Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет по дисциплине

«Основы Защиты Информации»

Студент: Аникеенко Е. В.

ФИТ 2 курс 2 группа

Преподаватель: Берников В.О.

Минск 2021

Практическое занятие №1

Тема «Концепция национальной безопасности Республики Беларусь»

Цель: изучить концепцию национальной безопасности Республики Беларусь.

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

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

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

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

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

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

Основными национальными интересами в информационной сфере являются:

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

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

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

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

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

* распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;
* зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;
* несоответствие качества национального контента мировому уровню;
* недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;
* рост преступности с использованием информационно-коммуникационных технологий;
* недостаточная эффективность информационного обеспечения государственной политики;
* несовершенство системы обеспечения безопасности критически важных объектов информатизации.

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

* открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;
* доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;
* информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;
* нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;
* развитие технологий манипулирования информацией;
* препятствование распространению национального контента Республики Беларусь за рубежом;
* широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;
* попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

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

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

Нейтрализации ряда **внутренних источников угроз национальной безопасности** способствует информационное обеспечение государственной политики, которое заключается в доведении до граждан Республики Беларусь и внешней аудитории объективной информации о государственном курсе во всех сферах жизнедеятельности общества, официальной позиции по общественно значимым событиям внутри страны и за рубежом, о деятельности государственных органов. Важной задачей при этом является расширение каналов и повышение качества информирования зарубежной общественности. Составной частью информационного обеспечения государственной политики выступает информационное противоборство, представляющее собой комплексное использование информационных, технических и иных методов, способов и средств для воздействия на информационную сферу с целью достижения политических, экономических и иных задач либо защиты собственного информационного пространства.

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

**Вывод:** я изучил концепцию национальной безопасности Республики Беларусь. Я считаю, что информационная безопасность является важным аспектом государственной безопасности в целом. Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

**Практическое занятие №2**

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

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

**Теоретическое введение**

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

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

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

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

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

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

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

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

Относительная эффективность:

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

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

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

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

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

где К≥1.

Выражения (2) – (1) примут вид:

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

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

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

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

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

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

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

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

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

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

или

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

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

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

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

то:

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

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

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

или:

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

где Cдоп — допустимые расходы на защиту.

**Задание на выполнение**

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

Таблица 2.1 - Исходные данные к решению задачи

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E0, бел. р*. | *E, бел. р.* | *K* | *C, бел. р.* |
| 2 | 100000 | 90000 | 50 | 5000 |

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

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

С - Стоимость средств защиты.

Эффективность функционирования объекта с учетом воздействия несанкционированного доступа:

*(руб).*

Относительная эффективность:

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

*(руб).*

Выражения (2.1) – (2.6) примут вид:

*(руб).*

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

**Вывод:**

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

**Практическое занятие №3**

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

Цель: разработать проект политики информационной безопасности торговой сети.

**Введение**

Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Прежде всего политика необходима для того, чтобы донести до бизнеса цели и задачи информационной безопасности компании. Бизнес должен понимать, что агент безопасности – это не только инструмент для расследования фактов утечек данных, но и помощник в минимизации рисков компании, а следовательно – в повышении прибыльности компании.

Любая защитная мера есть компромисс между снижением рисков и удобством работы пользователя. Когда специалист по безопасности говорит, что процесс не должен происходить каким-либо образом по причине появления некоторых рисков, ему всегда задают резонный вопрос: «А как он должен происходить?» Специалисту по безопасности необходимо предложить модель процесса, в которой эти риски снижены в какой-то мере, удовлетворительной для бизнеса.

При этом любое применение любых защитных мер, касающихся взаимодействия пользователя с информационной системой компании всегда вызывает отрицательную реакцию пользователя.

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

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

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

Определение политики ИБ должно сводиться к следующим практическим шагам:

1. Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:

* управление доступом к средствам вычислительной техники, программа и данным;
* антивирусную защиту;
* вопросы резервного копирования;
* проведение ремонтных и восстановительных работ;
* информирование об инцидентах об области ИБ.

2. Определение подходов к управлению рисками: является ли достаточным базовый уровень защищенности или требуется проводить полный вариант анализа рисков.

3. Структуризация контрмер по уровням.

4. Порядок сертификации на соответствие стандартам в области ИБ. Должна быть определена периодичность проведения совещаний по тематике ИБ на уровне руководства, включая периодический пересмотр положений политики ИБ, а также порядок обучения всех категорий пользователей информационной системы по вопросам ИБ.

Для построения системы защиты информации необходимо определить границы системы, для которой должен быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности (система защиты информации) должна строиться именно в этих границах.

**Описание структуры компании**

Эффективность управления деятельностью зависит оттого, насколько грамотно сформирована организационная структура управления и насколько она соответствует цели деятельности организации.

В настоящее время под организационной структурой понимается упорядоченная совокупность устойчиво взаимосвязанных элементов, обеспечивающих функционирование и развитие организации как единого целого. Структура управления определяется также как форма разделения и кооперации управленческой деятельности. Можно сказать, что структура управления есть не что иное, как оптимальное распределение работы, прав и ответственности, порядка и форм взаимодействия между членами коллектива организации.

Составляющими организационных структур являются:

* элементы организационных структур управления – службы или органы аппарата управления, а также отдельные работники этих служб (органов);
* организационные отношения – отношения (связи) между подразделениями организации, уровнями ее управления, персоналом, посредством которых реализуются функции управления;
* уровни управления – совокупность прав, обязанностей и ответственности, характерная для должностных лиц, занимающих определенную ступень в иерархической структуре организации.

На данном рисунке (3.1) представлена организационная структура завода по производству шин:

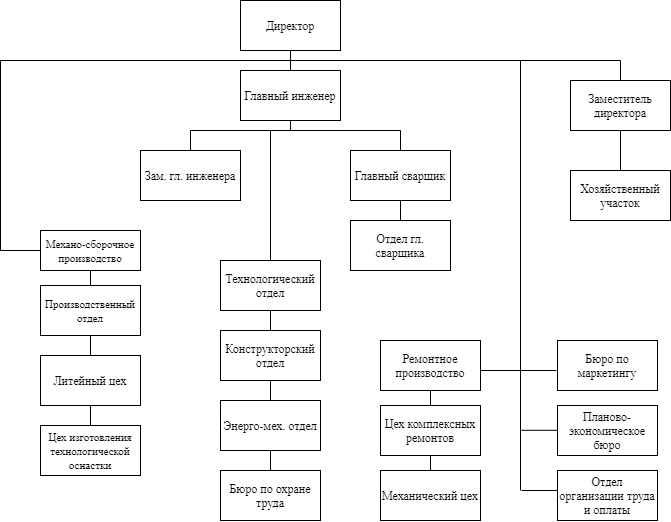


Рис.3.1 – Организационная структура завода по производству шин

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

**Оценка рисков**

Идентифицировать и оценить активы, разработать модель нарушителя и модель угроз, идентифицировать уязвимости – все это стандартные шаги, описание которых должно присутствовать в любой методике анализа рисков. Все перечисленные шаги могут выполняться с различным уровнем качества и детализации. Очень важно понять, что и как можно сделать с огромным количеством накопленной информации и формализованными моделями. На наш взгляд, этот вопрос наиболее важен, и ответ должна давать используемая методика анализа рисков.

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения:

* антропогенные,
* техногенные
* естественные (природные)

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала, так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок, и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.    
 Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре завода по производству шин могут быть как внешними, так и внутренними.

Источниками внутренних угроз являются:

* сотрудники организации;
* программное обеспечение;
* аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

* ошибки пользователей и системных администраторов;
* нарушения сотрудниками завода по производству шин установленных регламентов сбора, обработки, передачи и уничтожения информации;
* ошибки в работе программного обеспечения;
* отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

* компьютерные вирусы и вредоносные программы;
* организации и отдельные лица;
* стихийные бедствия.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации:

* информационные;
* программные;
* физические;

К информационным угрозам относятся:

* несанкционированный доступ к информационным ресурсам;
* незаконное копирование данных в информационных системах;
* хищение информации из архива, отделов и баз данных;
* нарушение технологии обработки информации;
* противозаконный сбор и использование информации;
* использование информационного оружия.

К программным угрозам относятся:

* использование ошибок и «дыр» в ПО;
* компьютерные вирусы и вредоносные программы;

К физическим угрозам относятся:

* уничтожение или разрушение средств обработки информации и связи;
* хищение носителей информации;
* хищение программных или аппаратных ключей и средств криптографической защиты данных;
* воздействие на персонал (шантаж, нападение).

Специфические угрозы безопасности

* Возможность отключения электричества, что приведет к сбою незавершенных операций и потере данных.
* Угроза возникновения неправильной адресации пакетов.
* Угроза проникновения на рабочие места сотрудников людей, не являющихся работниками отделов, которые имеют туда доступ, и попадания на завод по производству шин предметов, способных нанести ущерб.
* Угроза доступа в эксплуатационный отдел, могут быть нарушены эксплуатационные планы.
* Угроза изменения базы данных людей, получающих пенсию, в следствии чего не только заводу по производству шин, но и обществу будет нанесен урон.
* Угроза доступа в ИТ-отделе.

Полученные результаты необходимо оценить, агрегировать, классифицировать и отобразить. Так как ущерб определяется на этапе идентификации и оценки активов, необходимо оценить вероятность событий риска. Как и в случае с оценкой активов, оценку вероятности можно получить на основании статистики по инцидентам, причины которых совпадают с рассматриваемыми угрозами ИБ, либо методом прогнозирования – на основании взвешивания факторов, соответствующих разработанной модели угроз.

Хорошей практикой для оценки вероятности станет классификация уязвимостей по выделенному набору факторов, характеризующих простоту эксплуатации уязвимостей. Прогнозирование вероятности угроз производится уже на основании свойств уязвимости и групп нарушителей, от которых исходят угрозы.

В качестве примера системы классификации уязвимостей можно привести стандарт CVSS – common vulnerability scorning system. Следует отметить, что в процессе идентификации и оценки уязвимостей очень важен экспертный опыт специалистов по ИБ, выполняющих оценку рисков, и используемые статистические материалы и отчеты по уязвимостям и угрозам в области информационной безопасности

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре завода по производству шин могут быть как внешними, так и внутренними.

Величину(уровень) риска следует определять для всех идентифицированных и соответствующих друг другу наборов «актив – угроза». При этом величина ущерба и вероятности не обязательно должны быть выражены в абсолютных денежных показателях и процентах; более того, как правило, представить результаты в такой форме не удается. Причина этого – используемые методы анализа и оценки рисков информационной безопасности: сценарный анализ и прогнозирование.

Сущность любого подхода к управлению рисками заключается в анализе факторов риска и принятии адекватных решений по обработке рисков. Факторы риска – это те основные параметры, которыми мы оперируем при оценке рисков. Таких параметров всего семь:

* Актив.
* Ущерб.
* Угроза.
* Уязвимость.
* Механизм контроля.
* Размер среднегодовых потерь.
* Возврат инвестиций.

Общий подход и схема рассуждений при оценке рисков примерно одинаковая, независимо от того, какая методология используется. Процесс оценки рисков включает в себя две фазы. На первой, которая определяется в стандартах как оценка рисков, необходимо ответить на следующие вопросы:

* Что является активом компании?
* Какова ценность актива?
* Какие существуют угрозы в отношении этого актива?
* Каковы последствия этих угроз и ущерб для бизнеса?
* Насколько уязвим бизнес в отношении этих угроз?
* Каков ожидаемый размер среднегодовых потерь?

На второй фазе, которая определяется стандартами как оценивание рисков, необходимо ответить на вопрос: Какой уровень риска является приемлимым для организации и, исходя из этого, какие риски превышают этот уровень.

Таким образом, по результатам оценки рисков, мы получаем описание рисков, превышающих допустимый уровень и оценку величины этих рисков, которая определяется размером среднегодовых потерь. Далее необходимо принять решение по обработке рисков, ответить на следующие вопросы:

* Какой вариант обработки рисков выбираем?
* Если принимается решение о минимизации риска, то какие механизмы контроля необходимы?
* Насколько эффективны эти механизмы контроля и какой возврат инвестиций они обеспечат?

На выходе данного процесса появляется план обработки рисков, определяющий способы обработки рисков, стоимость контрмер, а также сроки и ответственных за реализацию контрмер.

Подводя итоги вышесказанного, обобщим их для торговой сети. Как уже было сказано, благодаря специфике работы торговой сети, атаки являются довольно редкими, так как даже при условии успешности, прибыль довольно мала. Однако вероятность угрозы все равно присутствует и руководству магазинов торговой сети, как и руководству компании в целом, необходимо осознавать и представлять возможные угрозы, чтобы иметь возможность подготовиться к ним и предотвратить их полностью, либо минимизировать возможный ущерб.

В связи с этим, наиболее возможными видами атаки на торговую сеть являются следующие:

* ограбление магазина торговой сети. При данном типе атаки, злоумышленники могут довольствоваться лишь выручкой магазина и товаром, который в нем находится. Связи с финансовой системой у магазинов нет. Однако данный тип атаки является наиболее опасным для жизни как персонала, так и посетителей;
* получение несанкционированного доступа к веб-сайту торговой сети. Данный тип атаки наименее опасен, поскольку у сайта так же нету связи с финансовой системой сети. Однако злоумышленники могут испортить информацию на веб-сайте и благодаря этому извлечь какую-нибудь выгоду, либо осуществить «взлом» просто ради интереса;
* атака на головной офис компании. Данная угроза очень опасна прежде всего риском жертв среди сотрудников фирмы. При осуществлении данной атаки, преступники могут завладеть финансами и/или банковскими данными компании;
* взлом банковского счета компании. В настоящее время у любой компании имеется свой счет, на котором находятся деньги фирмы. Естественно, данная угроза наименее зависима от сети, так как атака осуществляется на банк. Тем не менее, компания должна предусмотреть данный случай и минимизировать его возможность;
* недобросовестная конкуренция. Данная угроза так же присутствует всегда у любой компании, независимо от ее размера, поэтому ей необходимо уделить внимание при разработке политики информационной безопасности;
* физическое воздействие на магазины компании (например, поджог).

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

**Разработка мер защиты**

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

Целями защиты информации являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

При разработке политики безопасности можно использовать следующую модель (рис. 1), основанную на адаптации Общих Критериев (ISO 15408) и проведении анализа риска (ISO 17799).

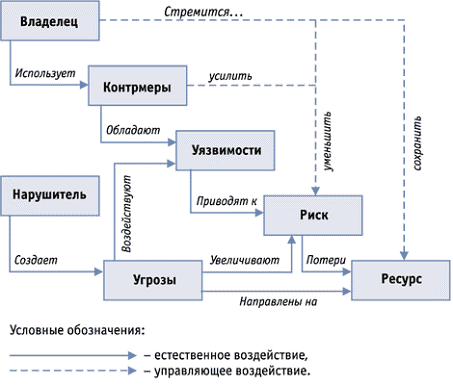


Рис.3.2.–Модель построения корпоративной системы защиты информации

Представленная модель – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Рассматриваются следующие объективные факторы:

* угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;
* уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;
* риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Для создания эффективной политики безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для предприятия на основе заданного критерия. Политику безопасности и соответствующую корпоративную систему защиты информации предстоит построить таким образом, чтобы достичь заданного уровня риска.

Предлагаемая методика разработки политики информационной безопасности современного предприятия позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности, избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить различные варианты контрмер.

В ходе работ должны быть установлены границы исследования. Для этого необходимо выделить ресурсы информационной системы, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные, а также информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (архивах, фондах, банках данных, других информационных системах). Примерами внешних элементов являются сети связи, внешние сервисы и т.п.

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

Эта модель, в соответствии с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы защиты.

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

По завершении работ, можно будет определить меру гарантии безопасности информационной среды, основанную на оценке, с которой можно доверять информационной среде объекта. Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности. Адекватность оценки основана на вовлечении в процесс оценки большего числа элементов информационной среды объекта, глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения, строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

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

* вооруженная охрана магазинов торговой сети и офисов компании;
* четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь каждого магазина с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, милиции;
* защита главных серверов компании (если такие существуют) и важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам. Уборщица не должна знать номер банковского счета фирмы и тем более, его пароля;
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие как в магазинах, так и в офисах, наглядного отображения плана по работе во время чрезвычайных ситуаций.

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

Отдельный раздел законопроекта "О коммерческой тайне", посвященный организации защиты коммерческой информации, определяет необходимый комплекс мероприятий по ее защите:

* установление особого режима конфиденциальности;
* ограничение доступа к конфиденциальной информации;
* использование организационных мер и технических средств защиты информации;
* осуществление контроля за соблюдением установленного режима конфиденциальности.

Установление особого режима конфиденциальности направлено на создание условий для обеспечения физической защиты носителей конфиденциальной информации. Как правило, особый режим конфиденциальности подразумевает:

* организацию охраны помещений, в которых содержатся носители конфиденциальной информации;
* установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;
* установление пропускного режима в помещения, содержащие носители конфиденциальной информации;
* закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;
* установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);
* организацию ремонта технических средств обработки конфиденциальной информации;
* организацию контроля за установленным порядком.

Эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации (СЗИ). Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

* средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;
* средства, обеспечивающие защиту информации при передаче ее по каналам связи;
* средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
* средства, обеспечивающие защиту от воздействия программ-вирусов;
* материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако это способ требует значительных капитальных затрат и практически не применяется.

Обеспечение требуемой защиты информационных ресурсов предприятий в этих условиях достигается применением дополнительных инструментальных средств. К их числу относятся:

* средства анализа защищенности операционных систем и сетевых сервисов;
* средства обнаружения опасных информационных воздействий (атак) в сетях.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок, и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.

Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

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

* вооруженная охрана магазинов торговой сети и офисов компании;
* четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь каждого магазина с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, милиции;
* защита главных серверов компании (если такие существуют) и важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам. Уборщица не должна знать номер банковского счета фирмы и тем более, его пароля;
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие как в магазинах, так и в офисах, наглядного отображения плана по работе во время чрезвычайных ситуаций.

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

**Выводы**

Важно помнить, что, прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности. При этом политику безопасности желательно оформить в виде отдельного документа и утвердить руководством предприятия.

Приведенные выше меры по защите информации в торговой сети являются лишь примерными. В реальности, следует провести комплексную оценку с привлечением специализированных людей, которые являются экспертами в вопросах обеспечения ИБ и проведением специальных тестов и экспериментов.

**Практическое занятие №4**

**Тема: «Настройка Брандмауэра Windows»**

**Цель**: Овладение навыками настройки и использования Брандмауэра Windows.

1. Включение брандмауэра

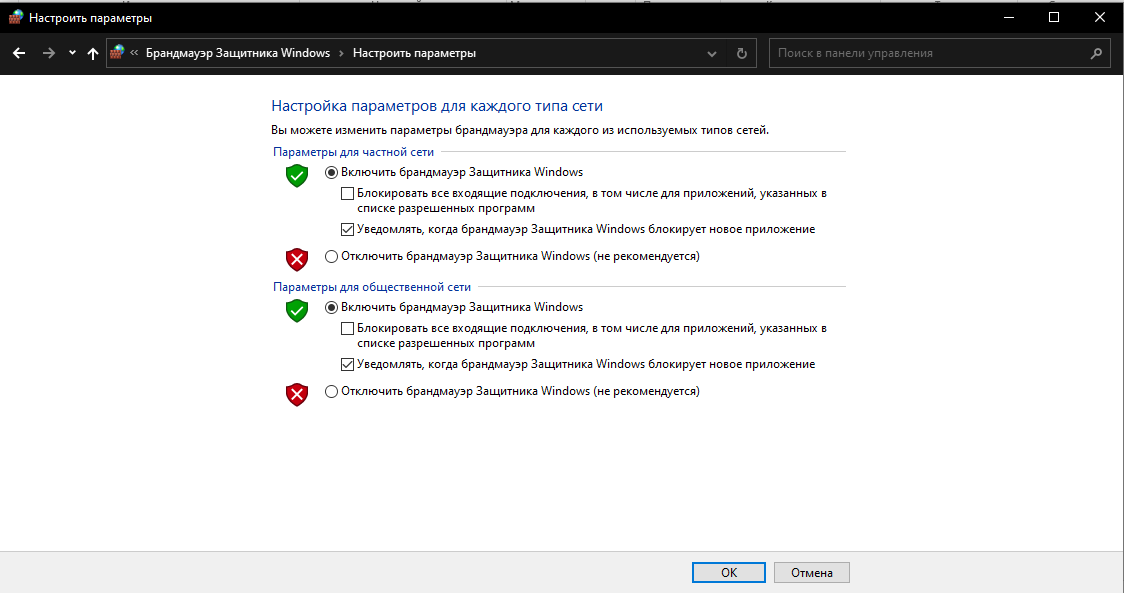
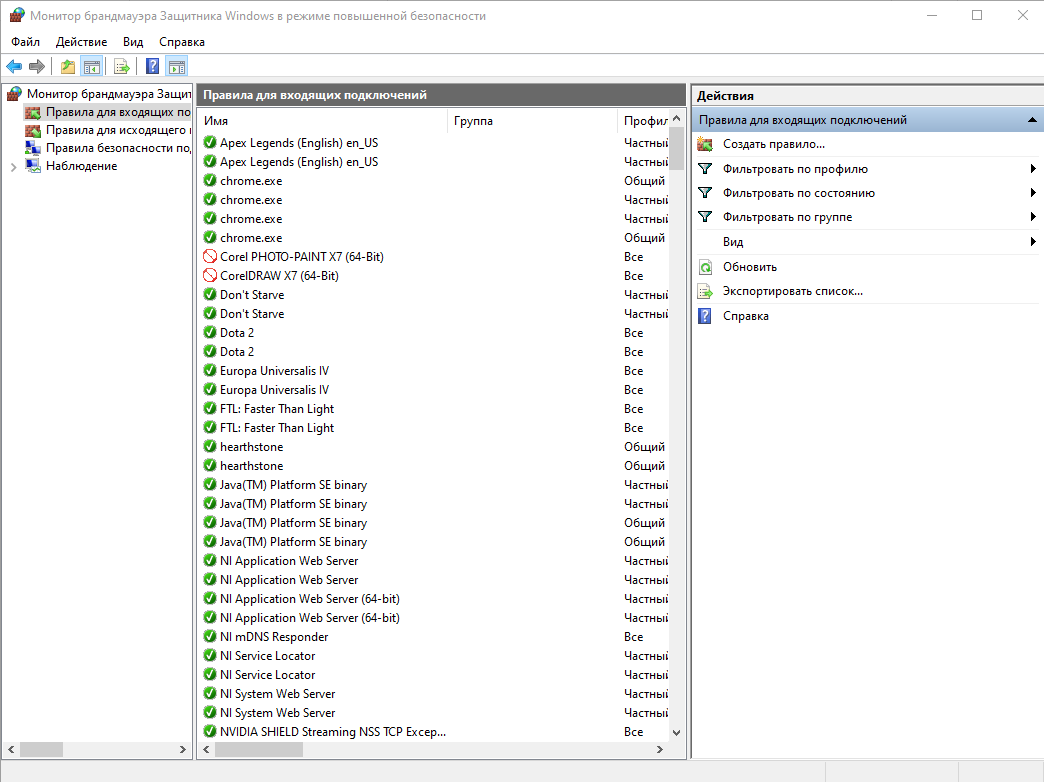


Рисунок 4.1 – Включение брандмауэра

2. Настройка входящих и исходящих подключений 

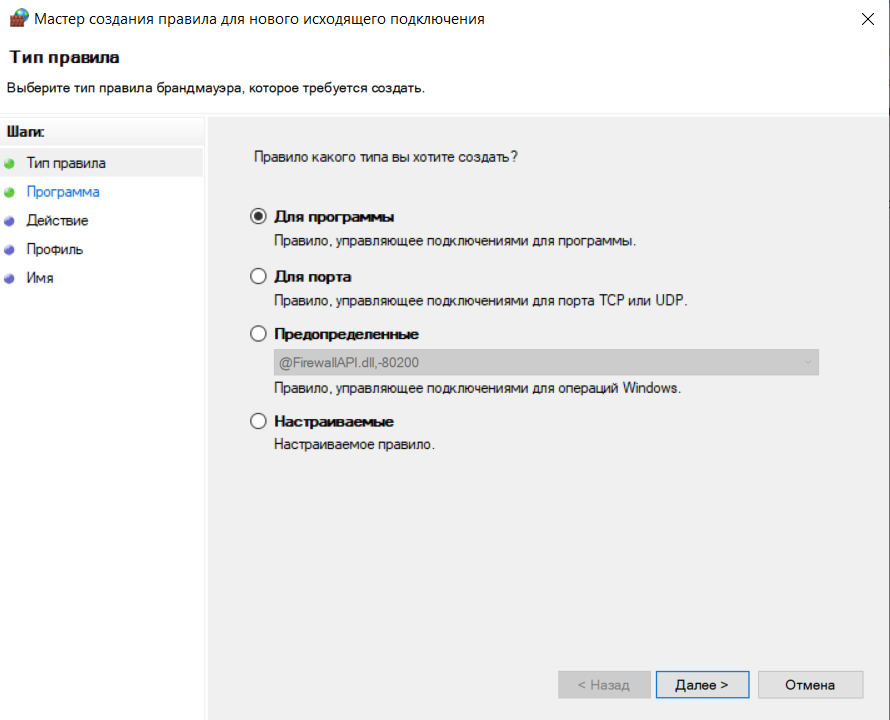
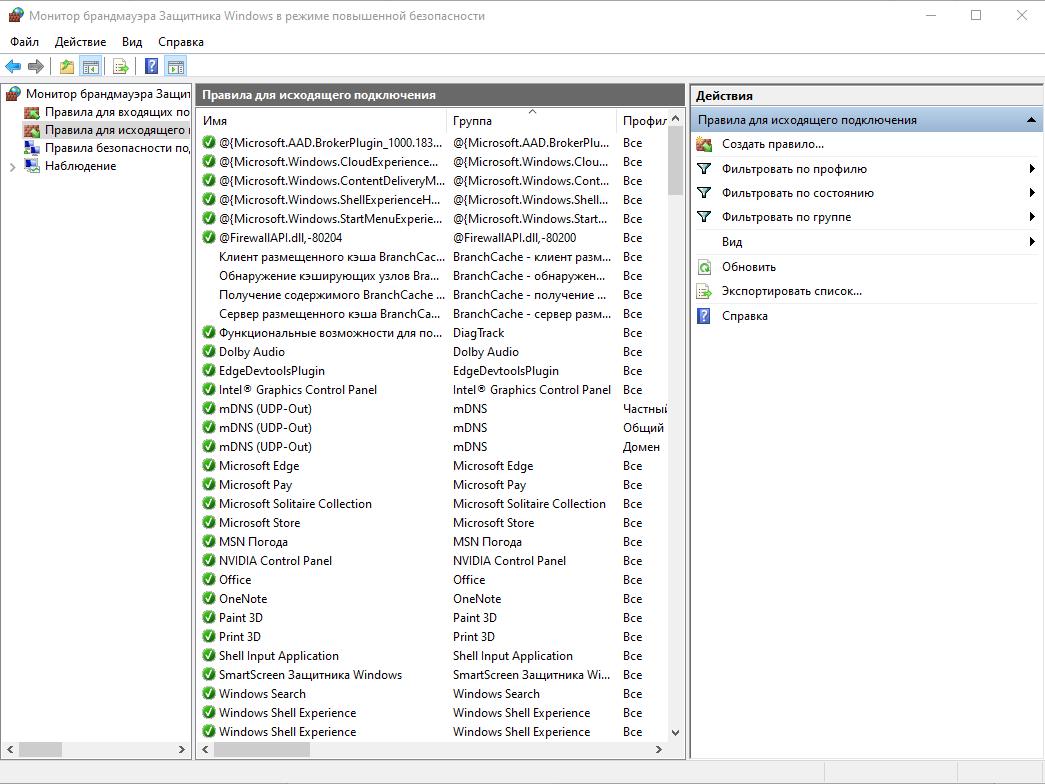
Рисунок 4.2 – Правила для входящих подключений  Рисунок 4.3 – Правила для исходящих подключений

Рисунок 4.4 - Мастер создания правил

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

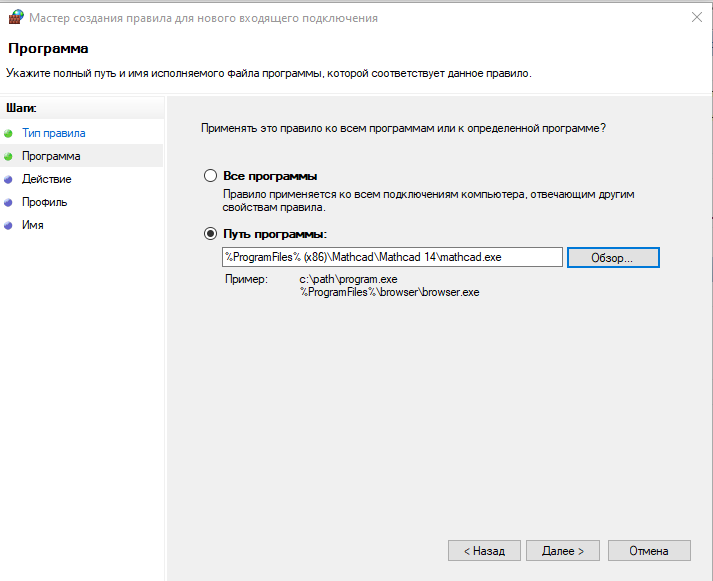


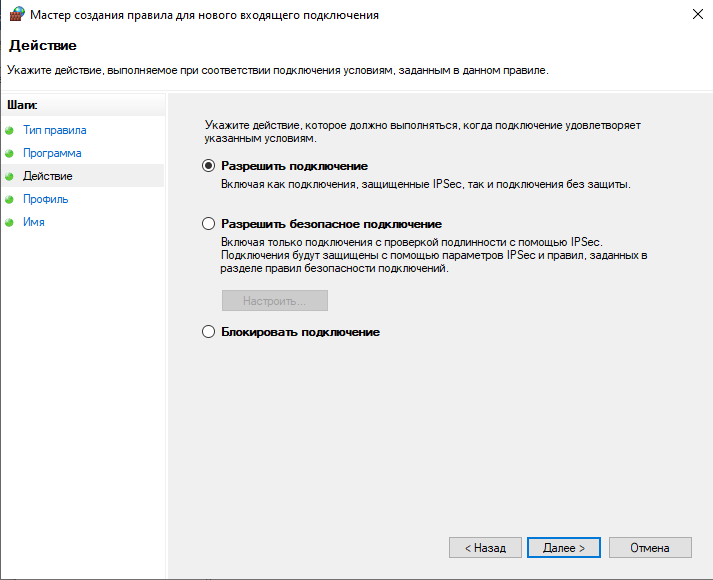
Рисунок 4.5 - Мастер создания правил, выбор пути

Рисунок 4.6 - Блокировка/разрешение подключения

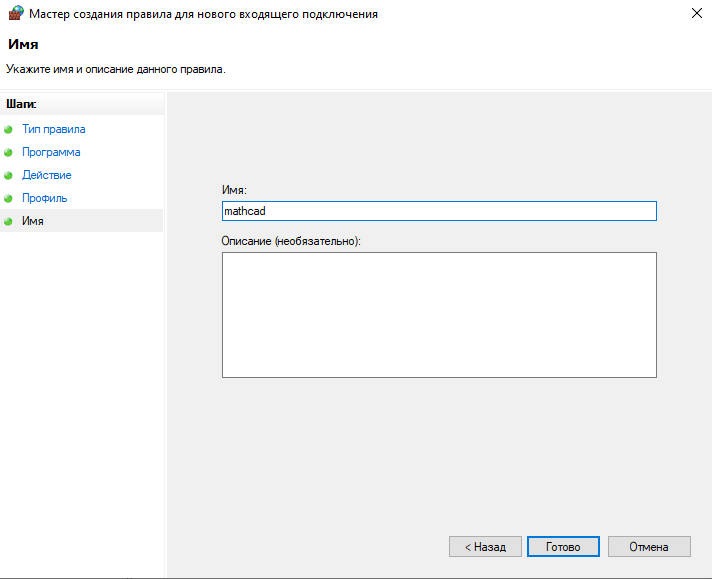


Рисунок 4.7 - Выбор имени

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

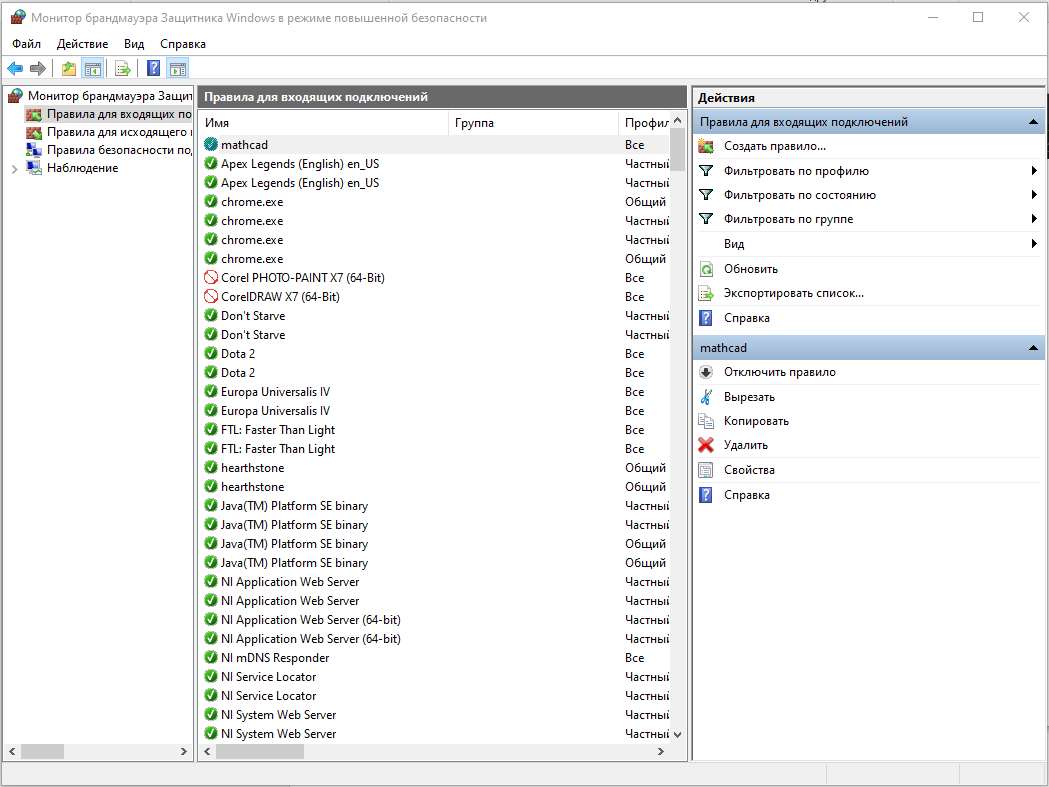


Рисунок 4.8 - Активные правила в списке

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

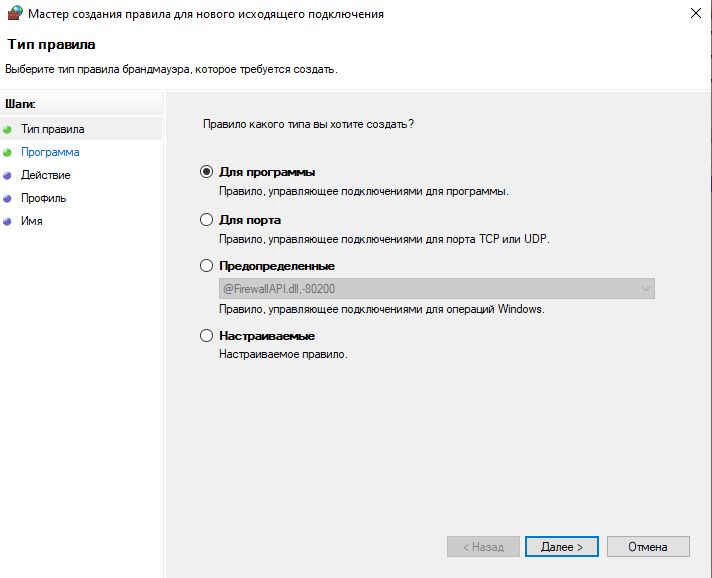


Рисунок 4.9 - Мастер создания правил

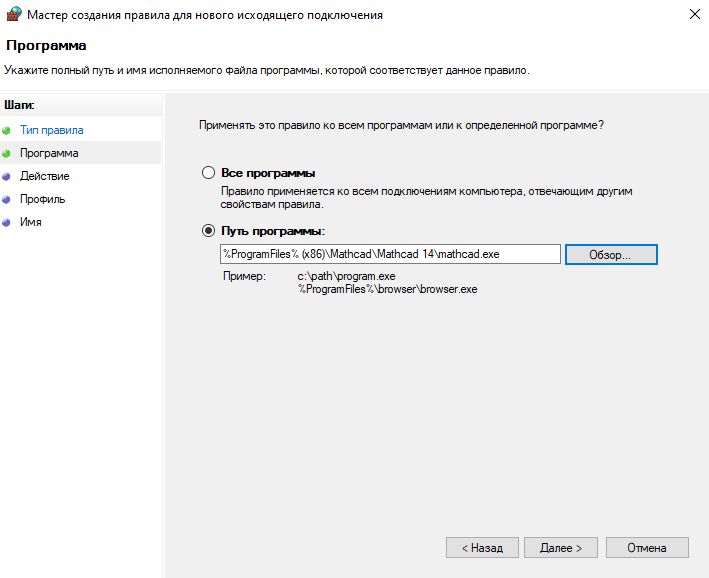


Рисунок 4.10 - Мастер создания правил, выбор пути

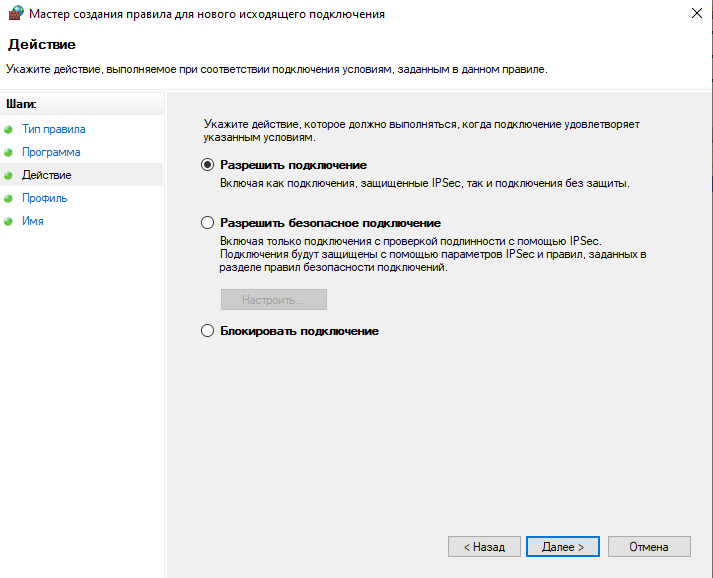


Рисунок 4.11 - Блокировка/разрешение подключения

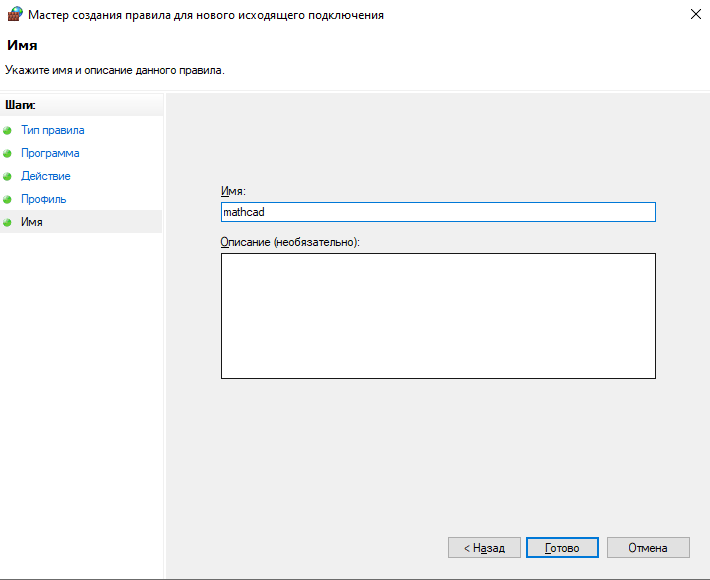


Рисунок 4.12 - Выбор имени

6. Опробовать действие нескольких команд:

1. Служба диагностики DirectX – dxdiag

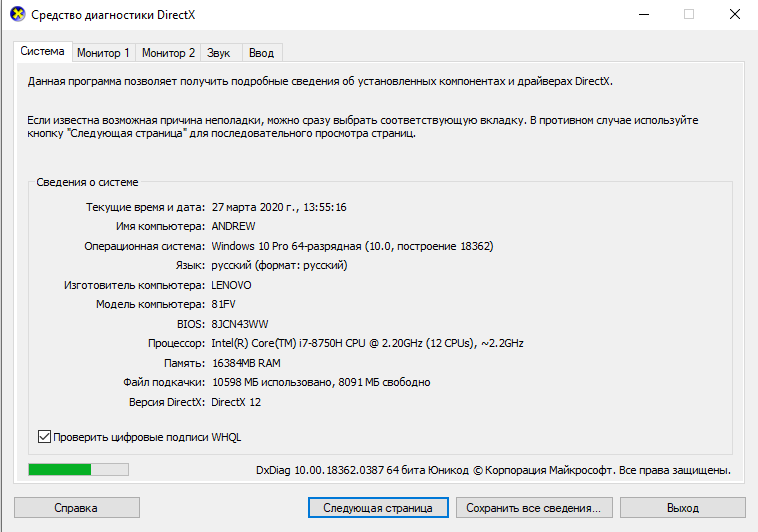


Рисунок 4.13 – Служба диагностики DirectX

2. Калькулятор – calc.

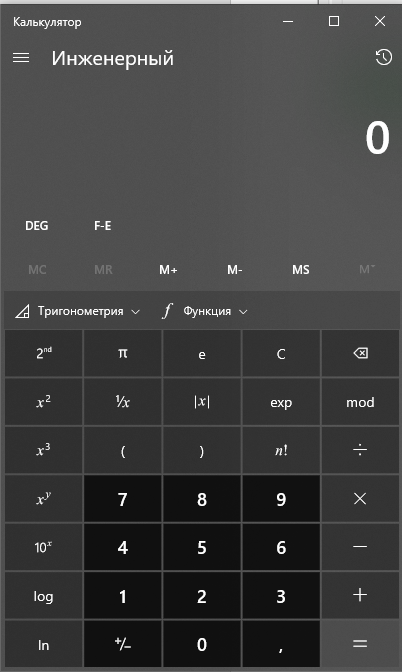


Рисунок 4.14 - Калькулятор

3. Производительность - perfmon.msc

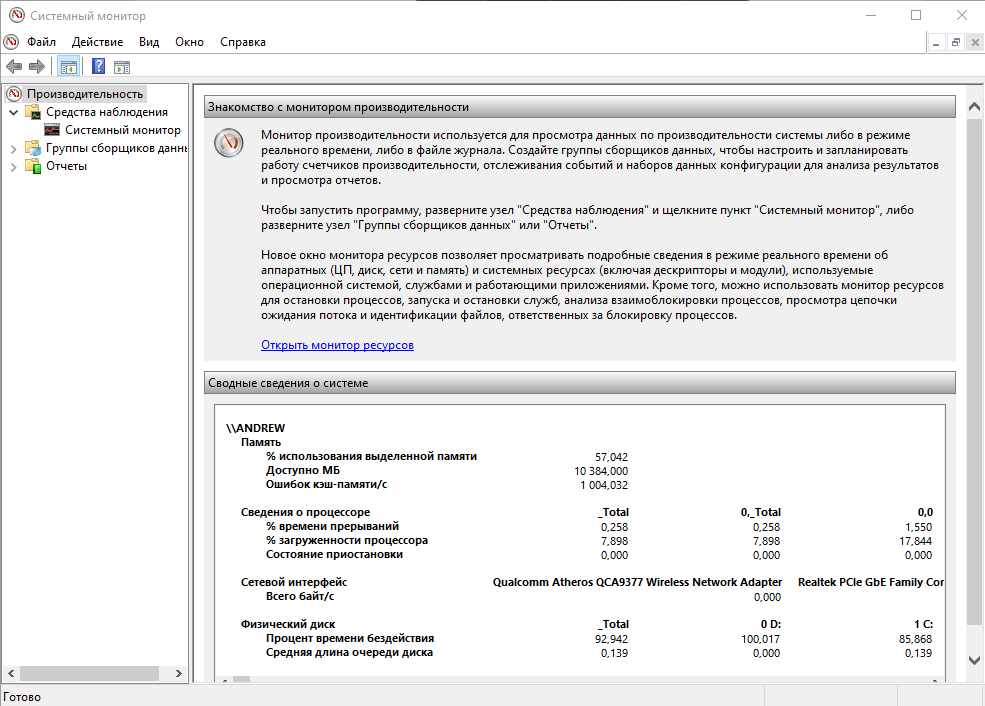


Рисунок 4.7 – Монитор производительности

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

**Практическое занятие №5**

**Тема «Криптографическая защита информации»**

**Теоретическое введение**

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

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

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

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

В англоязычной литературе зашифрование / расшифрование – enciphering / deciphering.

Классификация алгоритмов шифрования

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

1.1. Потоковые:

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

· с конечным ключом;

· на основе генератора псевдослучайных чисел.

1.2. Блочные:

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

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

· моноалфавитные;

· полиалфавитные;

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

· Диффи-Хеллман DH (Diffie, Hellman);

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

· Эль-Гамаль (ElGamal).

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

Обмен информацией осуществляется в 3 этапа:

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

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

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

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

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

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

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

·моноалфавитные (код Цезаря);

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

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



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

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

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

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

Схема обмена информацией такова:

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

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

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

**Алгоритм Диффи-Хелмана**

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

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

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

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

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

**Выполнение задания**

Практическая часть

1. Зашифровать сообщение «аникеенко егор вячеславович» с использованием шифра Цезаря и полученного секретного ключа.

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

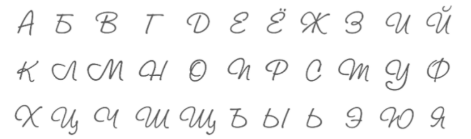
Шифруем по полученному ключу, равному 2, поэтому сдвиг будет происходить на два разряда вправо.

Рисунок 5.1 – Алфавит

Итог шифрования: впкмжжпмр жерт дбщжунвдрдкщ

Далее шифрование методом Трисемуса.

Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца.

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

Итог шифрования: гферммфрх мкхч йщюмшсгйхйею

Далее шифрование методом Плейфейра.

Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26 х 26 = 676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста.

Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – X, для русского алфавита — 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 | ч | ш | ъ | ы | ь |
| э | ю | я | 1 | 2 | 3 |

1) Разбиваем фразу на биграммы: ан ни ке ен ко ег ор вя че сл ав ов ич

2) Переводим биграммы по методу Плейфейра: тк мт мг мё лй ёд кх дэ ъг шс зг йж аъ

3) Приводим биграммы к конечному виду: ткмтмгмёлйёдкхдэъгшсзгйжаъ

Итоговый шифр: ткмтмгмёлйёдкхдэъгшсзгйжаъ

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. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

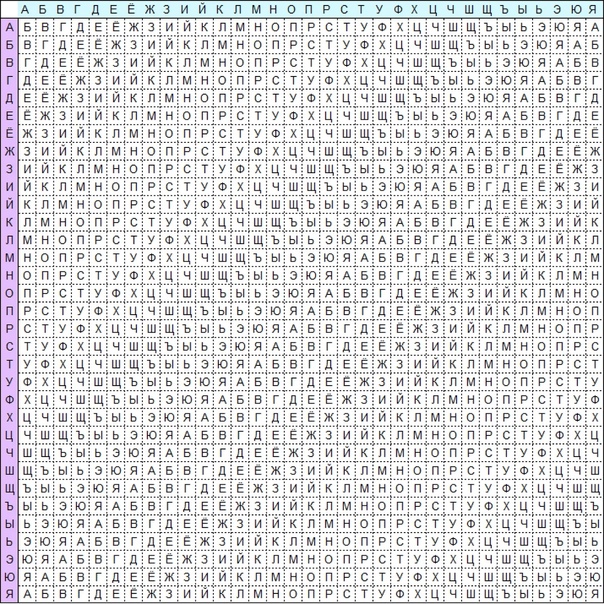


Рис 5.2 – таблица Виженера

1) Запишем фразу, которую нужно зашифровать без пробелов: аникеенкоегорвячеславович

2) Циклически запишем кодовое слово таким образом, чтобы его длина совпадала с фразой, которую необходимо зашифровать:

аникеенкоегорвячеславович

защитазащитазащитазащита

3) Совместим соответствующие буквы открытого и закрытого ключа для получения шифра: знвучехкзнхошвшачсуаычфия

Итоговый шифр: знвучехкзнхошвшачсуаычфия

2. Расшифровать следующее сообщение:

|  |  |  |
| --- | --- | --- |
| 2. | **съчпщг окхчхиге ичлкпщг** | Расшифровать с помощью шифра Цезаря. Ключ 7 |

Для того, чтобы расшифровать сообщение, которое было зашифровано по Цезарю, нужно производить сдвиг по алфавиту (рис. 5.1) не вправо, а влево.

Расшифрованное сообщение: курить здоровью вредить

Вывод: овладел основными криптографическими алгоритмами шифрования.

**Практическое занятие №6**

**Тема «Криптографическая защита информации»**

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

**Теоретические сведения**

*Реализация элементов криптосистемы RSA*

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

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других.

Весь алгоритм расписан в таблице:

|  |  |  |
| --- | --- | --- |
| 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} |

# *Реализация элементов схемы шифрования Эль-Гамаля*

## *****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).

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 

## *****Пример*****

**Шифрование**

Допустим, что нужно зашифровать сообщение ~M=5.

Произведем генерацию ключей:

пусть ~p=11, g=2. Выберем ~x=8 - случайное целое число ~x такое, что ~1 < x < p.

Вычислим ~y= g^x\bmod{p}=2^8\bmod{11}=3.

Итак, открытым является тройка ~(p,g,y)=(11,2,3), а закрытым ключом является число ~x=8.

Выбираем случайное целое число ~k такое, что 1 < k < (p − 1). Пусть ~k=9.

Вычисляем число ~a=g^k\bmod{p}=2^9 \bmod{11}=512 \bmod{11}=6.

Вычисляем число ~b=y^k M\bmod{p}=3^9 5 \bmod{11}=19683 \cdot 5 \bmod{11}=9.

Полученная пара ~(a,b)=(6,9) является шифротекстом.

**Расшифрование**

Необходимо получить сообщение ~M=5 по известному шифротексту ~(a,b)=(6,9) и закрытому ключу ~x=8.

Вычисляем M по формуле : ~M=b(a^x)^{-1}\bmod{p}=9(6^8)^{-1}\mod{11}=5

Получили исходное сообщение ~M=5.

*Реализация элементов схемы шифрования Дифи-Хеллмана*

## *****Генерация ключей*****

В 1976 году после публичной критики алгоритма DES и указания на сложность обработки секретных ключей Уитфилд Диффи (Whitfield Diffie) и Мартин Хеллман (Martin Hellman) опубликовали свой алгоритм обмена ключами. Это была первая публикация на тему криптографии с открытым ключом и, возможно, самый большой шаг вперед в области криптографии, сделанный когда‑либо.

Из‑за невысокого быстродействия, свойственного асимметричным алгоритмам, алгоритм Диффи‑Хеллмана не предназначен для шифрования данных. Он был ориентирован на передачу секретных ключей DES, ARS или других подобных алгоритмов через небезопасную среду. В большинстве случаев алгоритм Диффи‑Хеллмана не используется для шифрования сообщений, потому что он, в зависимости от реализации, от 10 до 1000 раз медленнее алгоритма DES.

До алгоритма Диффи‑Хеллмана было сложно совместно использовать зашифрованные данные из‑за проблем хранения ключей и передачи информации. В большинстве случаев передача информации по каналам связи небезопасна, потому что сообщение может пройти десятки систем, прежде чем оно достигнет потенциального адресата, и нет никаких гарантий, что по пути никто не сможет взломать секретный ключ. Уитфилд Диффи и Мартин Хеллман предложили зашифровывать секретный ключ DES по алгоритму Диффи‑Хеллмана на передающей стороне и пересылать его вместе с сообщением, зашифрованным с использованием DES. Тогда на другом конце его сможет расшифровать только получатель сообщения.

На практике **обмен ключами** по алгоритму Диффи‑Хеллмана происходит по следующей схеме.

1. 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.

**Самое сложное в алгоритме** Диффи‑Хеллмана обмена ключами – это понять, что в нем фактически два различных независимых цикла шифрования. Алгоритм Диффи‑Хеллмана применяется для обработки небольших сообщений от отправителя получателю. Но в этом маленьком сообщении передается секретный ключ для расшифровки большого сообщения.

**Сильная сторона алгоритма** - никто не сможет скомпрометировать секретное сообщение, зная один или даже два открытых ключа получателя и отправителя. В качестве секретных и открытых ключей используются очень большие целые числа. Алгоритм Диффи‑Хеллмана основан на полезных для криптографии свойствах дискретных логарифмов.

## *****Пример*****

Ева — криптоаналитик. Она читает пересылку Боба и Алисы, но не изменяет содержимого их сообщений.

* s = секретный ключ. s = 2
* g = простое число меньшее p. g = 5
* p = открытое простое число. p = 23
* a = секретный ключ Алисы. a = 6
* A = открытый ключ Алисы. A = ga mod p = 8
* b = секретный ключ Боба. b = 15
* B = открытый ключ Боба. B = gb mod p = 19



**Задание 1.**

Написать программу, которая получит общий секретный ключ из доступных публичных ключей с помощью алгоритма Диффи-Хеллмана.

Генерируйте секретный ключ Алисы и Боба, и высчитайте секретный ключ, удостоверьтесь что его одинаково смогут получить и Алиса и Боб.

Результат выполнения программы:

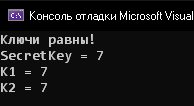


Рисунок 6.1. Реализация алгоритма Диффи-Хеллмана

Программа написана на языке C#.

**Задание 2.**

Написать программу, которая зашифрует и расшифрует текст, введенный с клавиатуры, зашифрует и расшифрует его алгоритмом RSA.

Ключи приведены в таблице.

|  |  |  |  |
| --- | --- | --- | --- |
| # | e | n | d |
| 1 | 13 | 1073 | 853 |
| 2 | 7 | 533 | 343 |
| 3 | 17 | 391 | 145 |
| 4 | 11 | 1121 | 95 |
| 5 | 17 | 497 | 173 |
| 6 | 17 | 989 | 761 |
| 7 | 5 | 559 | 101 |
| 8 | 13 | 403 | 277 |
| 9 | 17 | 493 | 369 |
| 10 | 11 | 779 | 131 |

Результат выполнения программы:

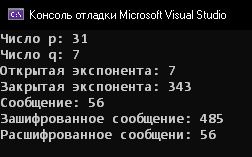


Рисунок 6.2. Реализация алгоритма RSA

Ключи использовались из строки 10. Программа написана на языке C#.

p = 89

q = 17

Сообщение: AAC

n = p \* q = 89 \* 17 = 1513

f(n) = (p - 1) \* (q - 1) = 88 \* 16 = 1408

e = 5;

Открытый ключ шифра: (5, 1513)

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

d вычисляется до тех пор, пока не получится первое целое число.

Причем k = 1, 2, 3 …

При k = 1, d – не целое число,

При k = 2, d – не целое число,

При k = 3, d = 845

Тогда закрытый ключ шифра: (845, 1513)

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

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

**Таблица 6.1. *Вычисление шифрограммы***

|  |  |  |
| --- | --- | --- |
| **Символы исходного сообщения, *Ti*** | **Коды символов *Ti*(табл. 6.1)** | **Зашифрованные коды символов*Ci*** |
| A | 65 | ***655mod 1513 = 1185*** |
| A | 65 | ***655mod 1513 = 1185*** |
| C | 67 | ***675mod 1513 = 1070*** |

Таким образом, мы исходное сообщение «AAC» представили в виде шифрограммы «1185, 1185, 1070».

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

http://altaev-aa.narod.ru/security/images/im10.png

**Таблица 6.3. *Восстановление сообщения***

|  |  |  |
| --- | --- | --- |
| **Зашифрованные коды символов *Ci*** | **Дешифрованные коды символов *Ti*(табл. 6.1)** | **Символы исходного сообщения,*Ti*** |
| 1185 | ***1185845 mod 1513 = 65*** | A |
| 1185 | ***1185845 mod 1513 = 65*** | A |
| 1070 | ***1070845mod 1513 = 67*** | C |

Таким образом, мы восстановили исходное сообщение «AAC».

**Задание 3.**

Написать программу, которая сгенерирует ключи, зашифрует и расшифрует текст, введенный с клавиатуры алгоритмом Эль-Гамаля.

В приложении приведен пример программы реализующий данный алгоритм, напишите на его примере программу обрабатывающую нашу задачу.

Результат выполнения программы:

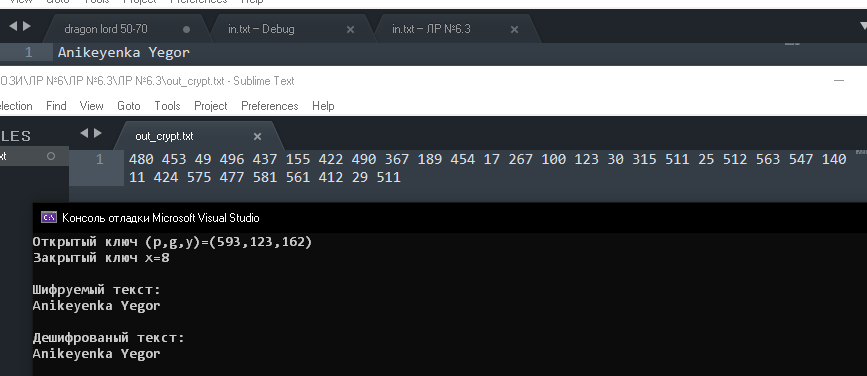


Рисунок 6.2. Реализация алгоритма Эль-Гамаля

Программа написана на языке C++.

**Вывод:** в ходе лабораторной работы я изучил и программно реализовал следующие алгоритмы шифрования: Эль-Гамаля, RSA, Диффи-Хеллмана. Также, вручную был проверен алгоритм шифрования и дешифрования RSA.

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

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

Разберем наглядный «бумажный» пример и пример с кодом. Возьмем основу 6-ой лабораторной работы.

**«Бумажный» пример**

p = 89

q = 17

Сообщение: AAC

n = p \* q = 89 \* 17 = 1513

f(n) = (p - 1) \* (q - 1) = 88 \* 16 = 1408

e = 5;

Открытый ключ шифра: (5, 1513)

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

d вычисляется до тех пор, пока не получится первое целое число.

Причем k = 1, 2, 3 …

При k = 1, d – не целое число,

При k = 2, d – не целое число,

При k = 3, d = 845

Тогда закрытый ключ шифра: (845, 1513).

*Отправка сообщения и электронной подписи:*

Отправка сообщения и ЭЦП на базе алгоритма RSA (отправитель **A**).



Возьмем хеш-образ из примера h = 7.

Тогда цифровая подпись s = 7^845 mod 1513 = 1485

Далее получателю отправляется исходное сообщение и цифровая подпись.

*Получение сообщения и проверка электронной подписи:*

Получение сообщения и проверка ЭЦП на базе алгоритма RSA (получатель **B**).



**Программная реализация этой же задачи (на основе 6-ой лабораторной работы)**

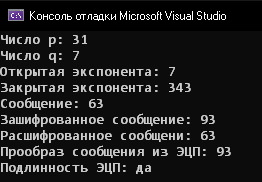


Рисунок 7.1 – Реализация ЭЦП на примере алгоритма RSA

**Контрольные вопросы:**

**1. Дайте определение понятию "электронная цифровая подпись".**

**Ответ:** 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. Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.**

**Ответ:** *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* 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.

**3. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП?**

**Ответ:** вначале отправитель использует свой закрытый ключ, а затем получатель применяет открытый ключ отправителя.

**4. Опишите схему протокола ЭЦП на основе алгоритма RSA.**

**Ответ:** выработка ЭЦП по формуле s = h^d mod n, где (d, n) – закрытый ключ отправителя. Вычисление хеш-образа из цифровой подписи по формуле h**”**= s^e mod n, где (e, n) – открытый ключ отправителя.

**5. Перечислите специальные схемы ЭЦП.**

**Ответ:**

* 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;
* и др.

**Вывод:** в ходе лабораторной работы была изучена и реализована ЭЦП на основе алгоритма RSA.

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

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

**Необходимые теоретические сведения**

Ниже рассматриваются: *N* – множество натуральных чисел, *Z* – множество рациональных чисел. Множество целых чисел *Z* – счетное, состоит из элементов 0; ±1; ±2; …; ± *n*,…. На нем определены две алгебраические операции – сложение и умножение. Эти операции обладают следующими свойствами (для любых ):

1. ассоциативность: ; ;

2. коммутативность: ; ;

3. существует нейтральный элемент – 0 и 1 соответственно:



4.  – закон дистрибутивности;

5. для каждого целого  существует единственное противоположное, то есть такое целое *b*, что *a* + *b* = *b* + *a* = 0.

*Теорема 2.1* (*О делении с остатком*). Для любых целых чисел *a* и *b*, , существует единственные целые числа *q* и  , такие, что .

В этом равенстве  называют остатком, а  – частным (неполным частным – при ) от деления *a*  на  При *r* = 0 величины *b* и *q* называют делителями или множителями числа *а*. Читатель со школьной скамьи умеет находить частное и остаток методом деления уголком.

*Следствие.* Пусть  – натуральное число,  Для всякого целого числа *a*  и максимального целого  с условием  существуют единственные целые  такие, что 

Такое равенство записывают сокращённо  или  (если *b* известно по контексту) и называют записью числа *a* в *b* – ичной позиционной системе счисления или системе счисления по основанию *b*. Нам кажется естественной привычная десятичная позиционная система записи целых чисел . В различных ситуациях более удобными оказываются другие основания. К примеру, во всех компьютерах на микроуровне вычисления проводятся в двоичной системе счисления. Для перехода к ней с десятичной применяют промежуточную – 16 - ричную систему счисления.

*Лемма 2.1.* Если в равенстве  все слагаемые – целые числа и все, кроме может быть одного, делятся на целое , то и это исключенное слагаемое делится на .

**Определение 2.1*.***Если целые числа  делятся на целое , то *d*  называют их *общим делителем*.

В дальнейшем речь идет только о положительных целых делителях.

**Определение 2.2.** Максимальный из общих делителей целых чисел  называется их *наибольшим общим делителем* и обозначается через НОД ().

*Теорема 2.2.* Если *,* то НОД *(a, b)* = НОД *(b, c).*

Теорема 2.2 позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

*Теорема 2.3.* Наибольший общий делитель целых чисел *a* и *b*   равен последнему отличному от нуля остатку цепочки равенств:

*;*

*;*

*…………………*

**

**

то есть  *=* НОД *.*

Теорема 2.3 формулирует алгоритм Евклида нахождения наибольшего общего делителя целых чисел. Его вариантом является следующий – второй способ вычисления наибольшего общего делителя по алгоритму Евклида – вычисляем последовательно разности  до получения последней ненулевой разности, которая и совпадает с НОД *(a, b).*

**Пример 2.1.** помощью алгоритма Евклида найти НОД (72, 26).

**Решение**. В соответствии с теоремой 2.2   ; . Следовательно, НОД (72, 26) = 2.

*Теорема 2.4.* Если *d* = НОД *(a, b)*, то существуют такие целые *u*  и *v*, что выполняется следующее соотношение (Безу): *d = au+ bv.*

**Пример 2.2.** Из примера 2.1 следует, что



Такой способ получения соотношения Безу для конкретных целых чисел называется расширенным алгоритмом Евклида. Он состоит из двух этапов: собственно алгоритма Евклида - прогонки вниз и прогонки вверх – последовательного выражения остатков в каждом из шагов предыдущего этапа (с соответствующим приведением подобных на каждом шаге).

**Определение 2.3.** Натуральное число ** называется *простым*, если оно делится только на1 и на себя.

*Теорема 2.5.* Всякое натуральное число ** либо является простым числом, либо имеет простой делитель.

Заметим, что из соотношения  натуральных чисел, больших единицы, следует, что, либо *p,* либо *q* принадлежит отрезку . Легко видеть, что наименьший натуральный делитель ** натурального числа ** является простым числом. Исторически первый метод проверки натурального числа ** на простоту заключается в делении его на простые числа, не превосходящие , носит название “решета Эратосфена”. К настоящему времени разработан достаточно большой цикл алгоритмов проверки числа на простоту.

*Теорема 2.6 (Евклид).* Простых чисел бесконечно много.

Значение простых чисел в том, что они по теореме 2.5 являются составными кирпичиками всех натуральных чисел.

**Определение 2.4.** Целые числа *a* и *b* называются *взаимно простыми,* еслиНОД .

*Теорема 2.7* (*Критерий взаимной простоты целых чисел*). Целые числа *a* и *b* взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство .

**Следствие.** НОД** тогда и только тогда, когдаНОД иНОД .

Важным в теории чисел и ее приложениях является следующее свойство взаимно простых целых чисел.

*Лемма 2.2.* Пусть произведение целых чисел *ab* делится на целое число *с* и НОД . Тогда *b* делится на *с*.

*Теорема 2.8**(Основная теорема арифметики)*. Всякое целое число ** однозначно раскладывается в произведение простых множителей

*.*

Если в этом равенстве собрать одинаковые множители, то получим каноническое разложение целого числа: .

**Пример 2.3.** Приведем примеры канонических разложений целых чисел:

а) 196 = 2⋅98 = 2⋅2⋅49 = 22⋅72;

б) 212-1 = 4095 = 32⋅5⋅7⋅13.

*Теорема 2.9.* Пусть *-* натуральное число*,* . Для любых целых чисел *a* и *b* следующие условия равносильны:

*1) a и b имеют одинаковые остатки от деления на *

*2) a – b делится на m, то есть a – b = mq для подходящего целого q;*

*3) a = b + mq для некоторого целого q.*

**Определение 2.5.**Целые числа *а* и *b* называются сравнимыми по модулю *m*, если они удовлетворяют одному из условий теоремы 2.9.Этот факт обозначают формулой ** илии называют данную формулу сравнением.

**Пример 2.4.** -57(mod 4) 11(mod 4) 23(mod 4) 3(mod 4).

**Пример 2.5.** Если  то всякое целое число сравнимо по модулю *m* со своим остатком от деления на *m*. Это следует из определения 2.5 и второго условия теоремы 2.9. Ведь *a*–*r* делится на *m*.

Основные свойства сравнений:

**1.** Пусть *.* Тогда  для всякого целого *c*, то есть к обеим частям сравнения можно добавить (или вычесть из обеих частей) одно и то же число.

**2.** Сравнения можно почленно складывать и вычитать: если **, *,* то  

**3.** Сравнения можно почленно перемножать: если ** *,* то **.

**4.** Сравнения можно почленно возводить в любую натуральную степень: если *,* то **.

**5.** Если в сравнении ** числа *a*, *b*, *m* имеют общий множитель *d*, то на него сравнение можно сократить: **.

**6.** Сравнение можно сократить на общий множитель, взаимно простой с модулем: если **, НОД (*d*, *m*) = 1, то из сравнения  следует сравнимость  и  по модулю .

**7.** Сравнение можно умножить на любой целый множитель: если **, то  для всякого целого *t*.

**8.** Рефлексивность: ** для любого целого *а* и всякого натурального *m* >1.

**9.** Симметричность: если **, то **.

**10.** Транзитивность: если **, **, то .

*Теорема 2.10*(*Малая теорема Ферма*). Пусть *p –* простое число и целое число *a* не делится на . Тогд*а .*

Теория сравнений и малая теорема Ферма позволяют быстро находить остаток от деления большого числа на простое число.

**Пример 2.6.** Найдем остаток от деления  на 31.

**Решение.** **. Поэтому в силу свойства 4 сравнений . Двоичная запись: 29=11101. Следовательно, для любого натурального *a* величина . Далее, . Поэтому . Тогда . Следовательно, . Таким образом, остаток от деления  на 31 равен 4.

**Индивидуальное задание к ПЗ**

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

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

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

4. Найти остаток от деления данного числа на простое.

1-3. *а* = 7049964661, *b* = 168687989.

4. Найти остаток от деления  на 17.

**Решение:**

* 1. *а* = 7049964661, *b* = 168687989

**a:**

|  |  |  |
| --- | --- | --- |
| 7049964661 | 79 | (7049964661: 79 = 89240059) |
| 89240059 | 79 | (89240059: 79 = 1129621) |
| 1129621 | 79 | (1129621: 79 = 14299) |
| 14299 | 79 | (14299: 79 = 181) |
| 181 | 181 | (181: 181 = 1) |
| 1 |  |  |

7049964661 = 79 · 79 · 79 · 79 · 181 = 794 · 181

**b:**

|  |  |  |
| --- | --- | --- |
| 168687989 | 79 | (168687989: 79 = 2135291) |
| 2135291 | 79 | (2135291: 79 = 27029) |
| 27029 | 151 | (27029 :151 = 179) |
| 179 | 179 | (179: 179 = 1) |
| 1 |  |  |

168687989 = 79 · 79 · 151 · 179 = 792 · 151 · 179

* 1. Алгоритмом Евклида:

7049964661 =168687989 ∙ 41 + 133757112;

168687989 = 133757112 ∙ 1 + 34930877;

133757112= 34930877 ∙ 3 + 28964481;

34930877= 28964481 ∙ 1 + 5966396;

28964481= 5966396 ∙ 4 + 5098897;

5966396= 5098897 ∙ 1 + 867499;

5098897 = 867499 ∙ 5 + 761402;

867499 = 761402 ∙ 1 + 106097;

761402 = 106097 ∙ 7 + 18723;

106097 = 18723 ∙ 5 + 12482;

18723 = 12482∙ 1 + 6241;

12482= 6241∙ 2;

Тогда, НОД (7049964661, 168687989) = 6241.

Найдём НОД (*a, b*), воспользовавшись разложением на простые множители чисел *a* и *b*, полученным в решении предыдущего задания: 7049964661 = 79 · 79 · 79 · 79 · 181 = 794 · 181; 168687989 = 79 · 79 · 151 · 179 = 792 · 151 · 179. Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел: НОД (7049964661, 168687989) = 792 = 6241.

**3.** Для нахождения целых *u*, *v*, удовлетворяющих соотношению Безу: *au* + *bv* = НОД  воспользуемся алгоритмом Евклида из второго задания и построим соотношение Безу для данных a и b.

НОД (7049964661, 168687989) = 6241.

7049964661 = 168687989 ∙ 41 + 133757112; поэтому 133757112 = 7049964661 + 168687989 ∙ (-41)

168687989 = 133757112 ∙ 1 + 34930877; поэтому 34930877=168687989 +133757112 ∙ (-1)

133757112= 34930877 ∙ 3 + 28964481; поэтому 28964481=133757112+34930877 ∙ (-3)

34930877= 28964481 ∙ 1 + 5966396; поэтому 5966396=34930877+28964481 ∙ (-1)

28964481= 5966396 ∙ 4 + 5098897; поэтому 5098897=28964481+5966396 ∙ (-4)

5966396= 5098897 ∙ 1 + 867499; поэтому 867499=5966396+5098897 ∙ (-1)

5098897 = 867499 ∙ 5 + 761402; поэтому 761402=5098897 +867499 ∙ (-5)

867499 = 761402 ∙ 1 + 106097; поэтому 106097=867499 +761402 ∙ (-1)

761402 = 106097 ∙ 7 + 18723; поэтому 18723=761402 +106097 ∙ (-7)

106097 = 18723 ∙ 5 + 12482; поэтому 12482=106097 +18723 ∙ (-5)

18723 = 12482∙ 1 + 6241; поэтому 6241=18723 +12482∙ (-1)

Тогда:

6241=18723 +12482∙ (-1)

6241=18723 + (106097 +18723 ∙ (-5)) ∙ (-1) = 18723 ∙ 6 + 106097 ∙ (-1)

6241= (761402 +106097 ∙ (-7)) ∙ 6 + 106097 ∙ (-1) = 761402 ∙ 6 + 106097 ∙ (-43)

6241= 761402 ∙ 6 + (867499 +761402 ∙ (-1)) ∙ (-43) = 761402 ∙ 49 + 867499∙ (-43)

6241= (5098897 +867499 ∙ (-5)) ∙ 49 + 867499∙ (-43) = 5098897 ∙ 49 + 867499 ∙ (-288)

6241= 5098897 ∙ 49 + (5966396+5098897 ∙ (-1)) ∙ (-288) = 5966396∙ (-288) + 5098897∙337

6241= 5966396∙ (-288) + (28964481+5966396 ∙ (-4)) ∙337= 5966396∙ (-1636) + 28964481∙337

6241= (34930877+28964481 ∙ (-1)) ∙ (-1636) + 28964481∙337= 34930877∙ (-1636) + 28964481∙1973

6241=34930877∙ (-1636) + (133757112 + 34930877 ∙ (-3)) ∙1973 = 133757112∙1973 + 34930877 ∙ (-7555)

6241=133757112∙1973 + (168687989 +133757112 ∙ (-1)) ∙ (-7555) = 168687989 ∙ (-7555) + 133757112∙9528

6241=168687989 ∙ (-7555) + (7049964661 + 168687989 ∙ (-41)) ∙9528 = 7049964661∙9528 + 168687989 ∙ (-398203)

Следовательно:

6241=7049964661 ∙ 9528 + 168687989 ∙ (-398203)

*u* = 9528, *v =* -398203

1. Найти остаток от деления  на 17.

1997 делится на 17 с остатком 8.

19972делится на 17 с остатком 13.

19973делится на 17 с остатком 2.

19974делится на 17 с остатком 16.

19975делится на 17 с остатком 9.

19976делится на 17 с остатком 4.

19977делится на 17 с остатком 15.

19978делится на 17 с остатком 1.

19979делится на 17 с остатком 8.

Получили один из предыдущих остатков, значит «зациклились». Число 19979 дает тот же остаток деления на 17, что и 19971. Значит, длина цикла равна 8. 2004 = 250 \* 8 + 4. Число 19972004 дает тот же остаток от деления на 17, что и 19974, то есть 16.

**Вывод:** в ходе лабораторной работы я изучил основные сведения из курса теории чисел, нашел каноническое разложение двух чисел и НОД этих чисел двумя способами, соотношение Безу этих чисел.