Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Основы Защиты Информации**

**Концепция национальной безопасности Республики Беларусь**

Студент: Басалай О.В.

ФИТ 2 курс 9 группа

Преподаватель: Берников В.О.

**Практическое занятие №1**

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

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

***Задание для выполнения***

Ответить на следующие вопросы:

1. Что такое информационная безопасность?
2. Перечислить основные национальные интересы в информационной сфере?
3. Основные угрозы национальной безопасности, связанные с ИТ-сферой?
4. Назвать основные внутренние и внешние источники угроз национальной безопасности в информационной сфере?
5. Основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере?

***Исполнительская часть***

***Информационная безопасность*** – это состояние защищённости информации от несанкционированного доступа к ней, её искажения или уничтожения. Защита как от внутренних, так и от внешних угроз.

***Национальные интересы*** – совокупность потребностей государства по реализации сбалансированных интересов личности, общества и государства, позволяющих обеспечивать конституционные права, свободы, высокое качество жизни граждан, независимость, территориальную целостность, суверенитет и устойчивое развитие Республики Беларусь.

***Основные национальные интересы в информационной сфере:***

* + 1. Реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;
    2. Формирование и поступательное развитие информационного общества;
    3. Равноправное участие Республики Беларусь в мировых информационных отношениях;
    4. Преобразование информационной индустрии в экспортно-ориентированный сектор экономики;
    5. Обеспечение надежности и устойчивости функционирования критически важных объектов информатизации;
    6. Эффективное информационное обеспечение государственной политики.

***Источник угрозы национальной безопасности*** – это фактор или совокупность факторов, способных при определенных условиях привести к возникновению угрозы национальной безопасности.

***Основные угрозы национальной безопасности в сфере ИТ:***

1. Деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;
2. Нарушение функционирования критически важных объектов информатизации;
3. Недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;
4. Снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента.

***Внутренние источники угроз национальной безопасности в информационной сфере:***

1. Распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;
2. 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;
3. Несоответствие качества национального контента мировому уровню;
4. Недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;
5. Рост преступности с использованием информационно-коммуникационных технологий;
6. Недостаточная эффективность информационного обеспечения государственной политики;
7. Несовершенство системы обеспечения безопасности критически важных объектов информатизации.

***Внешние источники угроз национальной безопасности в информационной сфере:***

1. Открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;
2. Доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;
3. Информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;
4. Нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;
5. Развитие технологий манипулирования информацией;
6. Препятствование распространению национального контента Республики Беларусь за рубежом;
7. Широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;
8. Попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

В ***информационной сфере*** с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием ***современных информационно-коммуникационных технологий***.

Государство **гарантирует** обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удалённого, 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.

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

***Вывод:*** я, в ходе выполнения лабораторной работы, изучил концепцию национальной безопасности РБ.

**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 для выполнения:***

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

Вариант: 1;

*E0* = 10000;

*E* = 9000;

K = 5;

C = 500.

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

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

В нашем варианте эффективность функционирования объекта с учетом взаимодействия несанкционированного доступа *E* равна 9000, а величина *E0* равна 10000. Исходя из полученных данных можно выразить величину .

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

Следуя полученному выражению, величина равна 1000.

Формула для вычисления относительной эффективности:

|  |  |
| --- | --- |
|  | (3) |

Следуя данному выражению, относительная эффективность равна 0,9.

Уменьшение эффективности функционирования объекта приведет к материальному ущербу для владельца. Материальный ущерб есть убывающая функция от :

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

Cнижение эффективности функционирования объекта при наличии средств защиты – *ΔЕ3*.

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

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

Cнижение эффективности функционирования объекта при наличии средств защиты равно 200.

Выражения (1) – (2) примут вид:

|  |  |
| --- | --- |
|  | (6) |
|  | (7) |

Величина равна 0,98.

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

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

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

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

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

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

Так как эффективность функционирования объекта имеет стоимостное значение, то величина *Е3* равна 9300.







***Вывод:*** в ходе лабораторной работы были изучены методы решения задач разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

**Практическое занятие №3**

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

Цель: разработать проект политики информационной безопасности бизнес-компании.

**Задание для выполнения.**

Разработать проект политики информационной безопасности бизнес-компании, оформив результаты в виде пояснительной записки. Пояснительная записка может, например, содержать следующие разделы:

1. Титульный лист;
2. Введение (обосновывается важность разработки политики информационной безопасности);
3. Описание структуры бизнес-компании (выбор компании предварительно согласовывается с преподавателем);
4. Оценка рисков;
5. Разработка мер защиты;
6. Выводы.

Электронный вариант вносится в электронную тетрадь и показывается преподавателю для предварительной проверки (объем – 10-20 страниц).

После предварительной проверки пояснительная записка распечатывается и проект политики информационной безопасности бизнес-компании защищается в указанные преподавателем сроки.

Вариант индивидуального задания: университет.

**Введение**

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

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

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

В наш век, в век информационных технологий, эта тема играет немаловажную роль и затрагивает самые различные сферы деятельности человека.

Ни одно учреждение или компания не могут успешно функционировать без использования благ информационного прогресса. Как пример это могут быть:

* Компьютеры;
* Сервера;
* Базы данных;
* Рабочий софт компании;
* Устройства коммуникации.

Надежная защита вычислительной и сетевой корпоративной инфраструктуры является базовой задачей в области информационной безопасности для любой компании.

Самый распространенный вариант контроля несанкционированного доступа – это процесс аутентификации пользователя. Эффективная защита IT инфраструктуры и прикладных корпоративных систем сегодня невозможна без внедрения современных технологий контроля сетевого доступа.

Любая защитная мера есть компромисс между снижением рисков и удобством работы пользователя. При этом любое применение любых защитных мер, касающихся взаимодействия пользователя с информационной системой компании всегда вызывает отрицательную реакцию пользователя. Однако при должном подходе к сотрудникам и четкой формулировке правил обеспечения информационной безопасности такой реакции наблюдаться не должно, что означает о достижении существенного прогресса в данном процессе.

**Описание структуры бизнес-компании**

Сегодня, в условиях широкой доступности Интернета и стремительного развития средств связи, становится очень заметен разрыв между ожиданиями студентов и тем, что могут им предложить учебные заведения. Методы работы в образовании должны постоянно развиваться, следуя за социальными изменениями и технологическим развитием. При этом не на последнем месте находится обеспечение защиты как образовательных материалов и иной информации ограниченного доступа, так и самой ИТ-инфраструктуры от случайных или направленных атак.

Как и любая другая компания, университет имеет свои защищенные от несанкционированного доступа базы данных. Они могут быть наполнены любой информацией: данные сотрудников, студентов, доходы и расходы университета, приобретенные лицензии, научные патенты и так далее.

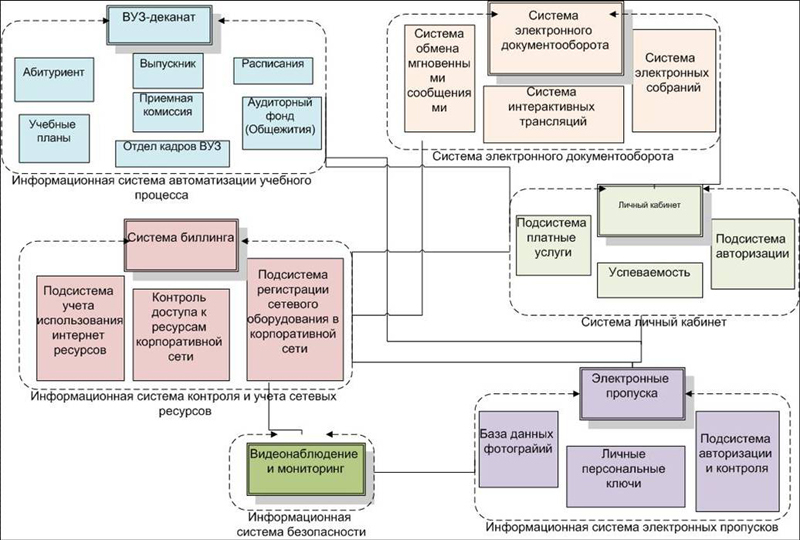
В целом информационная система построена по технологии **«клиент – сервер»** и обеспечивает многопользовательский режим работы в корпоративной вычислительной сети с большим числом терминалов на кафедрах, факультетах, в отделах учебного управления и др.

Рисунок 1.1 – Структура информационной системы ВУЗа

Процесс информатизации управления ВУЗа носит поэтапный характер и опирается на имеющиеся наработки, программные средства и системы.

Ниже перечислены основные положения, которые положены в основу информационной системы управления ВУЗом:

* наличие единой корпоративной сетевой инфраструктуры и единого центра управления разработками, обеспечивающих разработку информационных подсистем, направленных на автоматизацию задач, стоящих перед ВУЗом;
* создание комплексной информационной модели ВУЗа;
* разработка системы, включающей доступ ко всем информационным ресурсам ВУЗа;
* управление персоналом;
* управление персоналом;
* управление учебным процессом;
* повышение эффективности работы, как структурных подразделений, так и ВУЗа в целом;
* упорядочивание и поддержка всех основных процессов сферы деятельности ВУЗа, поднятие их на качественно новый уровень;
* использование современных средств и технологий для разработки общеуниверситетской системы управления: системы управления базами данных, технологии Internet/Intranet, OLAP-технологии, специализированных программных средств, систем управления электронным документооборотом;
* управление документооборотом.

Информационная система ВУЗа позволяет собирать и анализировать данные приема абитуриентов: их количество, проходные баллы, приоритетные направления и не только. Кроме того, отдельные функции и программы единой информационной системы позволяют отслеживать успеваемость и состав студентов, формировать учебные планы, оценивать нагрузку и составлять расписание. Это именно та область, которой информационная система соприкасается с большинством участников образовательного процесса.

Возможности информационной системы ВУЗа позволяют представить движения кадрового и преподавательского состава в масштабах всего вуза, а также ясно видеть структурную организацию отдельных подразделений.  
Благодаря этому централизованно готовятся приказы по назначению на должность, по увольнении или приеме на работу, по начислению заработной платы и пр.

С информационной системой вуза пересекает его ЭИОС — электронная информационно-образовательная среда. ЭИОС включает в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивающей освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся. Можно сказать, что именно ЭИОС является цифровым сердцем университета.

**Основные угрозы и их источники**

Среда угроз сетевой безопасности находится в постоянном развитии. Лидирующие позиции в ней занимают специально написанные, скрытые угрозы, которым все чаще удается преодолевать традиционные методы и средства защиты. Эти угрозы проникают внутрь сети — на уровень ядра, уровень распространения и уровень доступа пользователей, где защита от угроз и их видимость находятся на минимальном уровне. Оттуда эти угрозы без труда выбирают свои цели — конкретные ресурсы и даже конкретных людей в университете. Цель современных кибер-угроз заключается отнюдь не в получении известности и славы и даже не в создании прибыльного ботнета, а в захвате и краже интеллектуальной собственности или коммерческих и иных тайн для достижения конкурентных преимуществ.

Угрозы безопасности могут быть классифицированы по следующим признакам:

* По природе возникновения (искусственные и естественные);
* По степени преднамеренности (случайные и преднамеренные);
* По аспекту информационной безопасности;
* По компонентам, на которые нацелена угроза.

Если рассматривать угрозы подробнее, то для университета имеют право на существование следующие угрозы информационной безопасности:

* Несанкционированный доступ к персональным данным, конфиденциальной информации, и программам, хранящим важные документы. Для образовательных учреждений возможна подмена исходных данных в электронных журналах, личных делах преподавателей и студентов;
* Отрицательное влияние на психику учащегося. Свободный доступ в университете в интернет открывает для детей огромное количество информации, где помимо обучающих и развивающих ресурсов, также присутствуют и ресурсы с нежелательной информацией (материалы порнографического характера, насилия над людьми и животными, пропаганды наркотиков, экстремистской идеологии);
* Чрезмерное использование студентами социальных сетей, следствием чего является разрушение нормального образовательного процесса обучения;
* Кибертерроризм, как новая форма терроризма, возможна и в образовательных учреждениях. Создание безопасной информационно-технологической среды существенно снизит риск кибератаки на объекты образования, которые могут привести к нарушению функционирования управляющих автоматически систем и последующему повреждению инфраструктуры.

Администрация университета хранит на компьютерах персональные данные студентов и преподавателей, приказы и распоряжения, издаваемые в университете, банковские счета студентов и сотрудников, статистику расходов и доходов, данные о патентах и изобретениях, получает и отсылает почту – все это та информация, которая обязана подлежать защите от несанкционированного доступа к ней. Как показывает практика, в образовательных учреждениях защитой данной информации пренебрегают, либо осуществляют на примитивном уровне, устанавливая элементарно вскрываемые пароли (дата рождения, паспортные данные, простейшие наборы упорядоченных символов) при доступе к информационным системам. А отсутствие требований и проверок со стороны государства по построению безопасной информационной системы только усугубляет образовавшуюся проблему.

Основные объекты, которые нуждаются в защите от несанкционированного доступа:

* Бухгалтерские ЛВС;
* Данные финансового отдела;
* Сервера баз данных;
* ftp сервера;
* ЛВС и сервера исследовательских проектов.

**Оценка рисков**

Компьютерные сети ВУЗов – это совокупность сетевых ресурсов для учебной деятельности, рабочих станций персонала, устройств функционирования сети в целом.

Источниками угроз могут стать в первую очередь компьютеризированные лаборатории и учебные аудитории с беспрепятственным доступом в глобальную сеть Интернет. Особую опасность представляют рабочие станции неквалифицированных в сфере информационной безопасности сотрудников.

Анализ информационных рисков можно разделить на следующие этапы:

* Классификация объектов, подлежащих защите, по важности;
* Определение возможных угроз и каналы доступа для атаки информационных систем;
* Определение привлекательности объекта для его взлома;
* Оценка уже существующих мер безопасности данной информационной системы;
* Определение существующих или потенциальных уязвимостей и поиск способов их качественной ликвидации;
* Составление ранжированного списка угроз;
* Оценка ущерба от несанкционированного доступа, атак при отказе обслуживания, сбоев в работе оборудования.

Базовый (*baseline*) анализ рисков – анализ рисков, проводимый в соответствии с требованиями базового уровня защищенности. Прикладные методы анализа рисков, ориентированные на данный уровень, обычно не рассматривают ценность ресурсов и не оценивают эффективность контрмер. Методы данного класса применяются в случаях, когда к информационной системе не предъявляется повышенных требований в области ИБ.

Полный (*full*) анализ рисков – анализ рисков для информационных систем, предъявляющих повышенные требования в области ИБ. Включает в себя определение ценности информационных ресурсов, оценку угроз и уязвимостей, выбор адекватных контрмер, оценку их эффективности.

При анализе рисков, ожидаемый ущерб в случае реализации угроз, сравнивается с затратами на меры и средства защиты, после чего принимается решение в отношении оцениваемого риска, который может быть:

* Снижен, например, за счет внедрения средств и механизмов защиты, уменьшающих вероятность реализации угрозы или коэффициент разрушительности;
* Устранен за счет отказа от использования подверженного угрозе ресурса;
* Перенесен, например, застрахован, в результате чего в случае реализации угрозы безопасности, потери будет нести страховая компания, а не владелец ресурса;
* Принят.

**Разработка мер защиты и мероприятий по внедрению политики безопасности**

Борьба с различными видами атак на информационную безопасность должна вестись на пяти уровнях, причем работа должна носить комплексный характер. Существует ряд методических разработок, которые позволят построить защиту университета на необходимом уровне.

1. Морально-этические средства обеспечения информационной безопасности

В образовательной сфере большую роль играет система морально-этических ценностей. На ней должна основываться система мер, защищающих студента от травмирующей, этически некорректной, незаконной информации. В целях защиты от пропаганды необходимо применять нормы закона «О защите прав ребенка», определяющие его права на защиту от сведений, которые могут причинить моральную травму. Необходимо создавать перечни документов, программ и иных источников, которые могут травмировать психику учащихся, в целях недопущения их проникновения на территорию учебного заведения. Это станет одной из основ информационной безопасности.

### Административно-организационные меры

Этот комплекс мер целиком построен на создании внутренних правил и регламентов, определяющих порядок работы с информацией и ее носителями. Это внутренние методики, посвященные информационной безопасности, должностные инструкции, перечни сведений, не подлежащих передаче. Дополнительно должен быть разработан регламент, определяющий порядок взаимодействия с компетентными органами по запросам о предоставлении им тех или иных данных и документов.

Кроме того, эти методики должны определять порядок доступа студентов к сети Интернет в компьютерных классах, возможность защиты некоторых ресурсов неоднозначного характера от доступа студента, запрет на пользование собственными носителями информации.

### Физические меры

За данную систему мер и ее внедрение должно отвечать руководство образовательного учреждения и сотрудники IT-подразделений. Перекладывать организацию мер физической защиты компьютерной сети и носителей на сотрудников наемных охранных подразделений недопустимо. Среди физических мер должна быть предусмотрена пропускная система защиты в помещения, содержащие носители информации, организация контроля доступа посетителей, установления различных степеней допуска. Кроме того, к мерам физической защиты может быть отнесено обязательное копирование значимой информации на диски компьютеров, не имеющих доступа к сети Интернет. Обязательно не только установление паролей, но и их регулярная замена.

### Технические меры

Комплексную систему защиты всего периметра компьютерной сети должны обеспечивать специализированные программные продукты, например, DLP-системы и SIEM-системы, выявляющие все возможные угрозы безопасности и применяющие меры по борьбе с ними. Для тех учебных заведений, бюджет которых не позволяет внедрение профессиональных систем, необходимо использование разрешенных и рекомендуемых программных мер защиты, в частности антивирусов.

Электронная почта, к которой имеют доступ сотрудники и студенты, должна быть контролируема. Оптимально также ввести полный запрет на копирование любой информации с жестких дисков компьютеров образовательного учреждения.

Кроме того, должно быть предусмотрено программное обеспечение, ограничивающее доступ пользователя на определенные сайты (контент-фильтры).

Все меры должны применяться в комплексе, при этом необходимо определение одного или нескольких лиц, отвечающих за реализацию всех аспектов информационной безопасности.

Некоторые университеты используют свой пул дозвона для выходя в Интернет и используют каналы связи учреждения. Во избежание использования этого доступа посторонними лицами в незаконных целях, работники университета не должны разглашать номер пула, логины и пароли.

Степень защищенности высших учебных заведений в Республике Беларусь оставляет желать лучшего. Причин для этого существует немало, однако основных две. Первая заключается в плохой организации мер по разработке и обеспечению политики информационной безопасности и недооценке важности этих мероприятий. Вторая заключается в недостаточном финансировании закупок оборудования и внедрения новых технологий в сфере информационной безопасности.

**Вывод**

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки. Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Глобализация, являющаяся доминирующей тенденцией современного мирового общества, также влечет за собой и новые риски, вызовы и опасности.

При построении системы защиты информации обязательно нужно определить, что следует защищать и от кого (или чего) следует строить защиту. Защищаться следует от множества угроз, которые проявляются через действия нарушителя. Угрозы возникают в случае наличия в системе уязвимостей, то есть таких свойств информационной системы, которые могут привести к нарушению информационной безопасности.

Определение перечня угроз и построение модели нарушителя являются обязательным этапом проектирования системы защиты. Защищенность информации обеспечивается только при соответствии предполагаемых угроз и качеств нарушителя реальной обстановке. При наличии в системе уязвимости потенциальная угроза безопасности может реализоваться в виде атаки.

Для предупреждения успешных атак необходим поиск и анализ уязвимостей системы. Анализ уязвимостей — обязательная процедура при аттестации объекта информатизации. В связи с возможностью появления новых уязвимостей необходим их периодический анализ на уже аттестованном объекте.

**Практическое занятие №4**

**Тема «Настройка Брандмауэра Windows»**

Цель: Овладение навыками настройки и использования Брандмауэра Windows.

Ход работы:

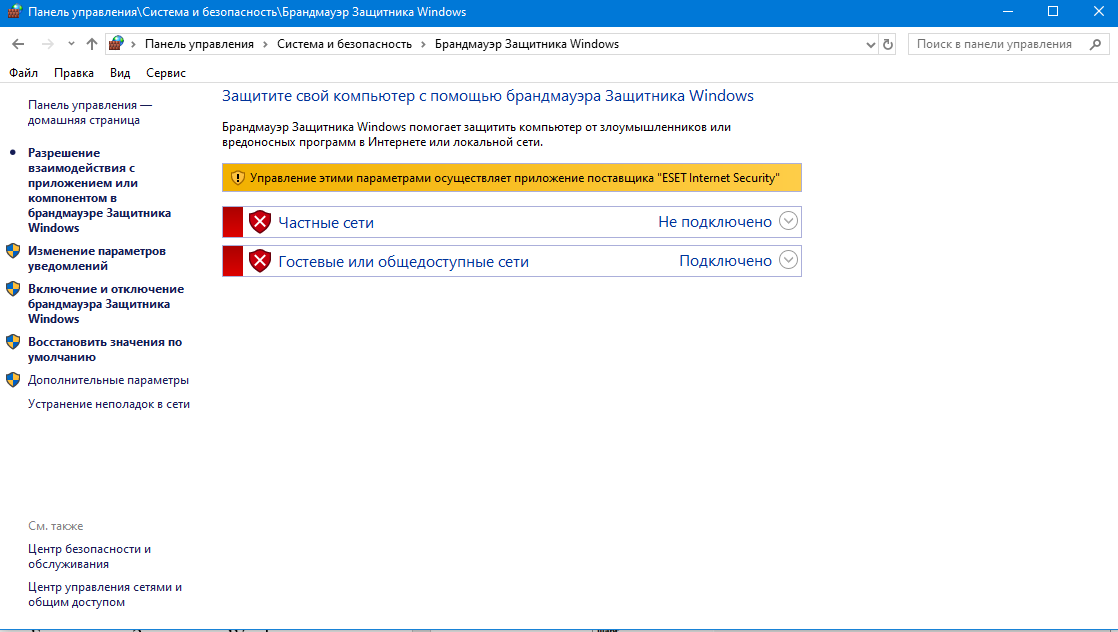
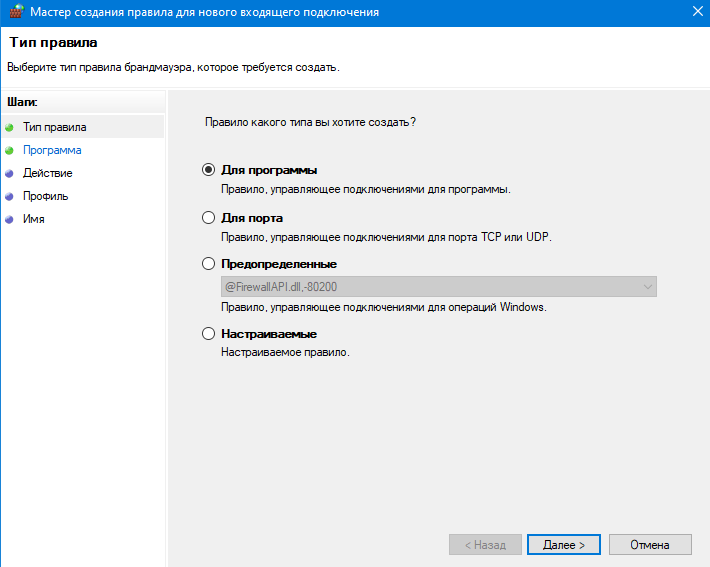
1. **Создать правила для входящих подключений (с помещением в электронный конспект копий экрана с пояснениями промежуточных действий)**

Рисунок 4.1 – Брандмауэр Windows

Так как защиту сети на ПК выполняется при помощи антивируса, некоторые сервисы брандмауэра выпадают в ошибку (рис. 4.1).

Для того, чтобы создать правило для входящих подключений требуется выполнить Панель управления – Система и безопасность – Брандмауэр Защитника Windows – Дополнительные параметры. В открывшемся окне во вкладке Правила для входящих подключений выбираем «Создать правило». В открывшемся окне (рис. 4.2) необходимо выбрать «Для программы». Затем выбрать необходимую программу для исключения. В данном случае исключение будет выполнятся для программы Opera. После выбора программы, выбираем действие (в нашем случае «Блокировать подключение»).

Рисунок 4.2 – Мастер создания правила

В результате мы создали запрещающее исключение для приложения Opera. Аналогичное, но разрешающее исключение создадим для приложения Sony Vegas.

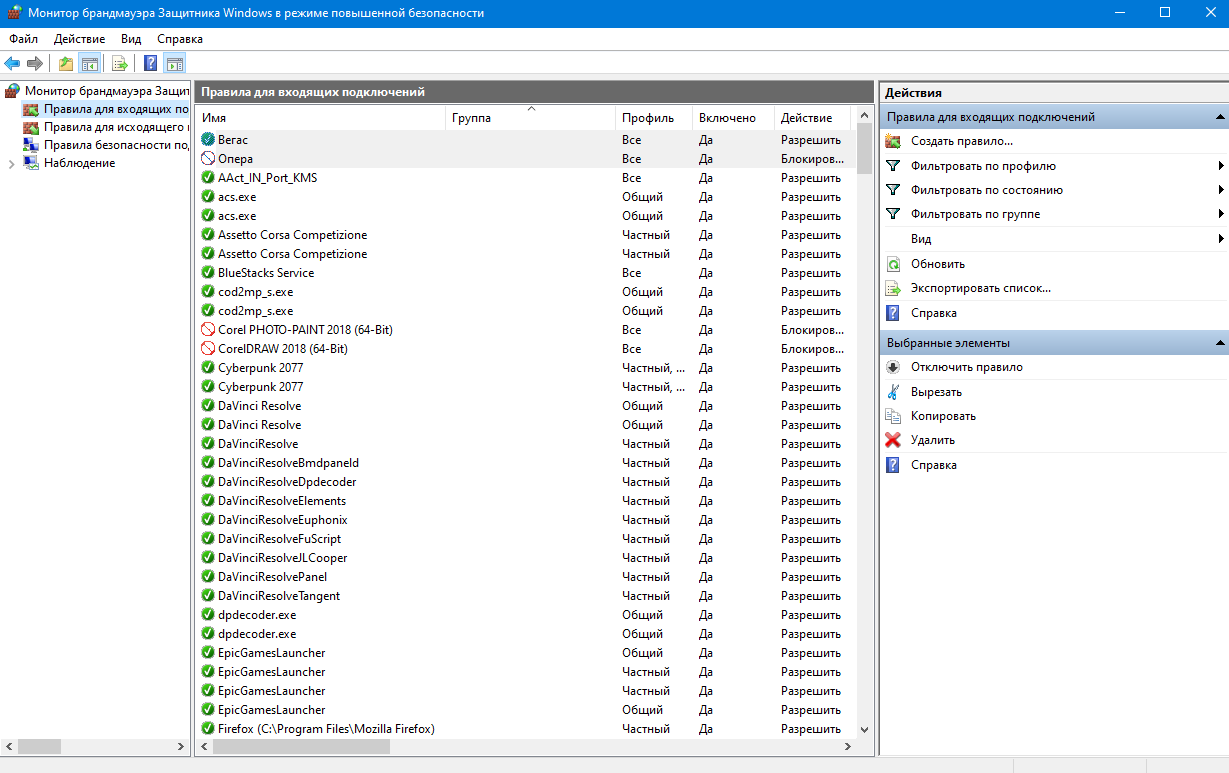
Результат представлен на рисунке 4.3.

Рисунок 4.3 – Результат блокирующих (Block) и разрешающих (Connect) исключений

1. **Создать правила для исходящих подключений (с помещением в электронный конспект копий экрана с пояснениями действий)**

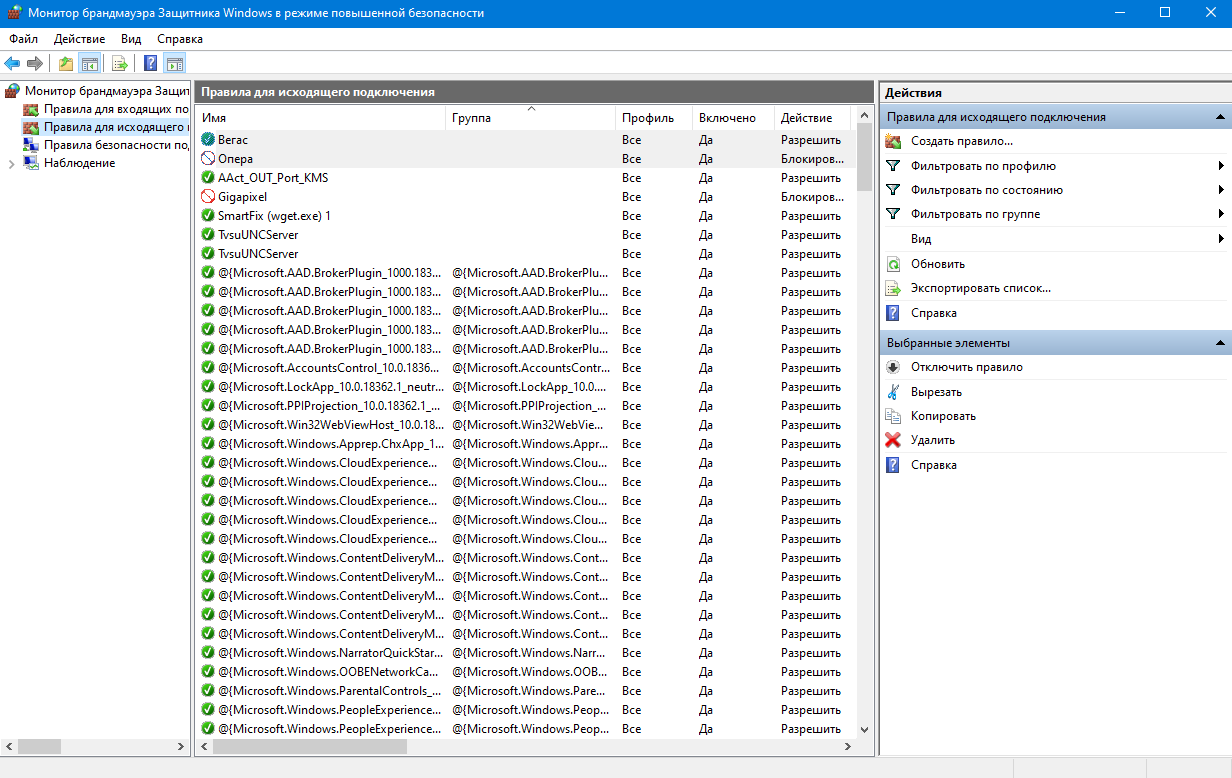
Для создания нового правила для исходящих подключений, требуется во вкладке «Правила исходящего подключения» выбрать «Создать правило». Абсолютно аналогичным способом создаем блокирующие и разрешающие правила для программ Opera и Sony Vegas соответственно. На этом создание исходящих подключений окончено. Результат создания исходящих подключений представлен на рисунке 4.4.

Рисунок 4.4 – Создание исходящих подключений

1. **Вернуть настройки Брандмауэра в исходное состояние до начала выполнения практического задания.**

Для возврата настроек Брандмауэра в исходное состояние требуется выбрать каждое созданное исключение и нажать кнопку «Удалить» либо «Delete».

После выполненных действий Брандмауэр вернется в исходное состояние.

Вывод: в ходе лабораторной работы были изучены навыки настройки и использования Брандмауэра Windows.

**Практическое занятие №5**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами симметричного шифрования.

Ход работы:

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

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

1. Зашифровать сообщение с использованием шифра Цезаря, Трисемуса, Плейфейра и Вижинера и полученного секретного ключа (по номеру варианта и ключевому слову «Защита»). В качестве сообщения использовать свою Фамилию Имя Отчество.

ФИО: Басалай Олег Васильевич.

Используя шифр **Цезаря** и исходный алфавит зашифруем ФИО при помощи ключа 1.

Исходный алфавит: а, б, в, г, д, е, ё, ж, з, и, й, к, л, м, н, о, п, р, с, т, у, ф, х, ц, ч, ш, щ, ъ, ы, ь, э, ю, я.

Шаг смещения: 1.

Басалай = Вбтбмбк;

Олег = Пмёд;

Васильевич = Гбтймэёгйш.

Метод **Трисемуса**

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

Басалай = Жвъвсвп;

Олег = Цсмк;

Васильевич = Йвъдсумйдю.

Метод **Плейфейра**

Разделенный на биграммы текст: ба-са-ла-йъ ол-ег ва-си-ль-ев-ич

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

Басалай = ущ-фз-кщ-лч;

Олег = пк-жд;

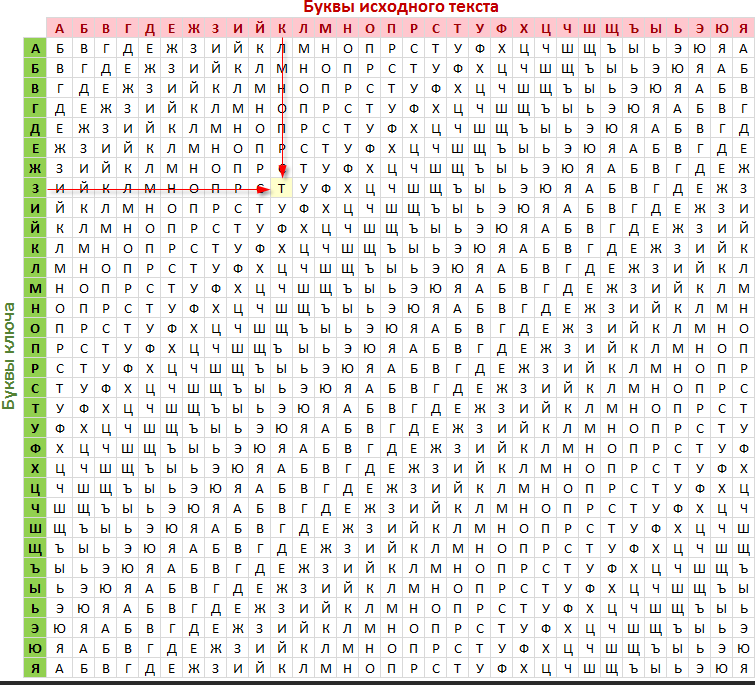
Васильевич = уи-цз-йю-жб-зы.

Метод **Вижинера**

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера.

Басалай = Йблйюбс;

Олег = Цмям;

Васильевич = Кблсюэнгва.

1. Расшифровать сообщение при помощи шифра **Цезаря**

**Исходное сообщение:** Ие михежцчжшйч сшихуцчб, ключ 5.

Исходный алфавит: а, б, в, г, д, е, ё, ж, з, и, й, к, л, м, н, о, п, р, с, т, у, ф, х, ц, ч, ш, щ, ъ, ы, ь, э, ю, я.

**Расшифрованное сообщение:** Да здравствует мудрость.

**Вывод:** в ходе лабораторной работы были изучены основные криптографические алгоритмами симметричного шифрования.

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

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

Протоколы ЭЦП с одной стороны относят к протоколам аутентификации, т.к. гарантируют, что сообщение поступило от достоверного отправителя, а с другой стороны к протоколам контроля целостности, т.к. гарантируют, что сообщение пришло в неискаженном виде.

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

При создании цифровой подписи по классической схеме отправитель:

* применяет к исходному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ r сообщения;
* вычисляет цифровую подпись **s по хеш-образу r с использованием своего закрытого ключа**;
* посылает сообщение **T** вместе с цифровой подписью s получателю.

Получатель, отделив цифровую подпись от сообщения, выполняет следующие действия:

* применяет к полученному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ r сообщения;
* расшифровывает хеш-образ **r’** из цифровой подписи s с использованием открытого ключа отправителя;
* проверяет соответствие хеш-образов r и r’ и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

Как видно из этой схемы, порядок использования ключей обратный тому, который используется при передаче секретных сообщений.

Вначале отправитель использует свой закрытый ключ, а затем получатель применяет открытый ключ отправителя.

Отправка сообщения и ЭЦП на базе алгоритма RSA (рис. 7.1). Первым делом генерируются ключи. Далее Отправитель выполняет отправку сообщения и электронной подписи.

Рисунок 7.1 – Отправка сообщения

Затем выполняетя проверка электронной подписи получателем (рисунок 7.2).

Рисунок 7.2 – Проверка сообщения

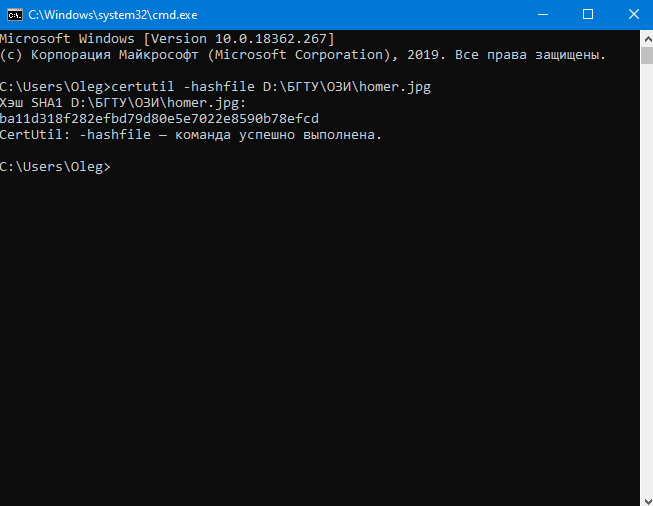
**Практическое задание:**

1. Получить ЭЦП и проверить её подлинность.

Создадим файл *homer.jpg* (рис. 7.3).

Рисунок 7.3 – Созданное изображение

Используя возможности командной строки, узнаем хэш нашего изображения. Для этого выполним операцию certutil –hashfile D:\БГТУ\ОЗИ\homer.jpg (рис. 7.4).

Рисунок 7.4 – хэш изображения

Хэш равен ba11d318f282efbd79d80e5e7022e8590b78efcd.

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

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

**Вариант:** 1.

1-3. *а*=101398751, *b*=326147777.

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

*a* = 101398751 = 311\*326041 = 311\*571\*571;

*b* = 326147777 = 571\*571187 = 571\*607\*941.

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

a меньше b, поэтому поменяем их местами для удобства счета

а) 326147777 = 101398751\*3 + 21951524;

101398751 = 21951524\*4 + 13592655;

21951524 = 13592655\*1 + 8358869;

13592655 = 8358869\*1 + 5233786;

8358869 = 5233786\*1 + 3125083;

5233786 = 3125083\*1 + 2108703;

3125083 = 2108703\*1 + 1016380;

2108703 = 1016380\*2 + 75943;

1016380 = 75943\*13 + 29121;

75943 = 29121\*2 + 17701;

29121 = 17701\*1 + 11420;

17701 = 11420\*1 + 6281;

11420 = 6281\*1 + 5139;

6281 = 5139\*1 + 1142;

5139 = 1142\*4 + 571;

1142 = 571\*2.

**НОД(*b, a*) *=* 571.**

б) *a* = 101398751 = 311\*326041 = 311\*571\*571;

*b* = 326147777 = 571\*571187 = 571\*607\*941.

**НОД(*a, b*) = 571.**

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

НОД(*a, b*) по алгоритму Евклида:

326147777 = 101398751\*3 + 21951524;

101398751 = 21951524\*4 + 13592655;

21951524 = 13592655\*1 + 8358869;

13592655 = 8358869\*1 + 5233786;

8358869 = 5233786\*1 + 3125083;

5233786 = 3125083\*1 + 2108703;

3125083 = 2108703\*1 + 1016380;

2108703 = 1016380\*2 + 75943;

1016380 = 75943\*13 + 29121;

75943 = 29121\*2 + 17701;

29121 = 17701\*1 + 11420;

17701 = 11420\*1 + 6281;

11420 = 6281\*1 + 5139;

6281 = 5139\*1 + 1142;

5139 = 1142\*4 + 571;

1142 = 571\*2.

**НОД(*b, a*) *=* 571.**

Найдём соотношения Безу для данных чисел:

326147777 = 101398751\*3 + 21951524;

21951524 = 326147777 + 101398751\*(-3)

101398751 = 21951524\*4 + 13592655;

13592655 = 101398751 + 21951524\*(-4)

21951524 = 13592655\*1 + 8358869;

8358869 = 21951524 + 13592655\*(-1)

13592655 = 8358869\*1 + 5233786;

5233786 = 13592655 + 8358869\*(-1)

8358869 = 5233786\*1 + 3125083;

3125083 = 8358869 + 5233786\*(-1)

5233786 = 3125083\*1 + 2108703;

2108703 = 5233786 + 3125083\*(-1)

3125083 = 2108703\*1 + 1016380;

1016380 = 3125083 + 2108703\*(-1)

2108703 = 1016380\*2 + 75943;

75943 = 2108703 + 1016380\*(-1)

1016380 = 75943\*13 + 29121;

29121 = 1016380 + 75943\*(-13)

75943 = 29121\*2 + 17701;

17701 = 75943 + 29121\*(-2)

29121 = 17701\*1 + 11420;

11420 = 29121 + 17701\*(-1)

6281 = 5139\*1 + 1142;

1142 = 6281 + 5139\*(-1)

5139 = 1142\*4 + 571;

571 = 5139 + 1142\*(-4)

1142 = 571\*2.

Замена чисел:

571 = 5139 + (6281 + 5139\*(-1))\*(-4) = 5139\*5 + 6281\*(-4);

571 = () + 6281\*(-4) = ;

571 =

1. Найти остаток от деления  на 17.

20052003 = x (mod 17)

2005 = 16 (mod 17)

162003 = x (mod 17)

(-1)2003 = x (mod 17)

-1 = x (mod 17)

x = -1 (mod 17)

x = 16 (mod 17)

**Ответ:** 20052003 = 16 (mod17)

**Практическое занятие №9**

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

Цель: Изучить основные положения авторского права и смежных прав.

**Практическая часть**

1. **На какие объекты распространяется авторское право?**

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

1. Произведения

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

2. Производные произведении

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

3. Компьютерные программы (все виды программ)

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

Авторские нрава распространяются на:

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

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

Авторские права делятся на: личные неимущественные (моральные права - droit moral) и имущественные (экономические) права.

Личные неимущественные права:

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

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

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

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

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

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

Авторское право на составные произведения:

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

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

Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно. Имущественные права действуют в течение всей жизни автора (соавторов) и 50 лет после его (последнего соавтора) смерти.

Общественное достояние по истечении срока действия имущественных прав на объекты авторского права или смежных прав означает переход этих объектов в общественное достояние и может свободно использоваться любым физическим или юридическим лицом без выплаты вознаграждения.

Переход авторского права по наследству, кроме прав авторства, на имя и на защиту репутации автора без ограничения срока.

Автор вправе указать лицо, на которое он возлагает охрану своих личных неимущественных прав после своей смерти и осуществляет свои полномочия пожизненно. При отсутствии указаний охрана осуществляется его наследниками или специально уполномоченным государственным органом РБ при отсутствии наследников.

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?**

Имущественные права автора могут быть уступлены полностью или в части и могут быть переданы по письменному договору, подписанному автором и лицом (правообладателем), которому уступаются имущественные нрава для использования по авторскому договору.

В первом случае авторский договор разрешает использование произведения определенным способом и в установленных договором пределах только лицу, которому эти нрава передаются, и дает такому лицу право запрещать подобное использование произведения другим лицам.

Во втором случае пользователю разрешается использование произведения наравне с обладателем исключительных прав, передавшим такие права, и с другими лицами, получившими разрешение на использование этого произведения таким же способом. Права, передаваемые по авторскому договору, считаются неисключительными, если в договоре прямо не предусмотрено иное.

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.

**Практическое занятие №10**

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

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

**Практическая часть**

1. **Основные составляющие описания изобретения?**

Описание изобретения должно давать точное и ясное представление о новизне, изобретательском уровне и промышленной применимости изобретения.

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

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

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.

Особенности изложения описания устройства:

В этом разделе приводится описание устройства в статическом состоянии со ссылками на фигуры чертежей и цифровые обозначения конструктивных элементов. Цифровые обозначения соответствующих частей, узлов, деталей проставляются но мере их упоминания, в порядке их возрастания, начиная с 1. Этими же числовыми обозначениями должны быть помечены упомянутые части, узлы и детали на чертежах или других графических материалах.

При описании устройства в статическом состоянии должны быть указаны все части, узлы и детали, составляющие данную конструкцию и показанные на чертеже, пояснены их названия, связи и взаимное расположение. При описании действия устройства или способа его использования цифровые обозначения упоминаются в любом порядке, удобном для изложения данной части раздела.

После описания устройства в действии приводятся другие примеры описания этого устройства, если они имеются с характеристикой тех или иных преимуществ.

Особенности изложения описания способа:

Если в формуле изобретения в качестве отличительных признаков приведены параметры режима, например, указан интервал температуры нагревания, и этот интервал сравнительно велик от -20 до +60°С, то следует привести конкретные обоснования граничных значений интервала и привести по одному примеру на оптимальный и граничные значения этого интервала с подробным указанием достигаемого технического результата.

При описании способа, характеризующегося использованием неизвестных средств, указываются эти средства, и подтверждается их известность до даты Приоритета. Для изображения, относящегося к способу получения изделия, элемент которого или само изделие изготовлены из материала неустановленного состава и структуры, приводятся данные о свойствах материала и эксплуатационная характеристика элемента или изделия в целом.

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

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

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

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

**Подача заявки на изобретение (20 лет):**

Заявка на выдачу патента на изобретение подается автором изобретения, нанимателем, если изобретение служебное, физическим или юридическим лицом, которым автор или наниматель передает на договорной основе свое право на подачу заявки или к которому они перешли в соответствии с законодательством Республики Беларусь в наследовании. Она может быть передана через служебного поверенного, зарегистрированного в патентном органе.

Заявки, поступившие в патентный орган, назад не возвращаются.

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.

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

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

Временная правовая охрана заявленному изобретению предоставляется с даты публикации заявки до даты публикации сведений о патенте. До даты публикации сведений о заявке на изобретение, но не позднее даты получения решения о выдаче патента на изобретение возможно по ходатайству преобразование заявки на изобретение в заявку на полезную модель.

Заявку на полезную модель преобразовать в заявку на изобретение возможно до даты получения решения о выдаче патента на полезную модель.

**Подача заявки на полезную модель (10 лет):**

Полезной моделью признается техническое решение, относящееся к устройствам и являющееся новым и промышленно применимым. К устройствам относятся конструкции и изделия.

Заявка на полезную модель должна относиться к одной полезной модели или гpyппу полезных моделей, связанных между собой так, что они образуют единый творческий замысел (требование единства полезной модели).

Заявка на полезную модель должна содержать:

* заявление о выдаче патента с указанием автора (соавторов) полезной модели и лица (лиц), на имя которого (которых) испрашивается патент;
* описание полезной модели, раскрывающее ее с полнотой, достаточной для осуществления;
* формулу полезной модели, выражающую ее сущность и полностью основанную на описании;
* чертежи;
* реферат.

К заявке прилагаются следующие документы:

* 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).

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

**Подача заявки на промышленный образец (5 лет):**

Промышленный образец представляет собой художественное или художественно-конструкторское решение, определяющее внешний вид изделия.

Заявка должна относиться к одному промышленному образцу и может включать его варианты (требование единства промышленного образца).

Заявка должна содержать:

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.

К заявке прилагаются документы:

* 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).

При экспертизе заявки на промышленный образец проверка соответствия заявленного промышленного образца условиям патентоспособности не осуществляется.

**Подача заявки на товарный знак (10 лет):**

Товарные знаки и знаки обслуживания представляют собой обозначения, которые способствуют отличию тоываров или услуг одних юридических или физических лиц от однородных товаров или услуг других юридических или физических лиц.

На каждый товарный знак или знак обслуживания должна быть оформлена отдельная заявка на специальном бланке. Заявка должна содержать сведения о заявителе. В заявке должен быть указан перечень товаров и услуг, для которых регистрируется товарный знак или знак обслуживания. В заявке может содержаться несколько классов товаров и услуг в соответствии с Международной классификацией товаров и услуг (МКТУ). К заявке прилагается графическое изображение товарного знака и описание (при необходимости) с указанием цвета или цветового сочетания, в котором испрашивается регистрация.

К заявке прилагается документ, подтверждающий уплату патентной пошлины в установленном размере.

Союзы, ассоциации и другие объединения юридических лиц могут регистрировать коллективные товарные знаки. Коллективный товарный знак и право на его использование не могут быть переданы другим лицам.

**Подача заявки на регистрацию топологии интегральной микросхемы (10 лет):**

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).

К заявке прилагается 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.

1. **На какие ОПС выдаются патенты?**

Патентная деятельность, полезные модели, промышленные образцы, интегральных микросхем, компьютерные программы, способы, вещества, биотехнологические продукты, применение всего вышеперечисленного.

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

Открытия, научные теории, математические методы, товарные знаки, географические указания.

**Практическое занятие №11**

**Тема «**Патентный поиск**»**

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

**Практическая часть**

**Задание 2**

В результате проведения исследовательских и проектно-конструкторских работ на промышленных предприятиях были разработаны методы испытания материалов. Для реализации этих методов предложены конструктивные решения приборов и приспособлений. В результате модернизации и совершенствования технологических процессов были предложены решения, позволяющие повысить качество и производительность выпускаемой продукции. Предполагается патентование разработок.

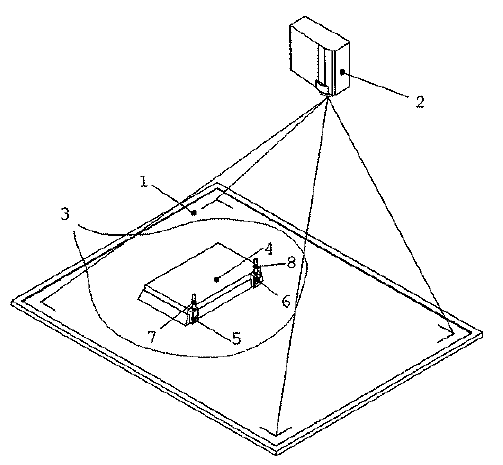
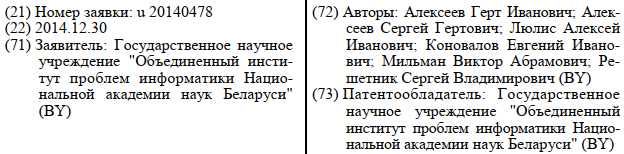
Необходимо выполнить экспертизу патентной чистоты разработанных конструктивных решений: методов испытания материалов и устройств для их осуществления; устройств и механизмов для реализации технологических процессов, представленных на рисунках 1 – 8. Вариант 1.

Рисунок 1 – Разработана интерактивная система сканирования, ввода и визуального отображения графических изображений

Изобретение относится к области информатики и вычислительной техники и может быть использовано для сканирования, дигитайзерного ввода и визуального отображения крупноформатных графических документов (карты и планы местности, снимки земной поверхности, инженерная документация и т.п.) в различных технических приложениях (ГИС-системы, компьютерные классы, средства мониторинга чрезвычайных ситуаций по данным дистанционного зондирования Земли и т.п.).

Известны интерактивные системы ввода и визуального отображения графической информации, содержащие интерактивную доску в составе широкоформатного электромагнитного дигитайзера (далее - дигитайзер) и короткофокусного мультимедийного проектора, оптически связанного с рабочей плоскостью планшета (экраном) этого дигитайзера, взаимодействующие друг с другом в едином комплексе под управлением специализированного программного обеспечения интерактивной доски, будучи подключенными к свободным портам компьютера. При этом многие современные интерактивные доски, выполненные по электромагнитной технологии, способны функционировать в интерактивной системе под управлением двух и большего числа пользователей одновременно (например, при поддержке интерактивного диалога учителя и ученика, находящихся у доски в процессе проведения урока). И каждый из названной пары (учитель - ученик) имеет возможность диалога и управления ресурсами компьютера с помощью своего электронного пера (всего их два) вне зависимости от действий партнера.

Наиболее близким по технической сущности к предлагаемому техническому решению (прототипом) является интерактивная система комбинированного ввода, визуального отображения и редактирования крупноформатных графических изображений ДИСКАН-ИД. Указанная интерактивная система ввода ДИСКАН-ИД включает сканер, проектор, оптически связанный с рабочей плоскостью крупноформатного дигитайзера, выступающего дополнительно в роли экрана полученной таким образом интерактивной доски. Кроме функции обычной интерактивной доски данная система обеспечивает возможности пофрагментного ввода крупноформатных графических изображений с последующим сведением (сшивкой) полученных сканерных данных в растровую копию всего введенного документа. К недостаткам системы ДИСКАН-ИД следует отнести большой объем и сложность электронного оборудования, включающего блок сопряжения дигитайзера и сканера с дополнительными индукционными датчиками координат, встраиваемыми в сканер при его модернизации. К тому же модернизация сканера получается достаточно "глубокой", требующей технологически сложной механической обработки несущей конструкции сканера для монтажа дополнительных датчиков координат.

**Практическое занятие №12**

**Тема «Патентный поиск»**

Цель: освоить навыки проведения патентного поиска по заданной тематике.

**Практическая часть**

Тема курсового проекта «Автостоянка».

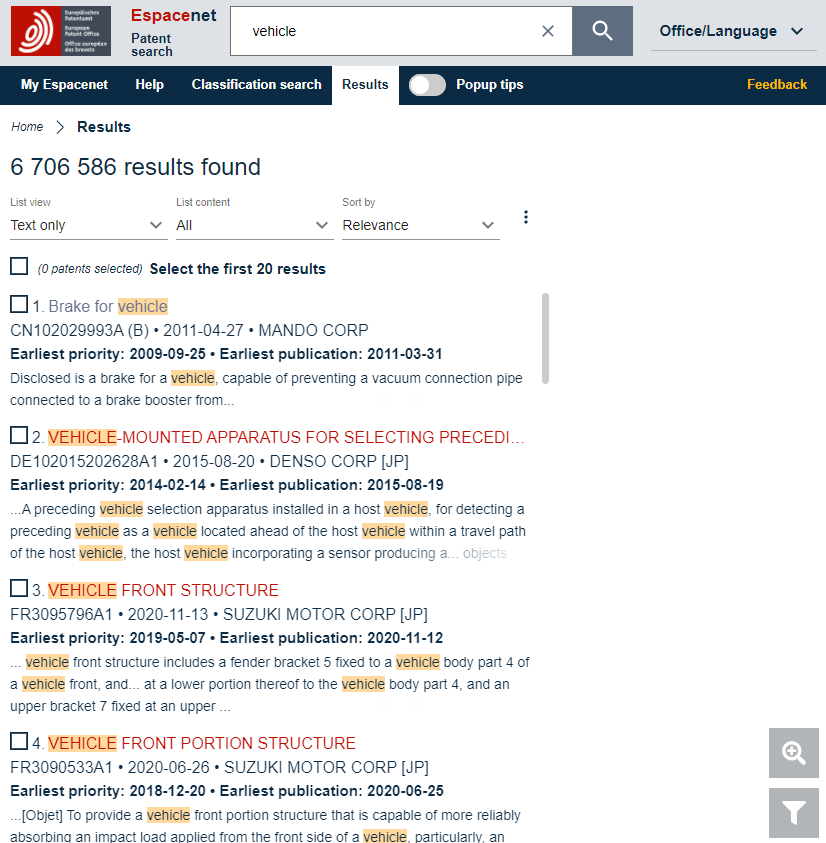
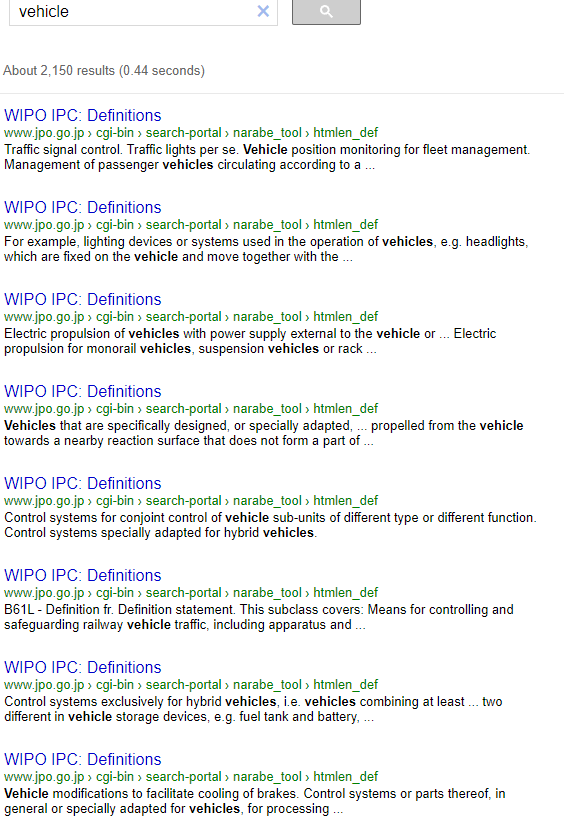
Поиск выполняется по ключевому слову «Автомобиль» или «Vehicle».

Рисунок 12.1 – Поиск на сайте [http://www.epo.org](http://www.epo.org/)

Рисунок 12.2 – Поиск на сайте [www.jpo.go.jp](http://www.jpo.go.jp)

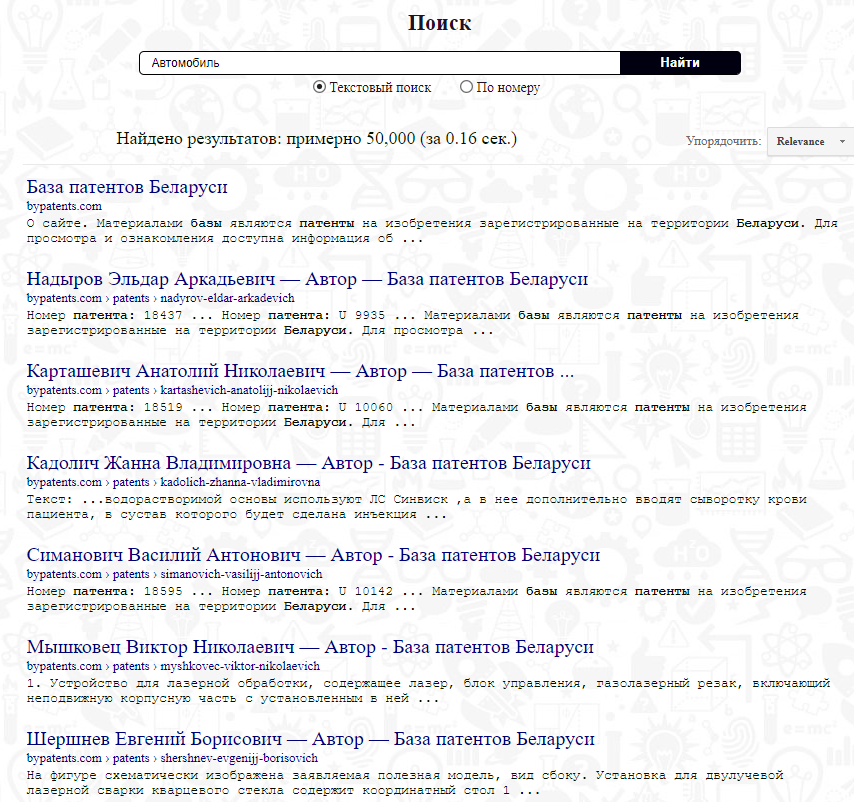


Рисунок 12.3 – Поиск на сайте bypatents.com



Рисунок 12.4 – Поиск на сайте patents.su

Вывод: при патентном поиске патенты, относящиеся к теме моего курсового проекта найдены не были.

**Практическое занятие №13**

**Тема «**Настройка антивирусов**»**

Цель: Овладение навыками настройки и использования различных антивирусов.

**Практическая часть**

1. Установить и настроить антивирусную программу по варианту.

По варианту требуется установить антивирусную программу Avast.

Рисунок 13.1 – Первоначальное окно установщика

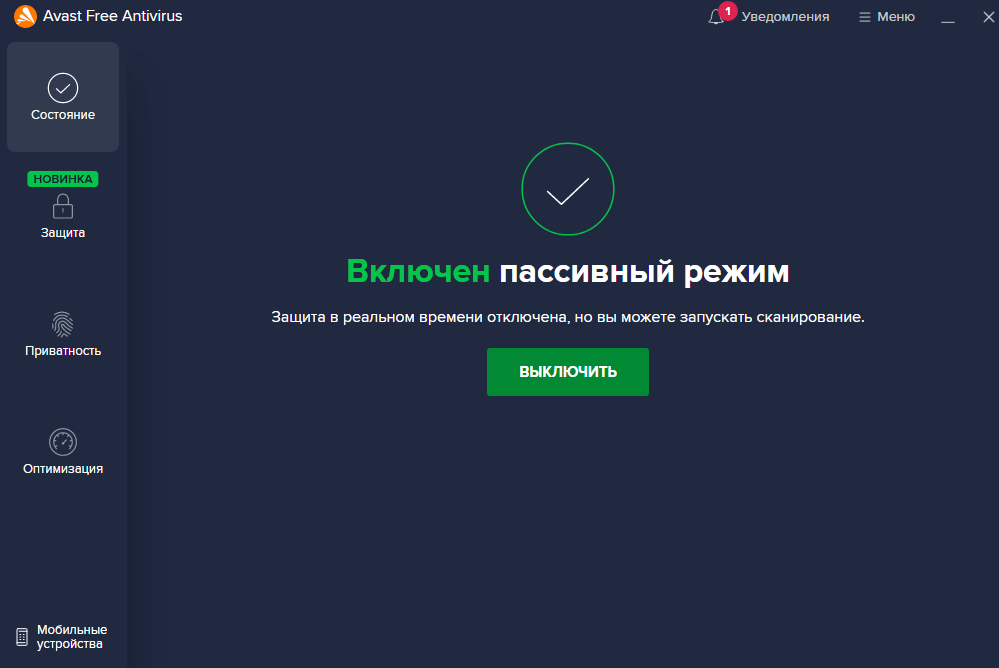
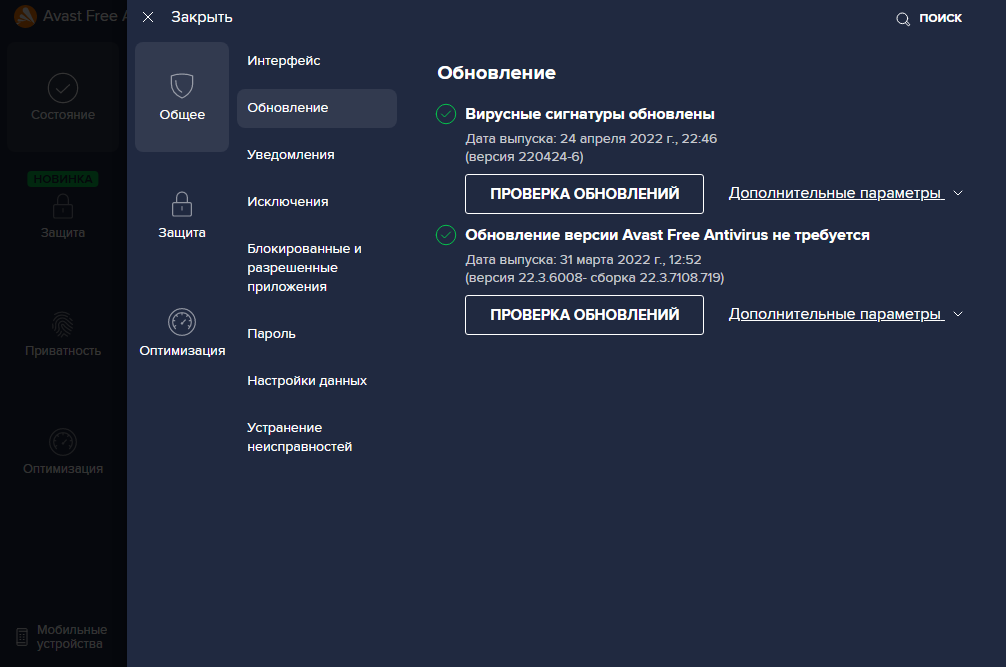


Рисунок 13.2 – Главная страница антивируса

1. Обновить базу данных сигнатур вирусов.

В моём случае были установлены актуальные версии баз данных сигнатур вирусов, поэтому обновление не требуется.

Рисунок 13.3 – База данных сигнатур вирусов

1. Выполнить сканирование дисков.

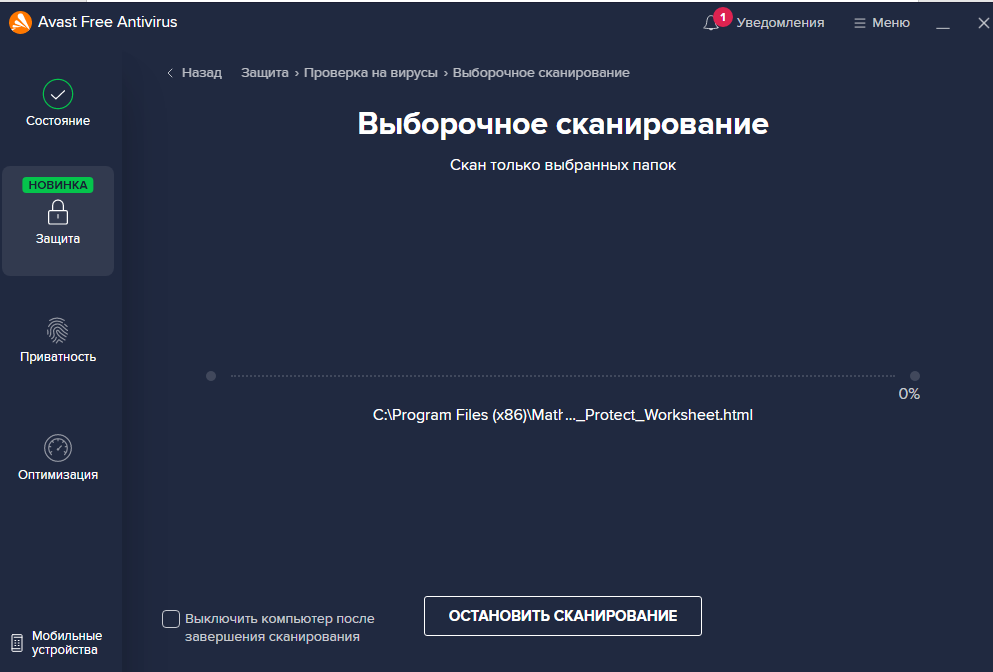
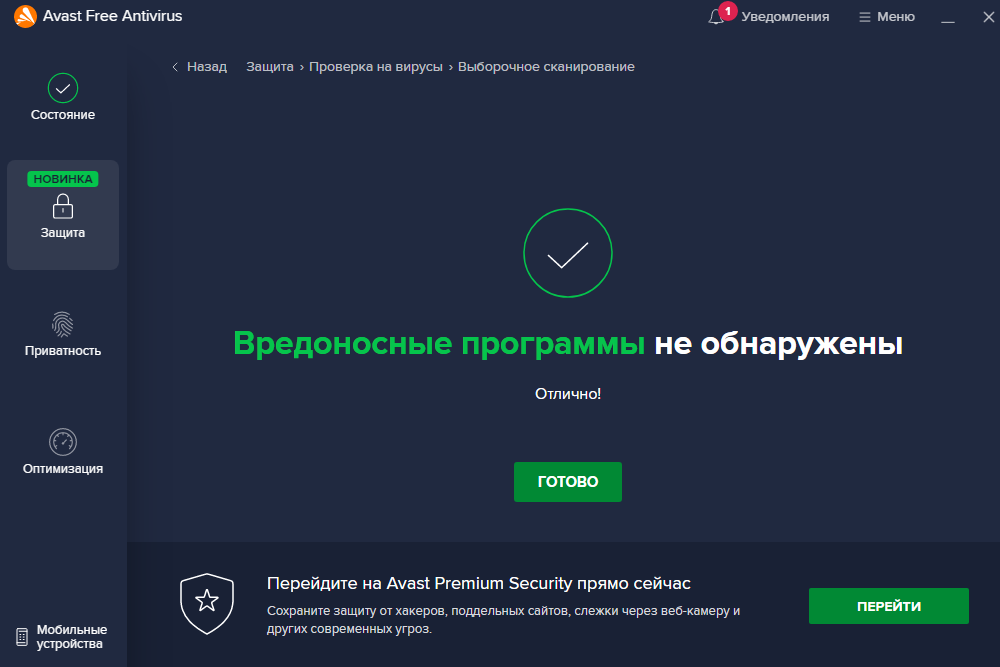
Выполним сканирование дисков. В данном случае выполним полное сканирование диска C (рисунок 13.4).

Рисунок 13.4 – Процесс сканирования диска C

Рисунок 13.5 – Результат сканирования

В результате сканирования угроз обнаружено не было (рисунок 13.5).

**Практическое занятие №14**

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

Цель: Изучить модель криптографии .NET Framework, Основные классы и структуры данных, разработать приложение для шифрования файлов использующих симметричные и ассиметричные алгоритмы шифрования

**Практическая часть**

* 1. **Какие симметричные алгоритмы шифрования Вы знаете?**

Алгоритмы Цезаря, Трисемуса, Плейфейра, Вижинера.

* 1. **Какие ассиметричные алгоритмы шифрования Вы знаете?**

Алгоритмы RSA, Эль-Гамаля, Деффи-Хеллмана.

* 1. **Основное назначение библиотеки System.Security.Cryptography?**

Открывает доступ к криптографическим сервисам. Можно шифровать и расшифровывать данные, обеспечивать их целостность и получать цифровую подпись.

* 1. **Влияет ли размер ключа на криптостойкость алгоритма?**

Да, влияет. К примеру, симметричный ключ длиной 40 бит расшифровывается сетью из нескольких компьютеров за сутки методом перебора чисел. Такой ключ называют слабым.

На расшифровку ключа длиной 64 бит понадобится намного больше компьютеров и такой ключ будет расшифровываться на протяжении нескольких недель. Мероприятие достаточно дорогостоящее, но хозяин барин.

Сильным ключом считается ключ длиной 128 бит.

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

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

Класс CspParameters представляет параметры, которые можно передавать управляемым криптографическим классам, использующим службы шифрования (CSP), с помощью интерфейса Microsoft Cryptography API (CAPI). Классы, имена которых заканчиваются на "CryptoServiceProvider", являются оболочками управляемого кода для соответствующего CSP.

Класс CspParameters используется для выполнения следующих задач:

- задание конкретного CSP путем передачи типа поставщика свойству ProviderType или ProviderName. Можно также задать CSP с помощью перегруженной версии конструктора;

- создание контейнера ключей, в котором можно хранить криптографические ключи. Контейнеры ключей предоставляют самый безопасный способ хранения криптографических ключей и позволяют скрыть их от злоумышленников;

- определение с помощью свойства KeyNumber типа создаваемого асимметричного ключа: ключ подписи или ключ обмена.

Класс RSACryptoServiceProvder - выполняет шифрование и дешифрование данных с помощью реализации асимметричного алгоритма RSA, предоставляемого поставщиком служб шифрования (CSP). Позволяет выполнить экспорт, импорт данных ассиметричной пары ключей. Поддерживаются ключи длиной от 384 до 16384 бит с приращениями по 8 бит, если установлен Microsoft Enhanced Cryptographic Provider, и ключи длиной от 384 до 512 бит с приращениями по 8 бит, если установлен Microsoft Base Cryptographic Provider.

Пространство имен Cryptography содержит базовый класс HashAlgorithm и производные классы, поддерживающие алгоритмы [MD5](https://ru.wikipedia.org/wiki/MD5), [SHA1](https://ru.wikipedia.org/wiki/SHA1), [SHA256](https://ru.wikipedia.org/wiki/SHA256), [SHA384](https://ru.wikipedia.org/wiki/SHA384) и [SHA512](https://ru.wikipedia.org/wiki/SHA512). [Алгоритм](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC) [MD5](https://ru.wikipedia.org/wiki/MD5) дает 128 битный [хеш](https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88), a [SHA1](https://ru.wikipedia.org/wiki/SHA1) — 160 битный

Класс CryptoStream – определяет поток, который связывает потоки данных с криптографическими преобразованиями.

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