законы РБ, так и международные договоры. Если последними установлены иные правила, чем те, которые содержатся в Законе, то применяются правила международного договора.

Авторское право распространяется как на обнародованные, так и на необнародованные произведения, существующие в какой-либо объективной форме.

**Ответы на вопросы:**

**На какие объекты распространяется авторское право?**

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

**Что относится к личным неимущественным правам?**

* 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).

**Что относится к личным имущественным правам?**

* 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.

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

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

**Каков срок действия авторского права?**

Имущественные права действуют в течение всей жизни автора (соавторов) и 50 лет после его (последнего соавтора) смерти.

**Кто является субъектом авторского права?**

Субъектом авторского права, как правило, является гражданин, творческим трудом которого создано произведение науки, литературы или искусства.

**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.

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.

**Наиболее распространенные виды авторских договоров?**

* изобретательский,
* постановочный,
* сценарный,
* художественного заказа,
* об использовании в промышленности неопубликованного произведения декоративно-прикладного искусства.

**Основные составляющие авторского договора?**

* Предмет договора;
* Срок передачи прав;
* Территория использования прав;
* Цена договора;
* Ответственность сторон;
* Адреса и реквизиты сторон.

**Вывод:** Изучил основные положения авторского права и смежных прав. Общие положения относятся равным образом и к авторским, и к смежным правам. Они регулируют отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), постановок, исполнений, фонограмм, передач организаций эфирного и кабельного вещания (смежные права).

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

**Практическое занятие №10**

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

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

**Теоретическое введение**

Правовая охрана объектов промышленной собственности (ОПС) осуществляется в рамках государственной, а также международных (надгосударственных) патентных систем. Уполномоченные организации выдают от имени государства или группы государств соответствующий охранный документ. 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.

**Ответы на вопросы:**

**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.

**Правила оформления описания 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.

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

* Все части, узлы и детали, составляющие данную конструкцию и показанные на чертеже, пояснены их названия, связи и взаимное расположение.
* Действие (работа) устройства или способ его использования со ссылкой на цифровые обозначения, ранее упомянутых частей, узлов, деталей.
* Примеры описания этого устройства, если они имеются с характеристикой тех или иных преимуществ.
* Сведение подтверждающие возможность описания изобретения относящегося к способу включают указания на последовательность действий.
* Если в формуле изобретения в качестве отличительных признаков приведены параметры режима.
* При описании способа, характеризующегося использованием неизвестных средств, указываются эти средства, и подтверждается их известность до даты Приоритета

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

* документ, подтверждающий уплату патентной пошлины (отмеченная банком копия платежного поручения или квитанция банка), или документ, подтверждающий основания для освобождения от ее уплаты или уплаты в меньшем размере;
* 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).

**Отличия заявок на охранные документы различных объектов промышленной собственности?**

* заявление о выдаче патента с указанием автора (соавторов) промышленного образца и лица (лиц), на имя которого (которых) испрашивается патент, а также их местожительства и местонахождения;
* комплект изображений изделия (макета, рисунка), дающих полное и детальное представление о внешнем виде изделия;
* описание промышленного образца, включающее совокупность его существенных признаков;
* чертеж общего вида изделия, эргономическую схему, конфекционную карту, если они необходимы для раскрытия сущности промышленного образца.

**На какие ОПС выдаются патенты?**

* На полезную модель
* на промышленный образец
* на сорт растений

**На какие ОПС выдаются свидетельства?**

* На товарный знак
* На географические указание на 10 лет с продлением
* на регистрацию топологии интегральной микросхемы

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

**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 классификация (мпк)**

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

**МПК**, кроме того, является:

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

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

По своей структуре МПК разделена на восемь основных разделов.

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

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

**A** – удовлетворение жизненных потребностей человека

**B** – различные технологические процессы; транспортирование

**C** – химия; металлургия

**D** – текстиль; бумага

**E** – строительство; горное дело

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

**G** - физика

**H** - электричество

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

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

Например, в разделе **D** имеются подразделы:

натуральные и химические нити и волокна; прядение; пряжа; окончательная обработка пряжи; ткачество; плетение; изготовление кружев; трикотажно-вязальное производство; нетканые материалы; шитье, вышивание, производство прошивных изделий; обработка текстильных изделий, стирка, эластичные материалы; канаты, тросы или кабели; производство бумаги; производство целлюлозы.

***Класс.*** Каждый раздел делится на классы. Индекс класса состоит из индекса раздела и двузначного числа.

Например: **D 06**

Заголовок класса отражает его содержание.

Например: **D 06** Обработка текстильных изделий; стирка; эластичные материалы, не отнесенные к другим классам

Далее идет разбивка по подклассам, основным группам и подгруппам.

***Полный классификационный индекс.***  Полный классификационный индекс состоит из комбинации символов, используемых для обозначения раздела, класса, подкласса и основной группы или подгруппы.

**Международная классификация промышленных образцов (мкпо)**

**МКПО** служит для классифицирования промышленных образцов и состоит из перечня классов и подклассов, и алфавитного перечня наименований изделий, в котором промышленные образцы объединены с указанием соответствующих им классов и подклассов.

Например: **Класс 02** - предметы одежды, галантерея.

**Международная классификация товаров и услуг (мкту)**

**МКТУ** используется при регистрации товарных знаков либо в качестве основной (единственной), либо вспомогательной классификации. В официальных публикациях о регистрации знаков указываются номера классов **МКТУ** товаров/услуг, в отношении которых зарегистрированы знаки.

Заголовки **классов** указывают в общем виде только области, к которым товары и услуги в принципе могут относиться, и не содержат названия конкретных товаров или услуг.

Для правильной классификации каждого конкретного товара или услуги необходимо пользоваться непосредственно перечнями товаров и услуг и пояснениями к каждому классу.

**Ход выполнения**

Изобретение «бытового нагревательного прибора, отличающегося особенностями расположения электронагревателя и вентилятора». Бытовой нагревательный прибор относится к коммунальной технике и может быть использован для отопления жилых и общественных зданий.

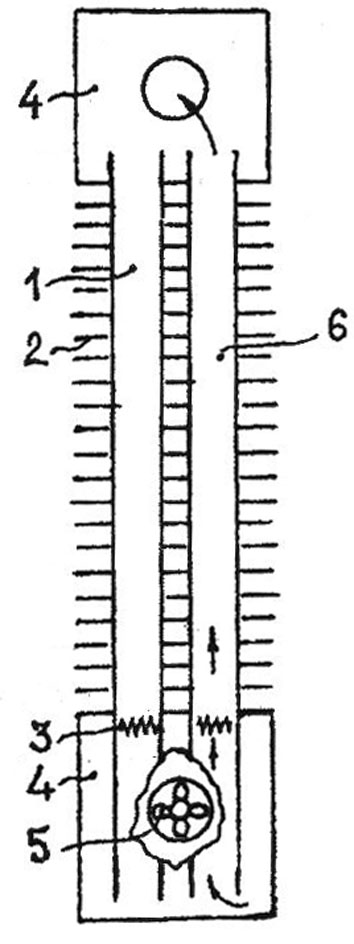


Рисунок 1 - Бытовой нагревательный прибор, содержащий первый канал, имеющий оребрение внешней поверхности. Патент 5596.

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

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

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

* объект – конструкция бытового нагревательного прибора;
* страна поиска – Республика Беларусь;
* источники информации – патентные;
* ретроспективность – 5 лет;

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

Проведенный патентный поиск по указанному классу, выявил следующие аналогичные по конструктивному выполнению патенты и полезные модели, приведенные на рисунках 2 – 5:

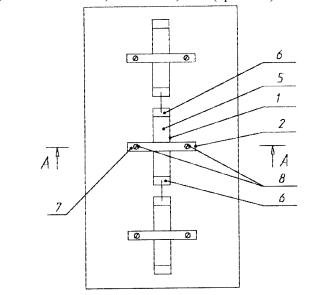


Рисунок 2 – Полезная модель «Пленочный керамический электронагреватель» патент 134

1. Пленочный керамический электронагреватель, содержащий нагревательный элемент, выполненный в виде тонкой диэлектрической подложки с нанесенной на одну из ее сторон резистивной пленкой, на концевых участках которой выполнены площадки контакта, и средство для закрепления нагревательного элемента на нагреваемой поверхности, отличающийся тем, что он дополнительно содержит слой теплопроводного легкодеформируемого материала, расположенный на противоположной резистивной пленке стороне подложки, средство для закрепления выполнено в виде узла для прижима нагревательного элемента к нагреваемой поверхности, который установлен с возможностью контакта с подложкой со стороны резистивного слоя, а тонкая диэлектрическая подложка выполнена из теплопроводной керамики.

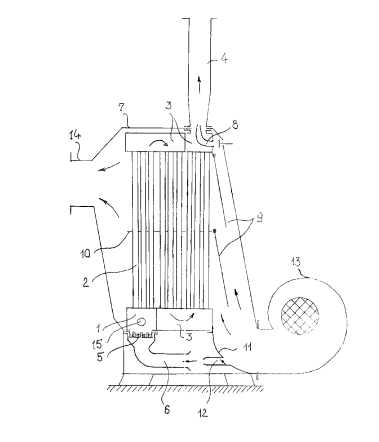


Рисунок 3 – Изобретение «Нагреватель» патент 4995

Нагреватель, содержащий теплообменник, камеру сгорания, дном которой является перегородка, снабженная патрубками со стороны теплообменника, и дымовую трубу, отличающийся тем, что камера сгорания и теплообменник заключены в кожух, соединенный с вентилятором, а на конце теплообменника, противоположном камере сгорания, установлено воздушное сопло, направленное по оси дымовой трубы, при этом в кожухе смонтирована напорная труба, направленная в сторону патрубков перегородки камеры сгорания, причем перегородка камеры сгорания выполнена съемной в виде противня.

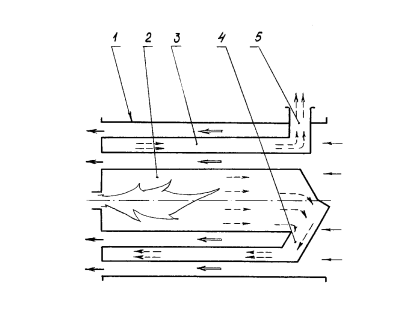


Рисунок 4 – Полезная модель «Нагреватель с кольцевым теплообменником» патент 833

Нагреватель с кольцевым теплообменником с принудительной или естественной циркуляцией теплоносителя, содержащий горизонтально расположенные цилиндрической формы корпус, камеру сгорания, кольцевой теплообменник, патрубок выхода отходящих газов из теплообменника в атмосферу, расположенный в зоне верхних образующих цилиндров теплообменника и корпуса, а также патрубка выхода отходящих газов из камеры сгорания в теплообменник, отличающийся тем, что последний патрубок расположен в зоне нижних образующих цилиндров камеры сгорания и теплообменника и на одной радиальной линии с предыдущим патрубком, а конструктивно выполнен так, что его поверхность омывается холодным теплоносителем.

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 охранного документа или причина его аннулирования (только для анализа патентной чистоты) |
| Нагреватель | Патент РБ  № 134  МПК  6 H 05B 3/00 | Проневич Игорь Иванович. Заявка u 19990101  от 1999.10.05  опубликовано 2000.06.30 | Пленочный керамический электронагреватель | Не действует |
| Патент РБ  № 4995  МПК  7 F 24H 3/02 | Учреждение образования "Брестский государственный технический университет". Заявка a 19981127  от 2000.06.30 | Нагреватель | Не действует |
| Патент РБ  № 833  МПК  7 F 24H 6/00 | Республиканское унитарное предприятие "Мозырский завод сельскохозяйственного машиностроения"  Заявка u 20020190  от 2002.07.08 | Нагреватель с кольцевым теплообменником | Не действует |

Дальнейшая информации, выполняемой специалистами, позволяет определить наличие существенных отличий и возможность получения патента на изобретение или полезную модель.

**Вывод:** в ходе практического занятия я изучил виды, содержание и порядок проведения патентных исследований