Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Электронная тетрадь**

по дисциплине «Основы защиты информации»

Студентка: Ездакова П.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?

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

1. Перечислить основные национальные интересы в информационной сфере?

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

- реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;

- формирование и поступательное развитие информационного общества;

- равноправное участие Республики Беларусь в мировых информационных отношениях;

- преобразование информационной индустрии в экспортно-ориентированный сектор экономики;

- эффективное информационное обеспечение государственной политики;

- обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

1. Основные угрозы национальной безопасности, связанные с ИТ-сферой?

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

- деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;

- нарушение функционирования критически важных объектов информатизации;

- возникновение на территории Республики Беларусь либо вблизи ее границ крупномасштабных чрезвычайных ситуаций природного и техногенного характера, эпидемий и эпизоотии;

- снижение научно-технологического и образовательного потенциала до уровня, не способного обеспечить инновационное развитие;

- недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;

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

1. Назвать основные внутренние и внешние источники угроз национальной безопасности в информационной сфере?

В информационной сфере **внутренними источниками** угроз национальной безопасности являются:

- распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;

- зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;

- несоответствие качества национального контента мировому уровню;

- недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;

- рост преступности с использованием информационно-коммуникационных технологий;

- недостаточная эффективность информационного обеспечения государственной политики;

- несовершенство системы обеспечения безопасности критически важных объектов информатизации.

В информационной сфере **внешними источниками** угроз национальной безопасности являются:

- открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;

- доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;

- информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;

- нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;

- развитие технологий манипулирования информацией;

- препятствование распространению национального контента Республики Беларусь за рубежом;

- широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;

- попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

1. 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.

**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.

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

**Практическое занятие №2**

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

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

**Задание на выполнение**

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E*0 | *E* | *K* | *C* |
| 1 | 10000 | 9000 | 5 | 500 |
| 2 | 100000 | 90000 | 50 | 5000 |
| 3 | 20000 | 18000 | 10 | 1000 |
| 4 | 15000 | 12000 | 2 | 1000 |
| 5 | 11000 | 9500 | 3 | 1500 |
| 6 | 12000 | 11000 | 6 | 300 |
| 7 | 13000 | 12000 | 5 | 600 |
| 8 | 16000 | 13000 | 6 | 1000 |
| 9 | 17000 | 15000 | 7 | 800 |
| 10 | 18000 | 15000 | 6 | 900 |
| 11 | 19000 | 17000 | 4 | 800 |
| 12 | 21000 | 18000 | 3 | 900 |
| 13 | 22000 | 17000 | 10 | 1000 |
| 14 | 25000 | 20000 | 8 | 2000 |
| 15 | 26000 | 20000 | 7 | 3000 |
| 16 | 30000 | 25000 | 10 | 3000 |
| 17 | 20000 | 19000 | 5 | 500 |
| 18 | 110000 | 91000 | 50 | 5000 |
| 19 | 27000 | 20000 | 10 | 1000 |
| 20 | 25000 | 12000 | 2 | 1000 |
| 21 | 31000 | 25000 | 3 | 1500 |
| 22 | 32000 | 26000 | 6 | 3000 |
| 23 | 33000 | 22000 | 5 | 6000 |
| 24 | 26000 | 23000 | 6 | 1000 |
| 25 | 22000 | 20000 | 6 | 1000 |
| 26 | 23000 | 20000 | 5 | 1000 |

**Вариант 8**

В условии задачи имеется эффективность функционирования объекта с учетом воздействия несанкционированного доступа *Е* и положительный эффект при нормальном (идеальном) функционировании *Е0*. Тогда величина *∆Е* будет равна:

|  |  |
| --- | --- |
| => *E = E0 – E = 16000 – 13000 = 3000* | (2.1) |

В итогевеличина *∆Е* = 3000. Относительная эффективность:

|  |  |
| --- | --- |
| = 1 – 3000/16000 = 0.8125 | (2.2) |

Величина δ = 0.8125. Уменьшение эффективности функционирования объекта приводит к материальному ущербу для владельца объекта. В общем случае материальный ущерб есть некоторая неубывающая функция от ΔЕ:

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

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:

|  |  |
| --- | --- |
| = 3000/6 = 500 | (2.4) |

Величина ΔЕ3 = 500. Выражения (1) – (2) примут вид:

|  |  |
| --- | --- |
| = 16000 – 500 = 15500 | (2.5) |
| = 15500/16000 = 0.96875 | (2.6) |

Величина δ3 соответственно равны 0.96875.

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

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

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

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

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

|  |  |
| --- | --- |
| = 16000 – 3000/6 – 1000 = 14500 | (2.9) |

Величина *Е3* = 14500.

Так как эффективность функционирования объекта имеет стоимостное значение, то величина *Е3* равна 14500.

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

**Вывод:** в ходе лабораторной работы мынаучились решать задачи по разработке средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

## Лабораторная работа №3

По теме «Разработка политики информационной безопасности оператора мобильной связи МТС»

Студентка: Ездакова П.В.

ФИТ 2 курс 9 группа

Преподаватель: Берников В.О.

**Введение**

**Политикой информационной безопасности** (ИБ) называется комплекс мер, правил и принципов, которыми в своей повседневной практике руководствуются сотрудники предприятия/организации в целях защиты информационных ресурсов.

За время, прошедшее с возникновения самого понятия ИБ, наработано немало подобных политик – в каждой компании руководство само решает, каким образом и какую именно информацию защищать.

Для чего нужна формализация защиты информации:

Политика безопасности является обязательной составляющей определенных стандартов (местных или международных). Необходимо соответствие конкретным требованиям, которые обычно выдвигают внешние аудиторы, изучающие деятельность организации. Отсутствие политики безопасности порождает отрицательные отклики, а подобные оценки негативно влияют на такие показатели, как рейтинг, уровень надежности, инвестиционная привлекательность и т. д.

Материалы об информационной безопасности появляются на свет, когда высший менеджмент сам приходит к пониманию необходимости структурированного подхода к теме защиты информации. Такие решения могут быть воплощены в жизнь после внедрения технических средств, когда появляется осознание того, что данными средствами надо управлять, они должны быть под постоянным контролем. Зачастую ИБ включает в себя и проблематику взаимоотношений с персоналом (сотрудник может рассматриваться не только как лицо, подлежащее защите, но и как объект, от которого информация должна быть защищена), иные аспекты и факторы, выходящие за рамки исключительно защиты компьютерной сети и предотвращения несанкционированного доступа к ней.

Наличие соответствующих положений говорит о состоятельности организации в вопросах информационной безопасности, ее зрелости. Четкая формулировка правил обеспечения информационной безопасности является свидетельством того, что в данном процессе достигнут существенный прогресс.

**Описание структуры бизнес-компании**

**Сотовая связь** – способ передачи данных по радиоканалам между точками, одна из которых относится к категории мобильных. Название телекоммуникационной технологии связано с разделением зоны покрытия на условные шестиугольные ячейки. Один ретранслятор (BTS-станция) создает покрытие на 3 «соты» через равное или кратное количество антенн.

Как правило, операторы мобильных сетей предлагают своим клиентам пакеты услуг для решения различных задач (звонки, СМС, Интернет). Сотовая сеть является одним из самых распространенных в наше время видов мобильной радиосвязи. Ключевой особенностью является то, что зона покрытия оператора разбивается на отдельные ячейки.

Белорусско-российское совместное ООО «**Мобильные ТелеСистемы**» (**МТС**)  – белорусский [оператор сотовой связи](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80_%D1%81%D0%BE%D1%82%D0%BE%D0%B2%D0%BE%D0%B9_%D1%81%D0%B2%D1%8F%D0%B7%D0%B8). Предоставляет услуги связи стандарта  [GSM 900/1800](https://ru.wikipedia.org/wiki/GSM), [UMTS](https://ru.wikipedia.org/wiki/UMTS) ([WCDMA](https://ru.wikipedia.org/wiki/WCDMA)/[HSDPA](https://ru.wikipedia.org/wiki/HSDPA)/[HSUPA](https://ru.wikipedia.org/wiki/HSUPA)/[HSPA+](https://ru.wikipedia.org/wiki/HSPA%2B)) и [4G](https://ru.wikipedia.org/wiki/4G) (через сеть beCloud), первый по численности [абонентов](https://ru.wikipedia.org/wiki/%D0%90%D0%B1%D0%BE%D0%BD%D0%B5%D0%BD%D1%82) [оператор сотовой связи](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80_%D1%81%D0%BE%D1%82%D0%BE%D0%B2%D0%BE%D0%B9_%D1%81%D0%B2%D1%8F%D0%B7%D0%B8) в [Белоруссии](https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D0%BB%D0%BE%D1%80%D1%83%D1%81%D1%81%D0%B8%D1%8F) (Структура представлена на рисунке 1.1.**)**. Основные виды деятельности компании МТС:

* оказание услуг связи (в том числе eSIM-карты);
* розничная торговля гаджетами и аксессуарами;
* сдача имущества в аренду (субаренду).

Рисунок 1.1­ Структура бизнес-компании МТС

ИС выступает как система, в которой есть два компонента: **объект**, **субъект**.

**Объект** – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

**Субъект** – активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

Для оператора сотовой связи объектами информационной системы выступают: документы об оказании услуг клиентам; носители, хранящие информацию о клиентах; различные базы данных, архивы и т.д. Это значит, что мы предоставляем оператору сотовой связи свои персональные данные, которые как раз-таки вносятся в базы данных и хранятся у оператора.

**Персональные данные** – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

В начальную анкету входят следующие данные:

* ФИО;
* Пол;
* Возраст (дата рождения);
* Место рождения;
* Прописка;

Пользуясь мобильным номером, абонент пополняет свое «личное дело» — карточку у оператора. С активных SIM-карт постоянно поступает следующая информация о:

* расходах и пополнениях счета;
* направлении вызовов, SMS-сообщений;
* содержании сообщений и звонков, переписке в большинстве мессенджеров;
* трафике (посещенных сайтах, просмотренных фильмах, скачанных файлах, использованных приложениях и т.д.);
* подписках, то есть основных увлечениях абонентах, вплоть до самых сокровенных;
* совершенных онлайн-покупках;
* местоположении с точностью до метра даже при заблокированной геолокации.

Эти данные автоматически поступают оператору связи при включении и выключении мобильного устройства, а также при перемещении в другую соту. Вручную подобный запрос оператор связи может сделать в любой момент.

Дополнительно фиксируются:

* IMEI мобильного устройства, модель;
* номер SIM-карты;
* ID соты. Это необходимо для контроля нахождения в роуминге и осуществления верной тарификации.

Целью Правил является обеспечение надлежащей защиты информации о пользователях, в том числе их персональных данных, от несанкционированного доступа и разглашения.

**Субъектами** информационной системы являются компания сотовой связи, которая может инициировать поток информации, в частности личные данные клиента; также клиент, которому предоставлен доступ к Приложению, который предлагает сотовый оператор.

В ходе существования компании могут возникать различные проблем с утечкой информации, несанкционированный доступ к данным, которые должны быть остаться конфиденциальными. Для этого необходимо грамотно подойти к политике безопасности компании, чтобы избегать проблем в будущем

**Основные угрозы и их источники**

**Угроза информационной безопасности объекта** – возможные воздействия на него, приводящие к ущербу. Данный объект имеет определенные свойства, одним из которых является **уязвимость**. Уязвимость – некоторое свойство объекта, делающие возможным возникновение и реализацию угрозы.

**Атака**– действие злоумышленников, заключающееся в поиске и использовании той или иной уязвимости. Угроза, как следует из определения, – это опасность причинения ущерба, то есть в этом определении проявляется жесткая связь технических проблем с юридической категорией, каковой является «ущерб».

Природа воздействий на информационный объект бывают непреднамеренными и преднамеренными, однако все воздействия могут привести к последствиям 3-х видов:

* нарушение конфиденциальности;
* нарушение доступности;
* нарушение целостности.

**Нарушение конфиденциальности** – нарушение свойства информации быть известной только определенным субъектам.

**Нарушение целостности** – несанкционированные изменения, искажения, удаления информации.

**Нарушение доступности** – нарушаются доступ к информации, работоспособность объекта, доступ в который получил злоумышленник.

**Информационная безопасность** – это всегда комплексная система, все составляющие которой призваны не допустить утечки конфиденциальных сведений по техническим каналам, а также воспрепятствовать стороннему доступу к носителям информации. Все это, соответственно, гарантирует целостность данных при работе с ними: обработке, передаче и хранении, которые должны осуществляться обязательно в правовом поле. Грамотно организованные технические мероприятия позволяют определить использование специальных электронных приспособлений несанкционированного снятия информации, размещенных как в помещении, так и в средствах связи.

Под угрозой информационной безопасности объекта будем понимать возможные воздействия на него, приводящие к ущербу. Такие угрозы можно классифицировать:

По виду:

* физической или логической ценности
* конфиденциальности
* доступности
* права собственности

По происхождению:

* Случайные (непреднамеренные);
* Преднамеренные.

**Непреднамеренные угрозы** – это действия, которые совершают люди по неосторожности, незнанию, невнимательности или из любопытства. К такому типу угроз относят установку программных продуктов, которые не входят в список необходимых для работы, и в последствии могут стать причиной нестабильной работы системы и потеря информации.

**Преднамеренные** угрозы-угрозы, связанные со злым умыслом преднамеренного физического разрушения, впоследствии выхода из строя системы. К преднамеренным угрозам относятся внутренние и внешние атаки.

По источникам:

* Люди
* Техническое устройство
* Алгоритмы, программы
* Внешнее влияние (среда)

В свою очередь, информационные угрозы могут быть обусловлены:

* Естественными факторами
* Человеческими факторами.

Человеческие факторы в свою очередь подразделяются на угрозы, несущие случайный неумышленный характер и угрозы умышленного характера, которые делятся на активные/неактивные и внутренние/внешние.

**Пассивные угрозы** направлены на несанкционированное использование информационных ресурсов (прослушивание).

**Активные угрозы** имеют цель: нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на информационные ресурсы.

Внутренние угрозы: утечки информации, неавторизированный доступ.

Внешние угрозы: вредоносные программы (вирусы, троянцы, черви), атаки хакеров, DOS-атаки, DDOS-атаки, таргетированные атаки, спам, фишинг, бутнет (зомби-сети), шпионские ПО.

Случайные угрозы обусловлены недостаточной надежностью программных ресурсов.

Преднамеренные угрозы связаны с действием людей. К преднамеренным угрозам относятся внутренние и внешние атаки. Для того чтобы риск таких случаев был минимален, необходимо, чтобы каждый сотрудник организации соответствовал, так называемому, «статусу благонадежности».

**Оценка рисков**

Чтобы заложить фундамент системы управления рисками, нужно выбрать за основу один из общепринятых подходов:

* **Активный** – установление максимального контроля над существующими угрозами, предполагает инвестиции в поддержание системы управления.
* **Адаптивный** – приспособление хозяйственной деятельности к внешним условиям, что позволяет контролировать только часть неопределенностей.
* **Консервативный** – локализация убытков, нейтрализация их влияния на работу предприятия, при этом затраты на управление угрозами минимальны, но возможный ущерб может оказаться критичным.
* **Комплексный** или интегрированный – объединение нескольких подходов, обеспечивает высокую гибкость в управлении риском, но требует инвестиций для разработки такой системы.

В целом, жизнеспособны все подходы. Но **комплексный** – самый универсальный и результативный, хотя затраты на его воплощение велики. Им обычно пользуются в крупных компаниях, особенно промышленных. Там инвестиции в формирование и внедрение системы риск-менеджмента, заточенной под особенности конкретного предприятия, являются оправданными.

Для компании сотовой связи основные **угрозы** это:

* ущерб репутации организации;
* неприятности, связанные с нарушением действующего законодательства;
* ущерб, связанный с разглашением персональных данных отдельных лиц;
* финансовые потери от разглашения информации;
* финансовые потери, связанные с восстановлением ресурсов;
* потери, связанные с невозможностью выполнения обязательств;

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

Задача управления рисками включает выбор и обоснование выбора контрмер, позволяющих снизить величины рисков до приемлемых. Главным является разработка такой защиты, которая при максимальной эффективности требовала минимальной стоимости. Ведь чем выше и сложнее защита, тем выше стоимость.

При этом важно понимать, что экономить на защите нельзя, ведь потеря данных и их восстановление потребуют куда больше убытков чем хорошая дорогостоящая защита.

**Снижение рисков** за счет использования контрмер может осуществляться различными способами:

* уменьшением вероятностей осуществления угроз безопасности;
* ликвидацией уязвимостей или уменьшением их величин;
* уменьшением величины возможного ущерба;
* восстановлением ресурсов, которым был нанесен ущерб;
* выявлением атак и других нарушений безопасности.

Задачи систем [информационной](https://arinteg.ru/articles/organizatsiya-sistemy-informatsionnoy-bezopasnosti-26382.html) безопасности предприятия многообразны:

* обеспечение защищённого хранения информации на разных носителях;
* защита данных, передаваемых по каналам связи;
* разграничение доступа к различным видам документов;
* создание резервных копий, послеаварийное восстановление информационных систем и т.д.

Обеспечение информационной безопасности предприятия возможно только при системном и комплексном подходе к защите. В системе ИБ должны учитываться все актуальные компьютерные угрозы и уязвимости.

Полноценная информационная безопасность предприятий и организаций подразумевает непрерывный контроль в реальном времени всех важных событий и состояний, влияющих на безопасность данных. Защита должна осуществляться круглосуточно и круглогодично и охватывать весь жизненный цикл информации от её поступления или создания до уничтожения или потери актуальности.

Группа технических средств защиты информации совмещает аппаратные и программные средства. Основные:

* резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе – на регулярной основе;
* дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных;
* создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;
* обеспечение возможности использовать резервные системы электропитания;
* обеспечение безопасности от пожара или повреждения оборудования водой;
* установка программного обеспечения, которое обеспечивает защиту баз данных и другой информации от несанкционированного доступа.

В комплекс технических мер входят и меры по обеспечению физической недоступности объектов компьютерных сетей, например, такие практические способы, как оборудование помещения камерами и сигнализацией.

Чтобы исключить неправомерный доступ к информации применяют такие способы, как идентификация и аутентификация.

**Идентификация** – это механизм присвоения собственного уникального имени или образа пользователю, который взаимодействует с информацией.   
 **Аутентификация** – это система способов проверки совпадения пользователя с тем образом, которому разрешен допуск.

Эти средства направлены на то, чтобы предоставить или, наоборот, запретить допуск к данным. Подлинность, как правила, определяется тремя способами: программой, аппаратом, человеком. При этом объектом аутентификации может быть не только человек, но и техническое средство (компьютер, монитор, носители) или данные. Простейший способ защиты – пароль.

Компаниям следует использовать современные эффективные средства защиты:

* Системы централизованного управления обновлениями и патчами для используемого ПО. Для правильной приоритизации планов по обновлениям необходимо учитывать сведения об актуальных угрозах безопасности.
* Системы антивирусной защиты со встроенной изолированной средой («песочницей») для динамической проверки файлов, способные выявлять и блокировать вредоносные файлы в корпоративной электронной почте до момента их открытия сотрудниками и другие вирусные угрозы. Наиболее эффективным будет использование антивирусного ПО, построенного на решениях одновременно нескольких производителей, способного обнаруживать скрытое присутствие вредоносных программ и позволяющего выявлять и блокировать вредоносную активность в различных потоках данных  – в почтовом, сетевом и веб-трафике, в файловых хранилищах, на веб-порталах. Важно, чтобы выбранное решение позволяло проверять файлы не только в реальном времени, но и автоматически анализировало уже проверенные ранее, это позволит выявить не обнаруженные ранее угрозы при обновлении баз сигнатур.
* SIEM-решения  – для своевременного выявления и эффективного реагирования на инциденты информационной безопасности. Это позволит своевременно выявлять злонамеренную активность, попытки взлома инфраструктуры, присутствие злоумышленника и принимать оперативные меры по нейтрализации угроз.
* Автоматизированные средства анализа защищенности и выявления уязвимостей в ПО.
* Межсетевые экраны уровня приложений (web application firewalls)  –  в качестве превентивной меры защиты веб-ресурсов.
* Системы глубокого анализа сетевого трафика  – для обнаружения сложных целевых атак как в реальном времени, так и в сохраненных копиях трафика. Применение такого решения позволит не только увидеть не обнаруженные ранее факты взлома, но и в режиме реального времени отслеживать сетевые атаки, в том числе запуск вредоносного ПО и хакерских инструментов, эксплуатацию уязвимостей ПО и атаки на контроллер домена. Такой подход позволит существенно снизить время скрытного присутствия нарушителя в инфраструктуре, и тем самым минимизировать риски утечки важных данных и нарушения работы бизнес-систем, снизить возможные финансовые потери от присутствия злоумышленников.
* Специализированные сервисы анти-DDoS.

Позаботьтесь о безопасности клиентов:

* повышайте осведомленность клиентов в вопросах ИБ;
* регулярно напоминайте клиентам о правилах безопасной работы в интернете, разъясняйте методы атак и способы защиты;
* предостерегайте клиентов от ввода учетных данных на подозрительных веб-ресурсах и тем более от сообщения такой информации кому бы то ни было по электронной почте или во время телефонного разговора;
* разъясняйте клиентам порядок действий в случае подозрений о мошенничестве;
* уведомляйте клиентов о событиях, связанных с информационной безопасностью.

**Вывод**

Информационные технологии стали неотъемлемой частью нашей жизни, но, как и любая система она должна иметь свою политику безопасности. Любая система имеет уязвимости, а задача информационной безопасности обеспечить наименьшее количество уязвимостей.

Следует понимать, что экономить на политике безопасности нельзя! Если произойдет такое, что злоумышленники выявят уязвимость, то устранение последствий может выйти намного дороже чем, чем затраты на защиту.

В современном мире полноценная защита информаций является частью успешного бизнеса. Ведь, чем меньше возможность похитить/удалить данные, тем больше средств уйдет на восстановление тех самых данных. Не будем забывать про ущерб, который будет нанесен пользователям тех самых данных, ведь при заключении договора компания обязывается хранить данные, которые предоставляет пользователь. Он дает личное согласие на распоряжение своими персональными данными, а это значит, что при утечке договор нарушается.

Дабы избежать лишних проблем в будущем, компаниям следует больше времени и средств уделять политике безопасности.

**Практическое занятие №4**

**Тема «**Настройка Брандмауэра Windows**»**

Цель: Овладение навыками настройки и использования Брандмауэра Windows.

**Задание к выполнению**

1. Создать правила для входящих подключений (с помещением в электронный конспект копий экрана с пояснениями промежуточных действий):
   1. Для 1 программы (по выбору) на блокировку подключения;
   2. Для 1 программы (по выбору) на разрешение подключения;
2. Создать правила для исходящих подключений (с помещением в электронный конспект копий экрана с пояснениями действий):
   1. Для 1 программы (по выбору) на блокировку подключения;
   2. Для 1 программы (по выбору) на разрешение подключения;
3. Вернуть настройки Брандмауэра в исходное состояние до начала выполнения практического задания.
4. Опробовать действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий)

**Теоретическое введение**

**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.

Межсетевой экран является одним из основных компонентов защиты сетей. Наряду с Internet-протоколом межсетевого обмена межсетевой экран является одним из важнейших средств защиты, осуществляя надежную аутентификацию пользователей и защиту от несанкционированного доступа. Большая часть проблем с информационной безопасностью сетей связана с "прародительской" зависимостью коммуникационных решений от ОС. Вследствие этого ряд Internet-служб и совокупность сетевых протоколов имеет "бреши" в защите.

Настройки межсетевого экрана, т.е. решение пропускать или отсеивать пакеты информации, зависят от топологии распределенной сети и принятой политики информационной безопасности. В связи с этим политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Эти правила базируются на двух общих принципах – запрещать всё, что не разрешено в явной форме, и разрешать всё, что не запрещено в явной форме. Использование первого принципа дает меньше возможностей пользователям и охватывает жёстко очерченную область сетевого взаимодействия. Политика, основанная на втором принципе, является более мягкой, но во многих случаях она менее желательна, так как она предоставляет пользователям больше возможностей "обойти" межсетевой экран и использовать запрещенные сервисы через нестандартные порты (User Data Protocol – UDP), которые не запрещены политикой безопасности.

**Выполнение заданий**

Создаем правило для нового входящего подключения (на блокировку)

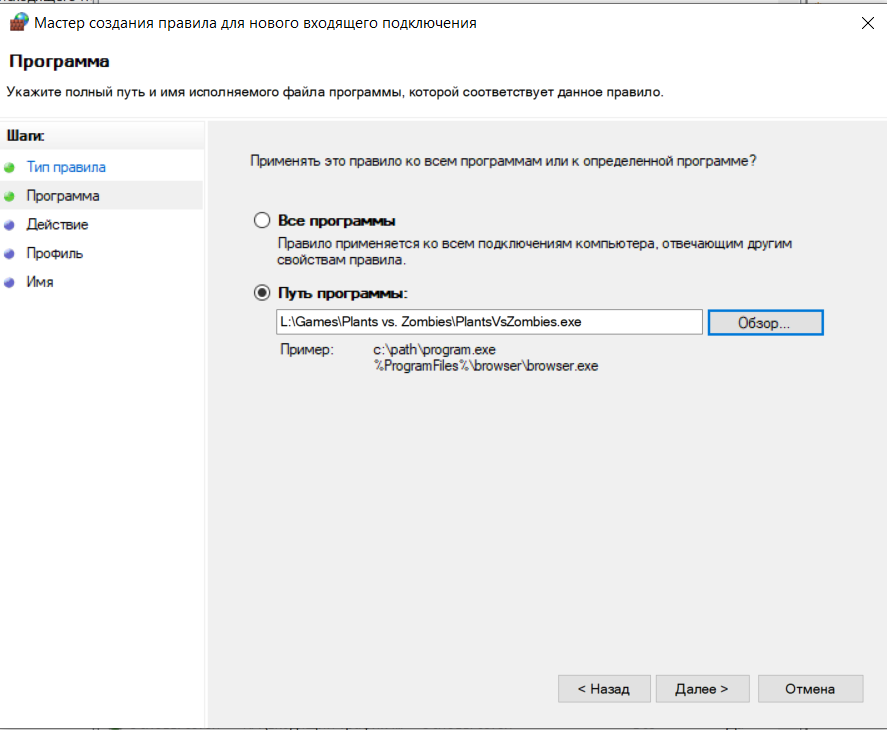


Рисунок 1 – Создание правила

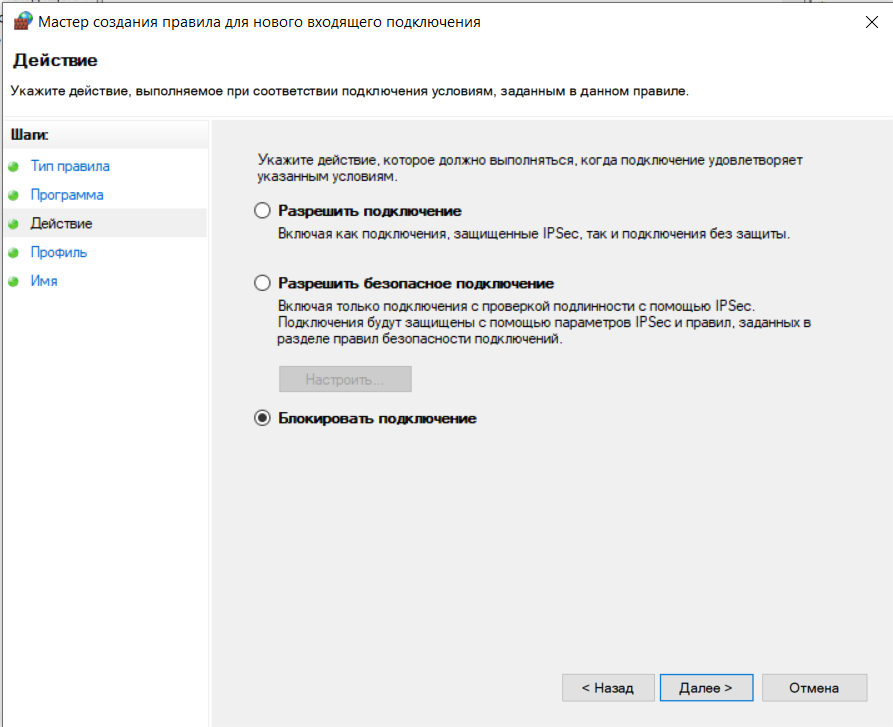


Рисунок 2 – Выбор действия

Мы можем выбрать нужные нам правила для профилей, а можем запретить для всех.

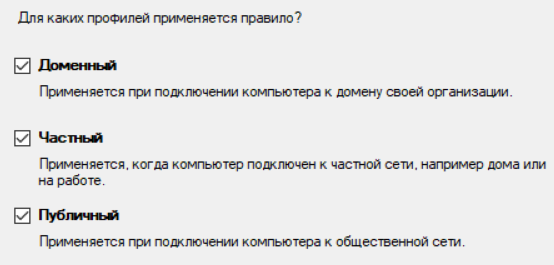


Рисунок 3 – Окно выбора профилей

Далее, мы задаем имя и нажимаем «готово»:

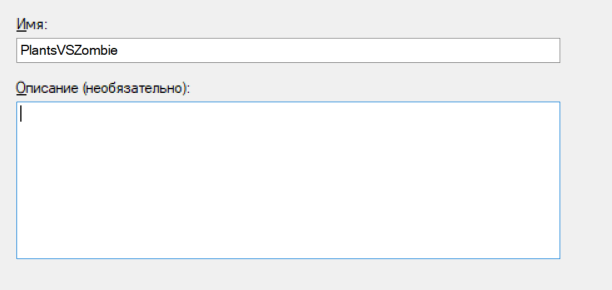


Рисунок 4 – Окно ввода имени

В общем списке появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели.

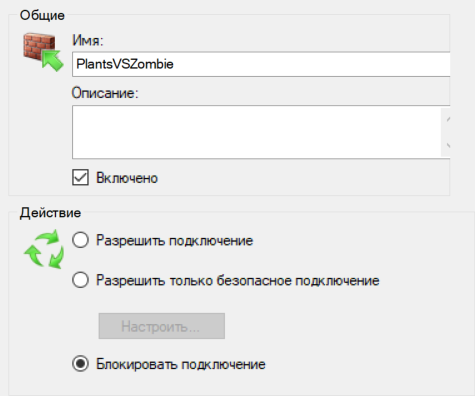


Рисунок 5 – Окно свойства

Теперь создаем подключение для другой программы на разрешенные подключения. Делаем все то же самое, что и делали выше, но вместо блокировки разрешаем.

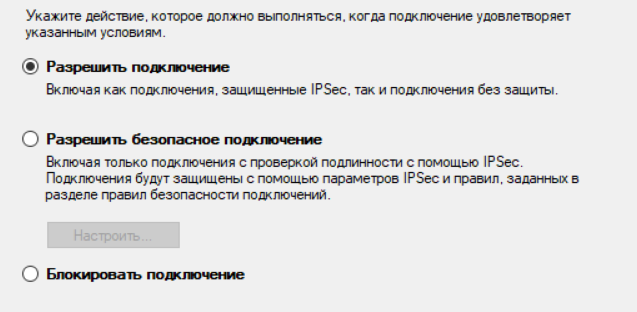
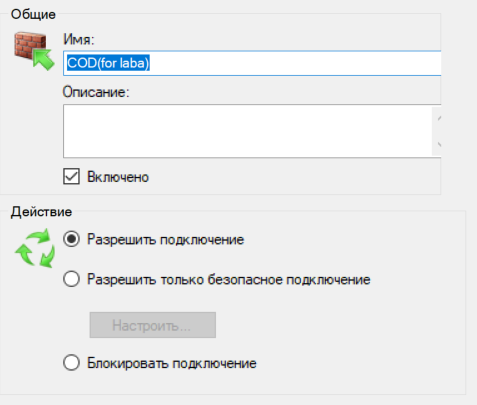
 

Рисунок 6 – Окно выбора действий и окно свойств

Теперь настраиваем для исходящего подключения. Принцип тот же:

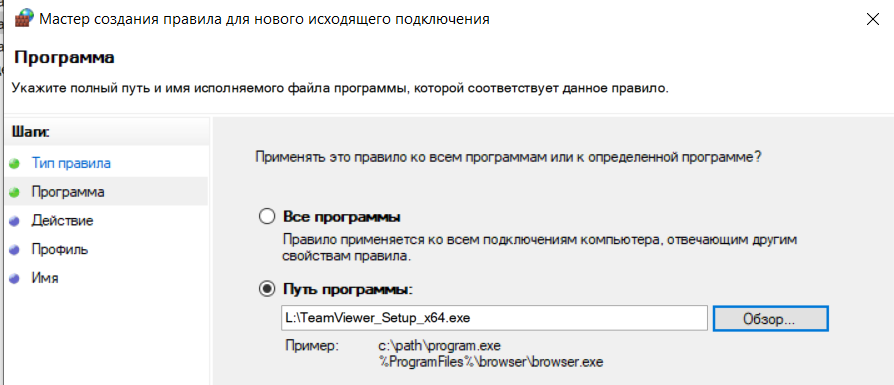


Рисунок 7 – Создание правила исходящего подключения

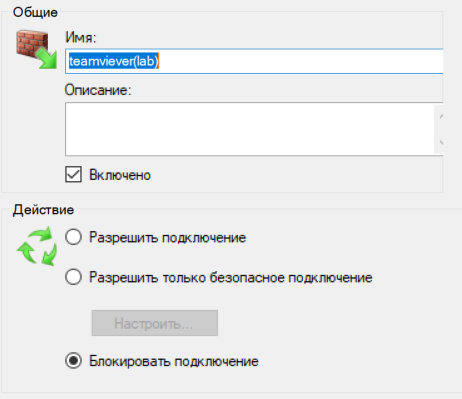


Рисунок 8 – Окно свойств исходящего подключения

Затем разрешеннное подключение:

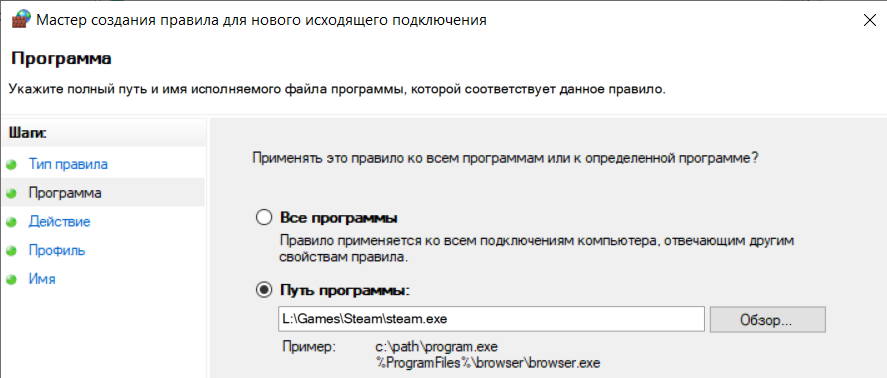


Рисунок 9 – Создание правила исходящего подключения

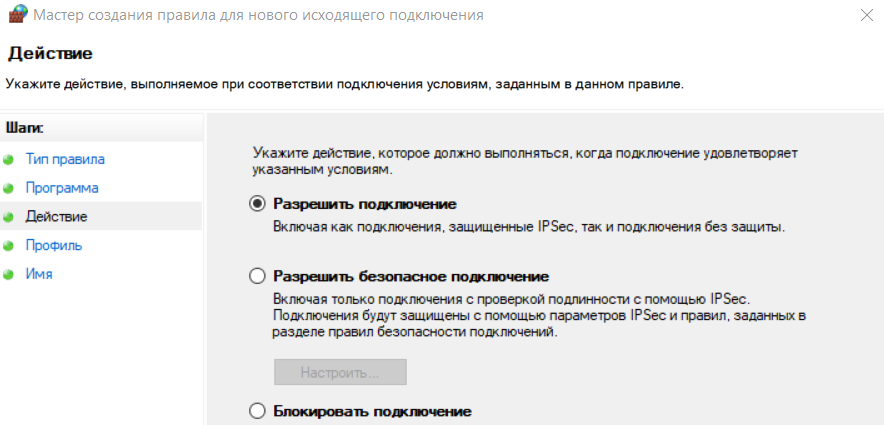


Рисунок 10 – Окно действий для правила исходящего подключения

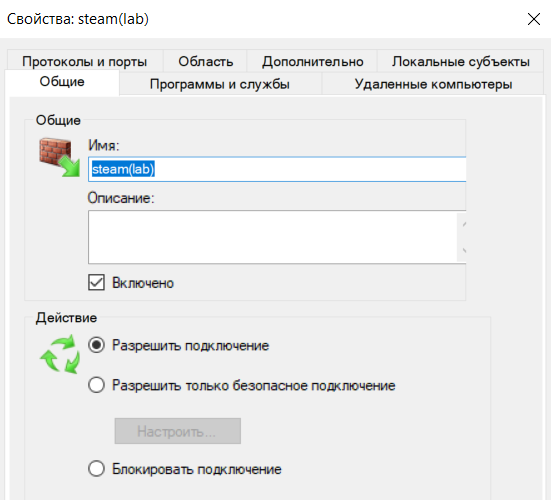


Рисунок 11 – Окно свойств исходящего подключения

Мы можем удалить наши правила, а можем воспользоваться восстановлением по умолчанию, однако эта функция удалит все правила, настроенные в ручную! Поэтому лучше воспользоваться обычным удалением :)

**Шпаргалка администратора ( Меню->Выполнить)**

Администрирование-control admintools  
Администратор источников данных-odbccp32.cpl  
Восстановление системных файлов-sfc /scannow  
Дефрагментация дисков-dfrg.msc  
Диспетчер проверки драйверов-verifier  
Дисптчер служебных программ-utilman  
Групповая политика-gpedit.msc  
Dr. Watson-drwtsn32  
Запросы операторов съемных ОЗУ-ntmsoprq.msc  
Защита БД учетных записей-syskey  
IExpress-iexpress  
Инфраструктура управления-wmimgmt.msc  
Проверка дисков-chkdsk  
Калькулятор-calc  
Командная строка-cmd  
Консоль управления-dcomcnfg  
Локальные параметры безопасности-secpol.msc  
Локальные пользователи и группы-lusrmgr.msc  
Мастер передачи файлов Bluetooth-fsquirt  
Настройка системы-msconfig  
Назначенные задания-control schedtasks  
Общие папки-fsmgmt.msc  
Общие ресурсы DDE-ddeshare  
Папка обмена-clipbrd  
Проверка подписи файла-sigverif  
Программа сетевого клиента SQL-cliconfg  
Производительность-perfmon.msc  
Просмотр событий-eventvwr.msc  
Подключение к рабочему столу-mstsc  
Результатирующая политика-rsop.msc  
Редактор системных файлов-sysedit  
Реестр-regedit  
Редактор личных символов-eudcedit  
Сертификаты-certmgr.msc  
Служба диагностики DirectX-dxdiag  
Службы-services.msc  
Службы компонентов-dcomcnfg  
Служба индексирования-ciadv.msc  
Съемные ЗУ-ntmsmgr.msc  
Телнет-telnet  
Управление дисками-diskmgmt.msc  
Управление рабочим столом-mstscoo  
Управление компьютером-compmgmt.msc  
Удаление вредоносных программ-mrt.exe

Опробуем действия нескольких команд. Для этого выполняем Меню -> Выполнить или Win + R. Перед нами появляется окно Выполнить. Выглядит оно следующим образом:

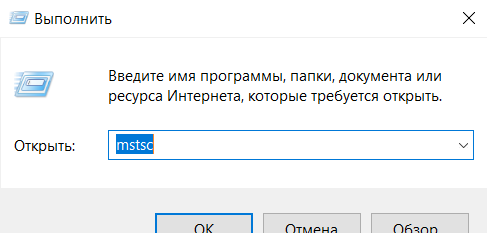


Рисунок 12 – Окно Выполнить

Здесь мы можем использовать наши команды для администрирования. Например, мы можем открыть Калькулятор (calc):

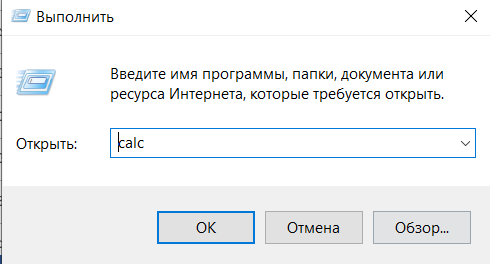
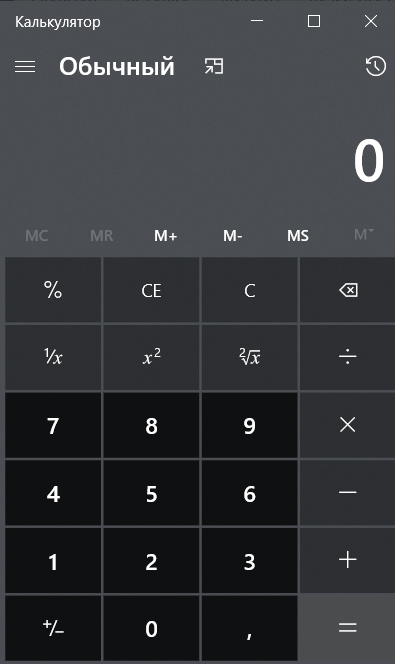
 

Рисунок 13 – Окно Выполнить с командой «calc» и результат (калькулятор)

При выполнении команды открывается обычный калькулятор. Мы можем так же открыть командную строку с помощью команды cmd:

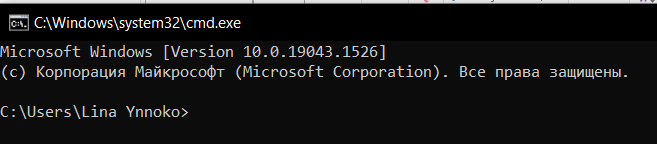


Рисунок 13 – Командная строка

Командная строка нужна для того, чтобы выполнять команды пользователя. Из курса Компьютерных сетей мы научились использовать несколько команд в командной строке. Например, ipconfig. Данная утилита служит для управления сетевыми интерфейсами.

Следующая команда позволяет зайти в Редактор реестра (regedit).

**Реестр** содержит информацию и настройки для аппаратного обеспечения, программного обеспечения, профилей пользователей, предустановки.

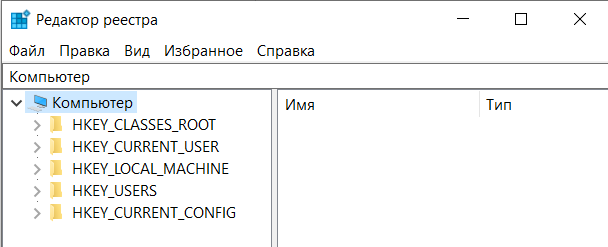


Рисунок 14 – редактор реестра

**Вывод:** Я овладела навыками настройки и использования Брандмауэра Windows, а также научилась использовать команды администрирования.

**Практическое занятие №5**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами симметричного шифрования.

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

**Задание к выполнению**

1. Изучить теоретические сведения по данной теме.
2. 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.

**Шифр Цезаря**

ФИО: Ездакова Полина Вадимовна.

Номер варианта 8, значит ключ для шифрования будет равен 8.

Е З Д А К О В А П О Л И Н А В А Д И М О В Н А

6 9 5 1 12 16 3 1 17 16 13 10 15 1 3 1 5 10 14 16 3 15 1

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33

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

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

**Ответ**: Эзьчигъч Дгтавч Ъчьабгъич. Ключ 8, кодовое слово «ЗАЩИТА».

**Шифр Трисемуса:**

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

**Ответ:** МВЛГРХЙГ ЦХСУФГ ЙГЛЕУХЙФГ.

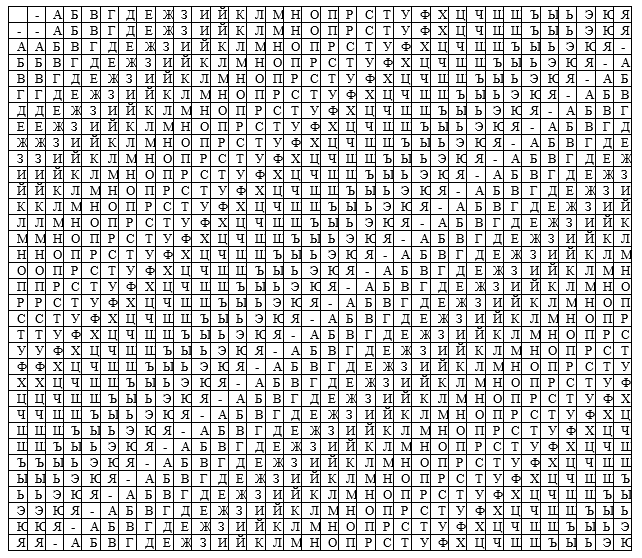
**Шифр Плейфейра.**

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

ЕЗ-ДА-КО-ВА ПО-ЛИ-НА ВА-ДИ-МО-ВН-АЪ

ДА-ЕЗ-ДУ-ГЩ РП-ЙБ-ЕГ ГЩ-ЙЗ-ДХ-ГМ-ЩШ

**Шифр Виженера:**



**Ответ:** мзэиэойа ичюиха ыицифоыцт.

1. Расшифровать следующие сообщения:

|  |  |  |
| --- | --- | --- |
| 8. | **дороюё дъ нозбъвё жодщйц** | Расшифровать с помощью шифра Цезаря.  Ключ 5.  Ключевое слово ОСЕНЬ |

Ключ 5. Ключевое слово ОСЕНЬ.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33

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

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

**Ответ:** Нечего на зеркало пенять.

**Вывод:** Я овладела основными криптографическими алгоритмами симметричного шифрования.

**Практическое занятие №6**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами асимметричного шифрования.

**Задание №1**

Рассказать процесс работы алгоритма RSA.

**RSA** (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Алгоритм RSA: Генерация ключей → Шифрование → Расшифрование.

|  |  |  |
| --- | --- | --- |
| Этап | Описание операции | Результат операции |
| Генерация ключей | Выбрать два простых различных числа | p=3557,  q=2579 |
| Вычислить модуль (произведение) | n = p \cdot q = 3557 \cdot 2579 = 9173503 |
| Вычислить функцию Эйлера | \varphi(n) = (p-1) (q-1) = 9167368 |
| Выбрать открытую экспоненту | e = 3 |
| Вычислить секретную экспоненту | d = e^{-1} \mod \varphi(n)  d = 6111579 |
| Опубликовать открытый ключ | \{e, n\} = \{3,9173503 \} |
| Сохранить закрытый ключ | \{d, n\} = \{6111579, 9173503 \} |
| Шифрование | Выбрать текст для зашифровки | m = 111111 |
| Вычислить шифротекст | \begin{align} c &= E(m) \\  &= m^e \mod n \\  &= 111111^3   \mod 9173503 \\  &= 4051753 \end{align} |
| Расшифрование | Вычислить исходное сообщение | \begin{align} m &= D(c) = \\   &= c^d \mod n \\   &= 4051753^{6111579} \mod 9173503 \\   &= 111111 \end{align} |

**Задание №2**

Рассказать процесс работы алгоритма Диффи-Хеллмана.

Алгоритм Диффи-Хеллмана: Генерация ключей → Шифрование → Расшифрование.

Протокол Диффи-Хеллмана – криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.

1. Принцип работы: у каждой стороны есть открытый ключ (который может видеть каждая сторона) и закрытый ключ (который видит только пользователь). К закрытому ключу нет доступа никому, кроме пользователя, кому пренадлежит ключ. Два участника обмена договариваются о двух числах. Один выбирает большое простое число, а другой – целое число, меньшее числа первого участника. Переговоры они могут вести открыто, и это никак не отразится на безопасности.
2. Каждый из двух участников, независимо друг от друга, генерирует другое число, которое они будут хранить в тайне. Эти числа выполняют роль секретного ключа. Далее в вычислениях используются секретный ключ и два предыдущих целых числа. Результат вычислений посылается участнику обмена, и он играет роль открытого ключа.
3. Участники обмена обмениваются открытыми ключами. Далее они, используя собственный секретный ключ и открытый ключ партнера, конфиденциально вычисляют ключ сессии. Каждый партер вычисляет один и тот же ключ сессии.
4. Ключ сессии может использоваться как секретный ключ для другого алгоритма шифрования, например DES. Никакое третье лицо, контролирующее обмен, не сможет вычислить ключ сессии, не зная один из секретных ключей.

**Задание №3**

Рассказать процесс работы алгоритма Эль-Гамаля.

Алгоритм Эль-Гамаля: Генерация ключей → Шифрование → Расшифрование.

**Генерация ключей**

1. Генерируется случайное простое число ~p длины ~n [битов](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82).
2. Выбирается случайный примитивный элемент ~g.
3. Выбирается случайное целое число ~x такое, что ~1 < x < p-1.
4. Вычисляется ~y = g^x\,\bmod\,p.
5. Открытым ключом является тройка \left( p,g,y \right), закрытым ключом — число ~x.

**Шифрование**

Сообщение ~M шифруется следующим образом:

1. Выбирается сессионный [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) — случайное целое число ~k такое, что ~1 < k < p - 1
2. Вычисляются числа a = g^k\,\bmod\,p и b = y^k M\,\bmod\,p.
3. Пара чисел \left( a, b \right) является [шифротекстом](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82" \o "Шифротекст).

Нетрудно видеть, что длина шифротекста в схеме Эль-Гамаля длиннее исходного сообщения M вдвое.

**Расшифрование**

Зная закрытый ключ ~x, исходное сообщение можно вычислить из шифротекста \left( a, b \right) по формуле:

M = b(a^x)^{-1}\,\bmod\,p.

При этом нетрудно проверить, что

~(a^x)^{-1}\equiv g^{-kx}\pmod{p}

и поэтому

~b(a^x)^{-1}\equiv (y^kM)g^{-xk}\equiv (g^{xk}M) g^{-xk}\equiv M \pmod{p}.

Для практических вычислений больше подходит следующая формула:

M = b(a^x)^{-1}\,\bmod\,p = b \cdot a^{(p-1-x)}\,\bmod\,p 

**Задание №4\***

Используя существующие криптографические библиотеки, создать приложение и проанализировать работу вышеперечисленных алгоритмов.

**Вывод:** Я овладела основными криптографическими алгоритмами асимметричного шифрования.

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

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

**Задание**

В практической работе необходимо объяснить последовательность выполнения процедур генерации и проверки ЭЦП.

Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.

Опишите схему протокола ЭЦП на основе алгоритма RSA.

\*На базе алгоритма RSA получить ЭЦП (в проекте можно использовать существующие криптографические алгоритмы). Удостовериться, что ЭЦП принадлежит именно этому сообщению.

Оформите отчет. Запишите результаты выполнения задания и код полученной программы в отчет. Ответить на контрольные вопросы.

using System;

using System.Security.Cryptography;

using System.Text;

namespace ConsoleApp1

{

class Program

{

static void Main()

{

string source;

Console.WriteLine(" Введите ваше сообщение: ");

source = Console.ReadLine().ToString();

SHA256 sha256Hash = SHA256.Create();

byte[] hashValue = sha256Hash.ComputeHash(Encoding.UTF8.GetBytes(source));

//Значение для хранения значения со знаком.

byte[] signedHashValue;

// Генерируем пару открытый/закрытый ключ.

RSA rsa = RSA.Create();

//Создаем объект RSAPKCS1SignatureFormatter и передаем ему

// Экземпляр RSA для передачи закрытого ключа.

RSAPKCS1SignatureFormatter rsaFormatter = new RSAPKCS1SignatureFormatter(rsa);

// Установите алгоритм хеширования SHA256.

rsaFormatter.SetHashAlgorithm("SHA256");

//Создаем подпись для hashValue и назначаем ее signedHashValue.

signedHashValue = rsaFormatter.CreateSignature(hashValue);

foreach (byte item in hashValue)

{

Console.Write(item + " ");

}

Console.WriteLine();

foreach (byte item in signedHashValue)

{

Console.Write(item + " ");

}

// byte[] mass\_byte = { 1, 2, 3, 4, 5 };

RSAPKCS1SignatureDeformatter rsaDeformatter = new RSAPKCS1SignatureDeformatter(rsa);

rsaDeformatter.SetHashAlgorithm("SHA256");

// Проверка ЭЦП

if (rsaDeformatter.VerifySignature(hashValue, signedHashValue )) //mass\_byte для проверки

{

Console.WriteLine("Цифровая подпись действительна");

}

else

{

Console.WriteLine("Цифровая подпись не действительна");

}

Console.ReadKey();

}

}

}

**Контрольные вопросы:**

1. Дайте определение понятию "электронная цифровая подпись".

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

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

* отправитель знает содержание сообщения, которое он подписывает;
* получатель, зная открытый ключ проверки подписи, может проверить правильность подписи полученного сообщения в любое время без какого-либо разрешения и участия отправителя;
* безопасность схемы подписи гарантируется.

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.

3. Перечислите специальные схемы ЭЦП.

* схема "конфиденциальной" (неотвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;
* схема подписи "вслепую" ("затемненной" подписи) - отправитель не знает подписанного им сообщения;
* схема "мультиподписи" - вместо одного отправителя сообщение подписывает группа из нескольких участников;
* схема "групповой" подписи - получатель может проверить, что подписанное сообщение пришло от члена некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано. В тоже время, в случае необходимости, отправитель может быть определен;

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

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

**Вариант 8**

1. Найти канонические разложения *а* = 83748733, *b* = 73435591.

*а* = 83748733 = 109\*97\*89\*89

*b* = 73435591 = 127\*89\*89\*73

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

а) 83 748 733 = 73 435 591\*1 + 10 313 142;

73 435 591 = 10 313 142\*7 + 1 243 597;

10 313 142 = 1 243 597\*8 + 364 366;

1 243 597 = 364 366\*3 + 150 499;

364 336 = 150 499\*2 + 63 368;

150 499 = 63 368\*2 + 23 763;

63 368 = 23 763\*2 + 15 842;

23 763 = 15 842\*1 + 7 921;

15 842 = 7 921\*2;

НОД = 7921;

б) *а* = 83748733 = 109\*97\*89\*89;

*b* = 73435591 = 127\*89\*89\*73;

НОД = 89\*89 = 7921;

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

Из п.2 НОД(a,b) = 7921.

83 748 733 = 73 435 591\*1 + 10 313 142 =>10 313 142 = 83 748 733 + 73 435 591\*(-1);

73 435 591 = 10 313 142\*7 + 1 243 597 => 1 243 597 = 73 435 591 + 10 313 142\*(-7);

10 313 142 = 1 243 597\*8 + 364 366 => 364 366 = 10 313 142 + 1 243 597\*(-8);

1 243 597 = 364 366\*3 + 150 499 => 150 499 = 1 243 597 + 364 366\*(-3);

364 336 = 150 499\*2 + 63 368 => 63 368 = 364 336 + 150 499\*(-2);

150 499 = 63 368\*2 + 23 763 => 23 763 = 150 499 + 63 368\*(-2);

63 368 = 23 763\*2 + 15 842 => 15 842 = 63 368 + 23 763\*(-2);

23 763 = 15 842\*1 + 7 921 => 7 921 = 23 763 + 15 842\*(-1);

7 921 = 23 763 + 15 842\*(-1) = 23 763 + (63 368 + 23 763\*(-2))\*(-1) =

= 23 763\*4 + 63 368\*(-1) = (150 499 + 63 368\*(-2))\*4 + 63 368\*(-1) =

= 63 368\*(-9) + 150 499\*4 = (364 336 + 150 499\*(-2))\*(-9) + 150 499\*4 =

= 150 499\*22 + 364 336\*(-9) = (1 243 597 + 364 366\*(-3))\*22 + 364 336\*(-9) =

= 364 336\*(-75) + 1 243 597\*22 = (10 313 142 + 1 243 597\*(-8))(-75) + 1 243 597\*22 =

= 1 243 597\*622 + 10 313 142\*(-75) = (73 435 591 + 10 313 142\*(-7))\*622 +

+ 10 313 142\*(-75) = 10 313 142\*(-4 429) + 73 435 591\*622 =

= (83 748 733 + 73 435 591\*(-1)) \*(-4 429) + 73 435 591\*622 =

= 83 748 733\*(-4 429) + 73 435 591\*5051 = 7 921

a u b v НОД(a,b)

4. Найти остаток от деления  на 11

1996 mod 11 = 5;

52003 mod 11 = ?;

5 mod 11 = 5; 1

25 mod 11 = 3; 2

125 mod 11 = 4; 3

625 mod 11 = 9; 4

3 125 mod 11 = 1; 5

15 625 mod 11 = 5; 6

2003 = 400\*5 + 3;

52003 mod 11 = 53 mod 11 = 4;

19962003 mod 11 = 4.

**Практическое занятие №9**

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

Цель: Изучить основные положения авторского права и смежных прав.

**Задание для выполнения.**

Ответить на следующие вопросы:

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?**

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?**

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

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

Наиболее распространенным видом авторского договора является издательский договор. В рамках данного договора осуществляется издание и переиздание любых произведений, которые могут быть зафиксированы на бумаге, т.е. произведений литературы (научных, художественных, учебных и т.п.), драматических, сценарных, музыкальных произведений, произведений изобразительного искусства и т.д. Издательский договор наиболее полно урегулирован действующим законодательством и исследован юридической наукой. Нередко выводы, которые первоначально делаются на базе применения норм об издательском договоре, а также сложившейся практики разрешения споров, впоследствии распространяются и на другие авторские договоры.

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.

**Задание для выполнения.**

Ответить на следующие вопросы:

1. **Основные составляющие описания 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 (и указанными выше документами) 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.

**Задание для выполнения.**

**Задание 1**

Изучить виды, содержание и порядок проведения патентных исследований.

**Задание 2**

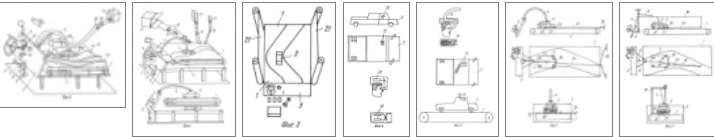
В результате проведения исследовательских и проектно-конструкторских работ на промышленных предприятиях были разработаны методы испытания материалов. Для реализации этих методов предложены конструктивные решения приборов и приспособлений. В результате модернизации и совершенствования технологических 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. Соответствие вариантов рисункам представлено ниже.

|  |
| --- |
|  |
| Рисунок 8 – Разработано игровое устройство для симуляции вождения |

**Выполнение:**

Изобретение относится к устройствам для получения навыков и понятий управления транспортным средством, обучения правилам дорожного движения, тренировки преодоления различных помех, развлечения. Имитатор дороги выполнен в виде бесконечной ленты. Имеются модель автомобиля и органы дистанционного управления. Отличительные признаки предложенного технического решения заключаются в том, что игровой тренажер оснащен внешней прижимной пружиной, связанной с объемной моделью автомобиля, устройством для создания помех и объемными элементами, закрепленными на бесконечной ленте. Имитатор дороги может поворачиваться вокруг собственной оси. Изобретение обеспечивает увеличение динамичности при обучении правил движения в дорожной среде, наглядности движения транспортных средств в трехмерном пространстве с программой задач на правила движения, программой помех и происшествий в изменяющейся дорожной обстановке.

**** 1. Игровой тренажер, содержащий установленный с возможностью поворота вокруг собственной оси имитатор дороги, размещенную на нем управляемую объемную модель автомобиля и связанный с приводами упомянутых имитатора и модели пульт управления, отличающийся тем, что в него введены внешняя пружинная опора, соединенная с моделью автомобиля с возможностью прижатия ее к имитатору дороги с обеспечением движения по всей его площади, поднятия над ним при критических положениях и передачи к модели автомобиля по внутренним проводам электрических сигналов от пульта управления, узел создания случайных движущихся помех и объемные препятствия, закрепленные на имитаторе дороги, при этом последний выполнен в виде бесконечной движущейся ленты.

2. Тренажер по п.1, отличающийся тем, что имитатор дороги выполнен в виде движущейся ленты, расположенной горизонтально с поворотом на 180o на торцах.

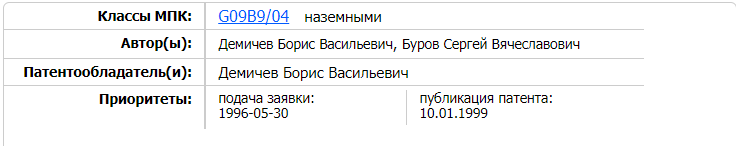
3. Тренажер по п.1 или 2, отличающийся тем, что имитатор дороги имеет дополнительные боковые движущиеся ленты с изображением боковой дорожной обстановки и помех.

4. Тренажер по п.1, отличающийся тем, что он снабжен двумя видеокамерами, установленными с возможностью передачи информации о дорожной обстановке на расположенные на шлеме оператора видеомониторы и с помощью зеркал - на окуляры.

5. Тренажер по п.1, отличающийся тем, что он снабжен двумя световодами, установленными с возможностью передачи оператору информации о дорожной обстановке.

6. Тренажер по п.1, отличающийся тем, что он снабжен внешней опорой вогнутой формы, с которой через свободно движущееся кольцо соединена эластичная тяга.

7. Тренажер по п.6, отличающийся тем, что внешняя опора размещена над моделью автомобиля, а эластичная тяга соединена с передней частью модели.



**Практическое занятие №12**

**Тема «Патентный поиск»**

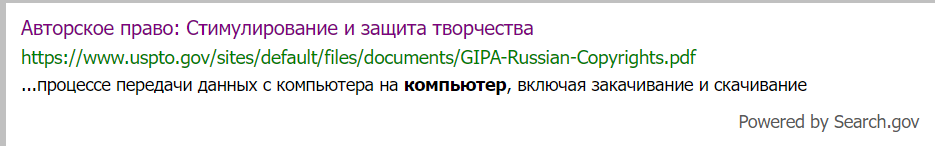
Цель: освоить навыки проведения патентного поиска по заданной тематике.

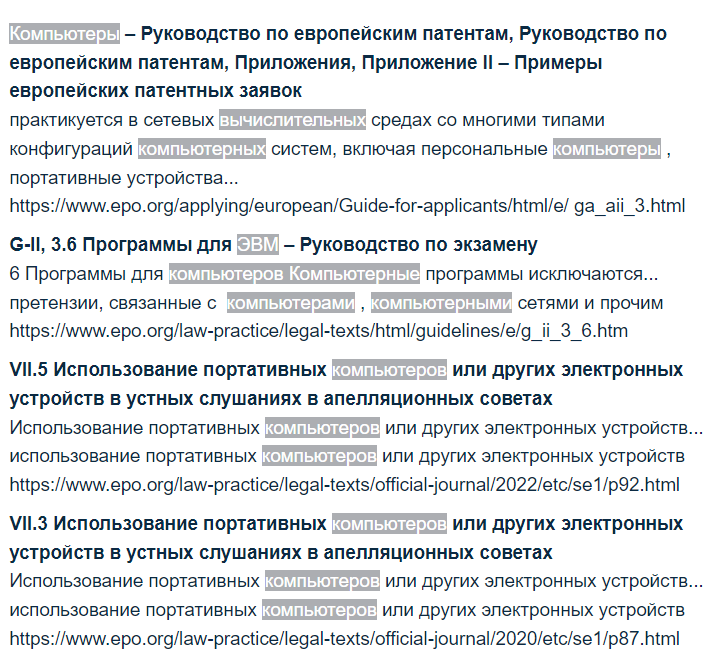
**Задание для выполнения**

Провести патентный поиск по теме своего курсового проекта. Тема «IT лаборатория»

**Выполнение**

Поиск осуществлялся в категории «Компьютер».

При проведении патентного поиска были получены следующие результаты: 



**Вывод:**

Патентный поиск выдал результаты, совершенно не схожие с темой моего курсового проекта. Если разделить курсовой проект на такие составляющие, как «Процессор», «Видеокарта» и «Жесткий диск», результат останется тем же.

**Практическое занятие №13**

**Тема «Настройка антивирусов»**

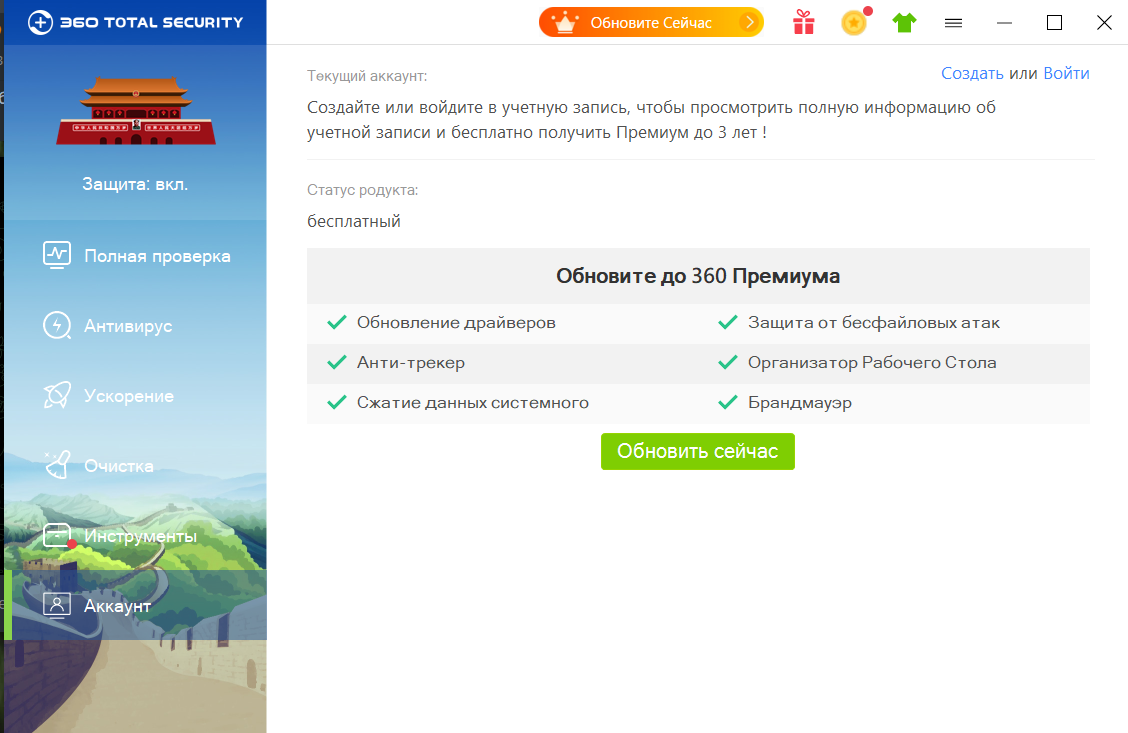
**Задание к выполнению**

1. Установить и настроить антивирусную программу по варианту.
2. Обновить базу данных сигнатур вирусов.
3. Выполнить сканирование дисков.

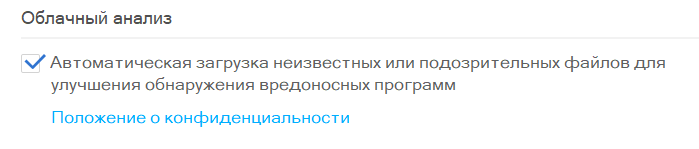
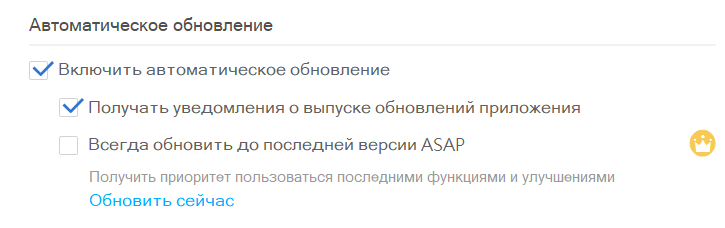
Варианты заданий находятся в презентации 6.2 (на последнем слайде).

В электронный конспект поместить копии экрана с пояснениями всех проведенных действий.

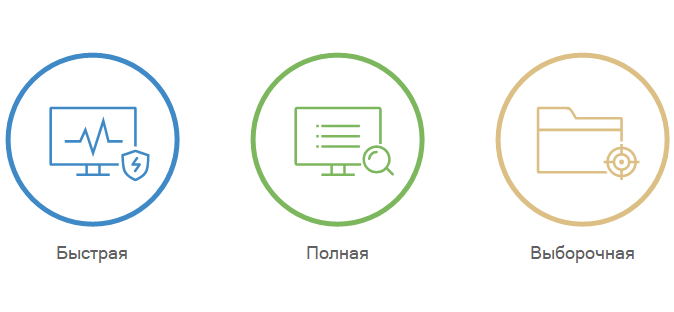
1.



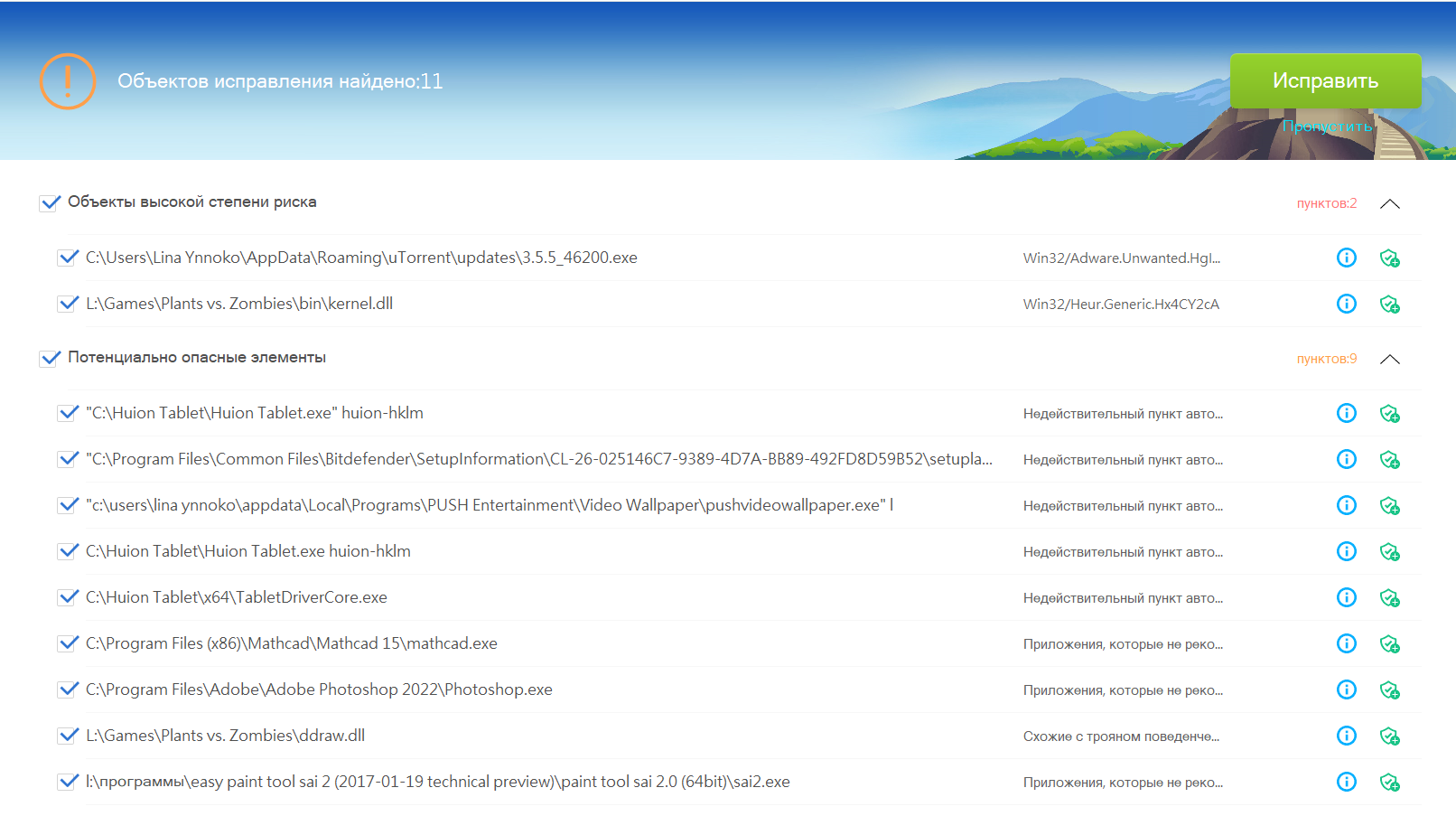
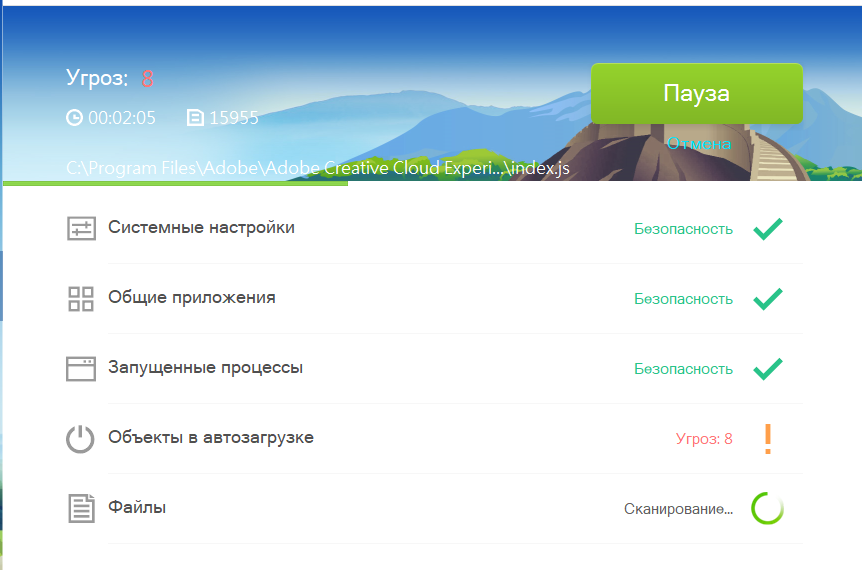
Устанавливаем нужную нам антивирусную программу. Для обновления базы данных сигнатур вирусов, нужно поставить галочки на следующие пункты, чтобы обновление происходило автоматически.



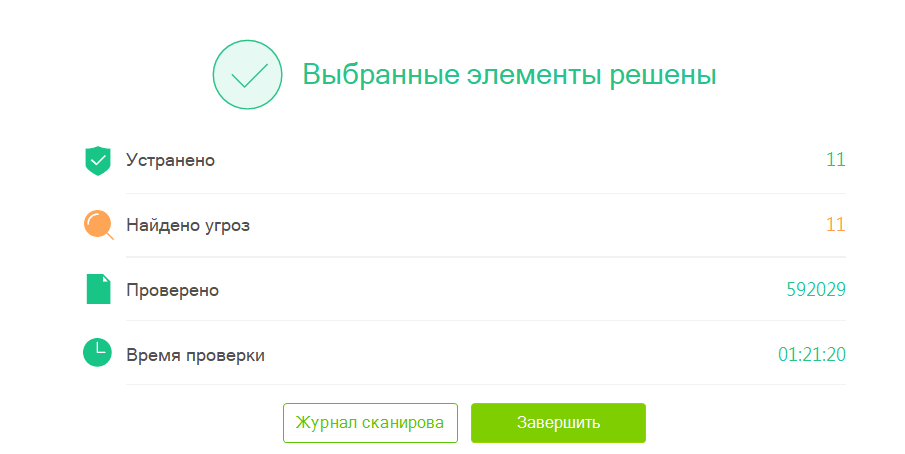
Далее, выбираем сканирование (я выбрала полное).



Ждем, пока сканирование полностью не закончится. Когда сканирование завершено, мы смотрим на наши файлы и анализируем, что с ними сделать.



После устранения всех угроз, завершаем сканирование и радуемся тому, какие мы молодцы :^)



**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)**»**

**Ход выполнения работы:**

1. Ознакомиться с созданием криптографического приложения.
2. Ответить на теоретические вопросы.
3. Ответы оформить в отчет.

**Контрольные вопросы:**

1) Какие симметричные алгоритмы шифрования Вы знаете?

Цезаря, Трисемуса, Плейфейра, Виженера.

2) Какие ассиметричные алгоритмы шифрования Вы знаете?

Эль-Гамаля, RSA, Деффи-Хеллмана.

3) Основное назначение библиотеки System.Security.Cryptography?

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

4) Влияет ли размер ключа на криптостойкость алгоритма?

Если длина симметричного ключа составляет 40 бит (такое шифрование называют слабым), то для его реконструкции надо перебрать числа. Используя несколько современных передовых компьютеров, задачу можно решить быстрее, чем за сутки. Это недешевый, но вполне возможен мероприятие. Если длина ключа составляет 64 бита, то необходимо иметь сеть из нескольких десятков специализированных компьютеров, и задача решается в течение нескольких недель. Это крайне дорогостоящее мероприятие, но технически он возможен при современном уровне развития техники. Сильным называют шифрования с длиной симметричного ключа 128 бит.

5) 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" \o "Хеш), 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.