Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Электронная тетрадь**

по дисциплине «Основы защиты информации»

Студентка: Дрожжа А.Д.

ФИТ 2курс 11 группа

Преподаватель: Берников В.О.

Минск 2021

**Практическое занятие №1**

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

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

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

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

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

− формирование и поступательное развитие информационного общества;

− равноправное участие Республики Беларусь в мировых информационных отношениях;

− преобразование информационной индустрии в экспортно-ориентированный сектор экономики;

− эффективное информационное обеспечение государственной политики;

− обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

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

− 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

− 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;

**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.

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

Таблица 2.1−Данные для лабораторной работы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № 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 |

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:

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

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

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

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

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

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

|  |  |
| --- | --- |
|  | (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 была найдены разработки 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 А1»

Студентка: Дрожжа А.Д.

ФИТ 2 курс 11 группа

Преподаватель: Берников В.О.

Минск 2021

**ВВЕДЕНИЕ**

Актуальность темы данной работы определяется возросшим уровнем проблем информационной безопасности даже в условиях стремительного роста технологий и инструментальной базы для защиты данных. Невозможно обеспечить стопроцентный уровень защиты корпоративных информационных систем, при этом корректно расставляя приоритеты в задачах по защите данных в условиях ограниченности доли бюджета, направленной на информационные технологии. Надежная защита вычислительной и сетевой корпоративной инфраструктуры является базовой задачей в области информационной безопасности для любой компании, в том числе и для унитарного предприятия «А1».

Эффективная защита IT-инфраструктуры и прикладных корпоративных систем сегодня невозможна без внедрения современных технологий контроля сетевого доступа. Участившиеся случаи кражи носителей, содержащих ценную информацию делового характера, все больше заставляют принимать организационные меры.

**Политика информационной безопасности** – это высокоуровневый документ, который включает в себя принципы и правила, определяющие и ограничивающие определенные виды деятельности объектов и участников системы информационной безопасности, направленные на защиту информационных ресурсов организации. Как известно, стратегическое планирование позволяет определить основные направления деятельности организации, связав воедино маркетинг, производство и финансы. Долгосрочный стратегический план позволяет компании выстроить все свои бизнес-процессы с учетом микро и макросреды для достижения наилучших финансовых показателей и темпов экономического роста.

Важной составляющей в стратегическом планировании является учет требований политики информационной безопасности, которые должны быть краеугольным камнем при определении среднесрочных и долгосрочных целей и задач организации. С ростом компании и пересмотром планов политика также должна пересматриваться. Низкоуровневые документы информационной безопасности необходимо пересматривать в соответствии с реализацией краткосрочных планов.

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

Эффективное обеспечение требуемого уровня информационной безопасности организации возможно только при наличии формализованного и системного подхода к выполнению мер по защите информации. Целью разработки политики информационной безопасности организации является создание единой системы взглядов и понимания целей, задач и принципов обеспечения информационной безопасности.

**Описание структуры бизнес-компании**

По варианту необходимо разработать политику безопасности для оператора мобильной связи «А1». Для того, чтоб описать все взаимоотношения субъектов и объектов, разберемся в терминологии используемой в данном пункте.

**Информационная безопасность** — это одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным состоянием (уровнем) защищенности, а защита информации – это процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы.

Под **субъектами** информационных отношений понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры.

**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.

**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. Операторы мобильных сетей предлагают своим клиентам пакеты услуг для решения различных задач (звонки и СМС/интернет), в частности высоким спросом пользуются предложения для бизнеса. Сотовая сеть является одним из самых распространенных в наше время видов мобильной радиосвязи. Ключевая особенность заключается в том, что вся зона покрытия оператора разбивается на отдельные ячейки.

На каждом участке за работу мобильной сети отвечает базовая станция, с которой обмениваются данными все телефонные аппараты на участке.

В местах с хорошим качеством связи оборудование оператора располагается на относительно небольшом расстоянии. Таким образом, участки покрытия отдельных базовых станций перекрываются, образуя сеть, внешний вид которой схематически напоминает пчелиные соты. Отсюда и пошло название «сотовая сеть».

Компания А1 предоставляет услуги связи стандарта GSM 900/1800, UMTS (WCDMA/HSDPA/HSUPA/HSPA+), 4G на территории Беларуси. Абонентам оператора доступны базовые услуги (голосовая связь, передача данных, SMS, MMS, голосовая почта и др.), а также дополнительные сервисы (роуминг, услуги для бизнеса и развлекательные услуги). Видеосервис от А1 предоставляется под брендом VOKA. Для всех пользователей сервиса доступны фильмы, мультфильмы и сериалы онлайн-кинотеатров MEGOGO, Амедиатека, START, ivi, more.tv, а также контент студии Disney. Сервис доступен для мобильных устройств на Android и iOS, для Smart TV на Tizen, WebOS, Android TV, через приставки Redbox Mini, Xiaomi Mi Box 3, Apple TV (через AirPlay). На компьютерах пользоваться видеосервисом можно через приложение VOKA для Windows или через веб-версию.

Для оператора сотовой связи **объектами** информационной системы выступают: документы об оказании услуг клиентам; носители, хранящие информацию о клиентах; различные базы данных, архивы, директории; папки, хранящиеся на электронных устройствах; ПО, которое предназначено для нормального функционирования отдела сотовой связи. Договор заключается путем подписания клиентом регистрационной формы или иными способами, предусмотренными Порядками оказания услуг. Услуги предоставляются клиенту при наличии в его собственности, владении либо пользовании оконечного абонентского устройства (модема, маршрутизатора, ТВ-приемника, ТВ-приставки и т.п.), сертифицированного в Национальной системе подтверждения соответствия Республики Беларусь. Предлагая подписать договор, компания обязуется предоставлять качественные услуги и соответственно не разглашать личную информацию клиента. Так как оператор сотовой связи предлагает и мобильное приложение для мобильного телефона, то нужно и учитывать клиент согласен на сбор, поиск, обработку, накопление, хранение, проверку, использование и совершение иных действий с данными и сведениями о нем и его персональными данными в Приложении, а также на передачу Компанией сведений о Пользователе привлеченными ими партнерами, которые осуществляют взаимодействие с Компанией для идентификации и последующих уведомлений.

**Персональные данные Пользователей включают в себя:**

− ФИО;

− Адрес электронной почты;

− Пароль, необходимые для регистрации в Приложении;

−  История событий за семь календарных дней, содержащая информацию о смене статуса подключенных к Приложению датчиков мониторинга и устройств управления и полученных уведомлениях об опасностях, отображаемая во вкладке «История» в Приложении;

−  Информация, создаваемая пользователями в Приложении вне раздела редактирования Аккаунта (в том числе Названия помещений, Фото и Картинки помещений, Локация устройств в Помещении, количество Помещений, Сценарии использования Устройств, а также режим Охраны);

− Информация, полученная в результате действий Пользователя в Приложении (в частности, информация о входе и выходе из Приложения). Данная информация о Пользователе может быть доступна Компании в соответствии с настройками пользователя;

− Паспортные данные;

−  Видеозаписи Пользователя за 24 часа, хранящиеся в облачном хранилище Компании;

−  История событий за семь календарных дней, содержащая информацию о смене статуса подключенных к Приложению датчиков мониторинга и устройств управления и полученных уведомлениях об опасностях, отображаемая во вкладке «История» в Приложении;

− Дополнительные данные, получаемые при доступе к Приложению, включающие в себя данные о технических средствах (устройствах), технологическом взаимодействии с Приложением (в т.ч. IP-адрес хоста, вид операционной системы пользователя, данные, полученные в результате доступа к камере, микрофону и т.п. устройств, ID используемого устройства, Пароль от устройства, Данные точки доступа клиента, к которой подключено устройство, и последующих действиях Пользователя в Приложении;

 Целью настоящих 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**

Под **угрозой** информационной безопасности объекта понимаются возможные воздействия на него, приводящие к ущербу. **Источник угрозы** — это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

**Уязвимость объекта** — это присущие объекту причины, приводящие к нарушению безопасности информации на объекте.

**Атака** — это возможные последствия реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости. Атака – это всегда пара «источник – уязвимость», реализующая угрозу и приводящая к ущербу. 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». Угрозами безопасности информации являются **нарушения** при обеспечении:

− конфиденциальности;

− доступности;

− целостности.

**Конфиденциальность информации** — это свойство информации быть известной только аутентифицированным законным ее владельцам или пользователям.

**Доступность информации** — это свойство информации быть доступной для аутентифицированных законных ее владельцев или пользователей.

**Целостность информации** — это свойство информации быть неизменной в семантическом смысле при воздействии на нее случайных или преднамеренных искажений, или разрушающих воздействий.

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.

Угрозы информационной безопасности делятся на два основных типа — это **естественные и искусственные** угрозы. Если помещения с носителями ценной информации располагаются в непосредственной близости от водоемов, то они подвержены угрозе потери информации вследствие наводнения. Единственное что можно предпринять в данной ситуации — это исключить хранение носителей информации на первых этажах здания, которые подвержены затоплению.

Еще одной естественной угрозой являются молнии. Очень часто при ударах молнии выходят из строя сетевые карты, электрические подстанции и другие устройства. Особенно ощутимые потери, при выходе сетевого оборудования из строя, несут крупные организации и предприятия, такие как банки. Во избежание подобных проблем необходимо соединительные сетевые кабели были экранированы (экранированный сетевой кабель устойчив к электромагнитным помехам), а экран кабеля следует заземлить. Для предотвращения попадания молнии в электрические подстанции, следует устанавливать заземленный громоотвод, а компьютеры и серверы комплектовать источниками бесперебойного питания.

Следующим видом угроз являются **искусственные** угрозы, которые в свою очередь, делятся на непреднамеренные и преднамеренные угрозы. **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. Сюда же можно отнести и другие «эксперименты», которые не являлись злым умыслом, а люди, совершавшие их, не осознавали последствий. К сожалению, этот вид угроз очень трудно поддается контролю, мало того, чтобы персонал был квалифицирован, необходимо чтобы каждый человек осознавал риск, который возникает при его несанкционированных действиях.

**Преднамеренные** угрозы-угрозы, связанные со злым умыслом преднамеренного физического разрушения, впоследствии выхода из строя системы. К преднамеренным угрозам относятся внутренние и внешние атаки. Вопреки распространенному мнению, крупные компании несут многомиллионные потери зачастую не от хакерских атак, а по вине своих же собственных сотрудников. Современная история знает массу примеров преднамеренных внутренних угроз информации — это проделки конкурирующих организаций, которые внедряют или вербуют агентов для последующей дезорганизации конкурента, месть сотрудников, которые недовольны заработной платой или статусом в фирме и прочее. Для того чтобы риск таких случаев был минимален, необходимо, чтобы каждый сотрудник организации соответствовал, так называемому, «статусу благонадежности».

**Оценка рисков**

Целью анализа рисков, связанных с эксплуатацией информационных систем (ИС), является **оценка угроз** (т. е. условий и факторов, которые могут стать причиной нарушения целостности системы, ее конфиденциальности, а также облегчить несанкционированный доступ к ней) и уязвимостей (слабых мест в защите, которые делают возможной реализацию угрозы), а также определение комплекса контрмер, обеспечивающего достаточный уровень защищенности ИС. При оценивании рисков учитываются многие факторы: ценность ресурсов, значимость угроз, уязвимостей, эффективность имеющихся и планируемых средств защиты и многое другое.

В настоящее время используются два подхода к анализу рисков - базовый и полный вариант. Выбор зависит от оценки собственниками ценности своих информационных ресурсов и возможных последствий нарушения режима информационной безопасности. В простейшем случае собственники информационных ресурсов могут не оценивать эти параметры. Подразумевается, что ценность ресурсов с точки зрения организации не является чрезмерно высокой. В этом случае анализ рисков производится по упрощенной схеме: рассматривается стандартный набор наиболее распространенных угроз без оценки их вероятности и обеспечивается минимальный или базовый уровень ИБ.

Полный вариант анализа рисков применяется в случае повышенных требований к ИБ. В отличие от базового варианта в том или ином виде оцениваются ресурсы, характеристики рисков и уязвимостей. Как правило, проводится анализ соотношения стоимость/эффективность нескольких вариантов защиты.

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;

Для данных и программного обеспечения выбираются применимые к данной ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10.

К примеру, если данные содержат подробности коммерческой конфиденциальной (критичной) информации, эксперт, проводящий исследование, задает вопрос: как может повлиять на организацию несанкционированный доступ посторонних лиц к этой информации?

Возможен такой ответ: провал сразу по нескольким параметрам из перечисленных выше, причем каждый аспект следовало бы рассмотреть подробнее и присвоить ему самую высокую из возможных оценок.

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

Задача управления рисками включает выбор и обоснование выбора контрмер, позволяющих снизить величины рисков до приемлемых. При выборе варианта средств обеспечения безопасности активов, в зависимости от разработанной стратегии управления рисками, определяются подходы к снижению риска, такие как уменьшение риска, уклонение от риска, изменение характера риска, принятие риска. Управление рисками включает в себя также оценку стоимости реализации контрмер, которая должна быть меньше величины возможного ущерба. Разница между стоимостью реализации контрмер и величиной возможного ущерба должна быть тем больше, чем меньше возможность (достоверность) причинения ущерба.

**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. Выбор варианта защиты активов осуществляется на основании результатов оценки рисков с учетом требований безопасности и существующих стоимостных и других ограничений.

**Система мер**, рекомендуемая для большинства компаний, перед которыми стоит вопрос защиты информации, призвана обеспечить соблюдение основных признаков ее безопасности:

− Доступность сведений. Под этим определением понимается возможность и для авторизованного субъекта в любое время получить требуемые данные, и для клиентов в регулярном режиме получать информационные услуги;

− Целостность информации. Это означает ее неизменность, отсутствие любых посторонних, неавторизованных вмешательств, направленных на изменение или уничтожение данных, нарушение системы их расположения;

− Конфиденциальность или абсолютная недоступность данных для неавторизованных субъектов;

− Отсутствие отказа или невозможность отрицать принадлежность действий или данных;

− Аутентичность или возможность достоверного подтверждения авторства информационных сообщений или действий в системе.

Выделяют 4 **основные задачи** организационно-управленческой деятельности в сфере информационной безопасности: обеспечение комплексности всех решений, реализуемых в процессе обеспечения информационной безопасности; обеспечение непрерывности и целостности процессов информационной безопасности; решение методических задач, лежащих в основе эффективного управления информационной безопасностью (вопросов управления рисками, экономического моделирования и т.п..).; управление человеческими ресурсами и поведением персонала с учетом необходимости решения задач информационной безопасности. При этом данные задачи должны решаться в комплексе и непрерывно. Управление человеческими ресурсами в рамках управления информационной безопасностью включает в себя комплекс задач, охватывающий все основные аспекты деятельности людей: отбор и допуск персонала для работы с определенными информационными ресурсами, обучение, контроль правильности выполнения обязанностей, создание необходимых условий для работы и т.п. Под организационным обеспечением и менеджментом в сфере информационной безопасности обычно принято понимать решение управленческих вопросов на уровне отдельных субъектов (предприятий, организаций) или групп таких субъектов (партнеров по бизнесу, организаций, которые совместно решают определенные задачи, требующие защиты информации)



**Рисунок 5.1**− Классификация методов обеспечения информационной безопасности на основе технических средств

Защита информационной инфраструктуры от несанкционированного доступа обеспечивается регламентацией доступа субъектов (работников) к объектам (носителям данных и каналам их передачи). Организационный метод обеспечения информационной безопасности не подразумевает использования технического инструментария. Такая информационная безопасность зачастую состоит, например, в удалении ОТСС за периметр охраняемой территории на максимально возможное расстояние.

**Вывод**

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

Эффективное обеспечение требуемого уровня информационной безопасности организации возможно только при наличии формализованного и системного подхода к выполнению мер по защите информации. Целью разработки политики информационной безопасности организации является создание единой системы взглядов и понимания целей, задач и принципов обеспечения информационной безопасности.

Определение эффективности реализации требований безопасности является одной из ключевых задач обеспечения безопасности активов на всех этапах жизненного цикла объектов информационных технологий (ОИТ). Ее решение связано с разработкой соответствующих методик, методов и средств оценки эффективности защиты активов, которая затруднена рядом объективных факторов, обусловленных сложностью и динамичностью процессов и информационных потоков, существующих в ОИТ, стремительным развитием информационных технологий, хаотичностью возникновения новых видов угроз, приводящих к появлению новых уязвимостей аппаратных и программных средств как в самом объекте информационных технологий, так и в средствах обеспечения безопасности.

Адекватный уровень ИБ в современной организации может быть обеспечен только на основе комплексного подхода, реализация которого начинается с разработки и внедрения эффективных ПБ. Эффективные ПБ определяют необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски ИБ до приемлемой величины. Они оказывают минимальное влияние на производительность труда, учитывают особенности бизнес-процессов организации, поддерживаются руководством, позитивно воспринимаются и исполняются сотрудниками организации. Для того чтобы ПБ оставалась эффективной, необходимо осуществлять непрерывный контроль ее исполнения, повышать осведомленность сотрудников организации в вопросах ИБ и обучать их выполнению правил, предписываемых ПБ. Регулярный пересмотр и корректировка правил ПБ необходимы для поддержания ее в актуальном состоянии.

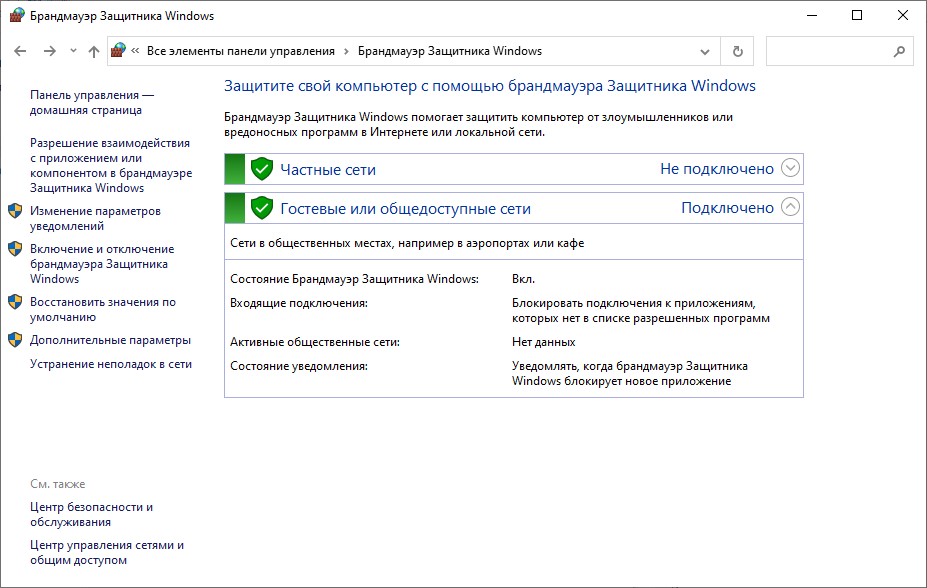
Разработка и внедрение ПБ в организации – процесс коллективного творчества, в котором должны участвовать представители всех подразделений, затрагиваемых производимыми изменениями. Координатором этого процесса является специалист, на которого руководство организации возлагает ответственность за обеспечение ИБ.

**Практическое занятие №4**

**Тема «Настройка Брандмауэра Windows»**

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

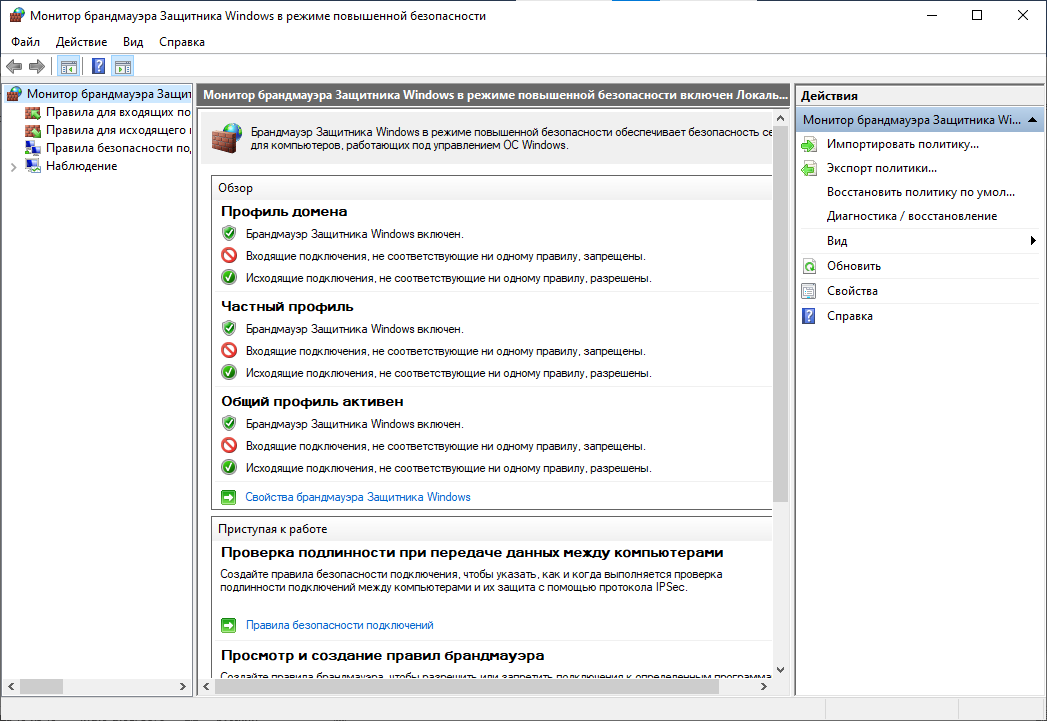
**Задание 1.** Создать правила для входящих подключений (с помещением в электронный конспект копий экрана с пояснениями промежуточных действий)



**Рисунок 4.1 −** Окно Брандмауэра Защитника Windows

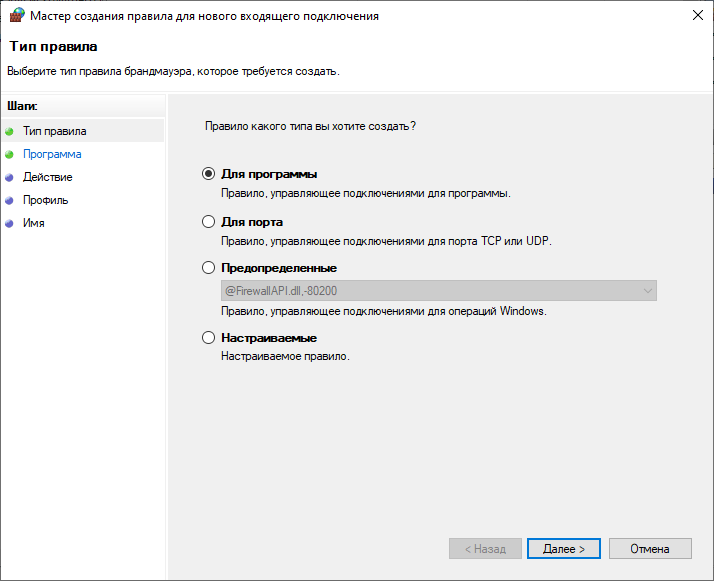
Заходим в Панель управления− Брандмауэр Защитника Windows и проверяем, включен ли брандмауэр. Так как он включен, то можно переходить к созданию правил. Для этого выбираем «Дополнительные параметры» «слева» окна. Откроется новое окно (Рис. 4.2).

Для создания нового правила на входящие подключения «слева» выбираем Правила для входящих подключений − Создать правило. Откроется мастер создания правил для новых входящих подключений (Рис. 4.3). В открывшемся окне выбираем «Для программы», так как необходимо перекрыть доступ к сети конкретной программе. Создадим блокирующее правило для Microsoft Edge. Следуя методическим указаниям создалось правило на блокировку. Выполняя аналогичные действия создадим разрешающее правило для программы Google Chrome (Рис. 4.4). Создание входящих подключений закончено.



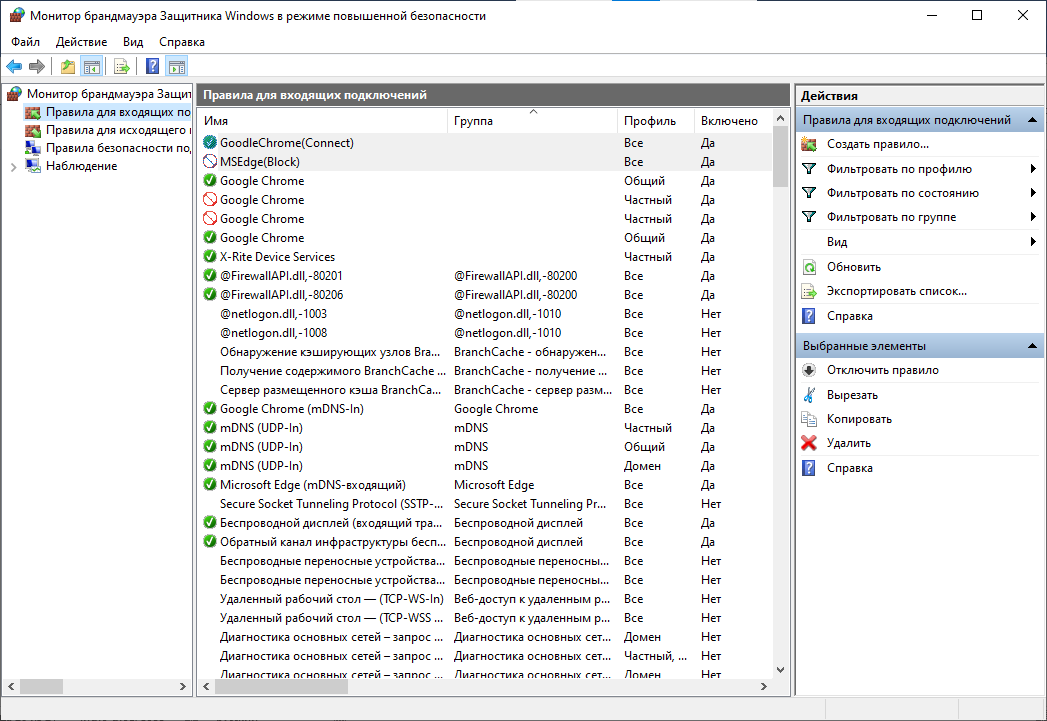
**Рисунок 4.2 −** Монитор Брандмауэра Защитника Windows

В открывшемся окне выбираем «Для программы», так как необходимо перекрыть доступ к сети конкретной программе. Создадим блокирующее правило для Microsoft Edge.

****

**Рисунок 4.3 −** Мастер создания правила для входящего подключения

Выполняя аналогичные действия создадим разрешающее правило для программы Google Chrome (Рис. 4.4). Создание входящих подключений закончено.

****

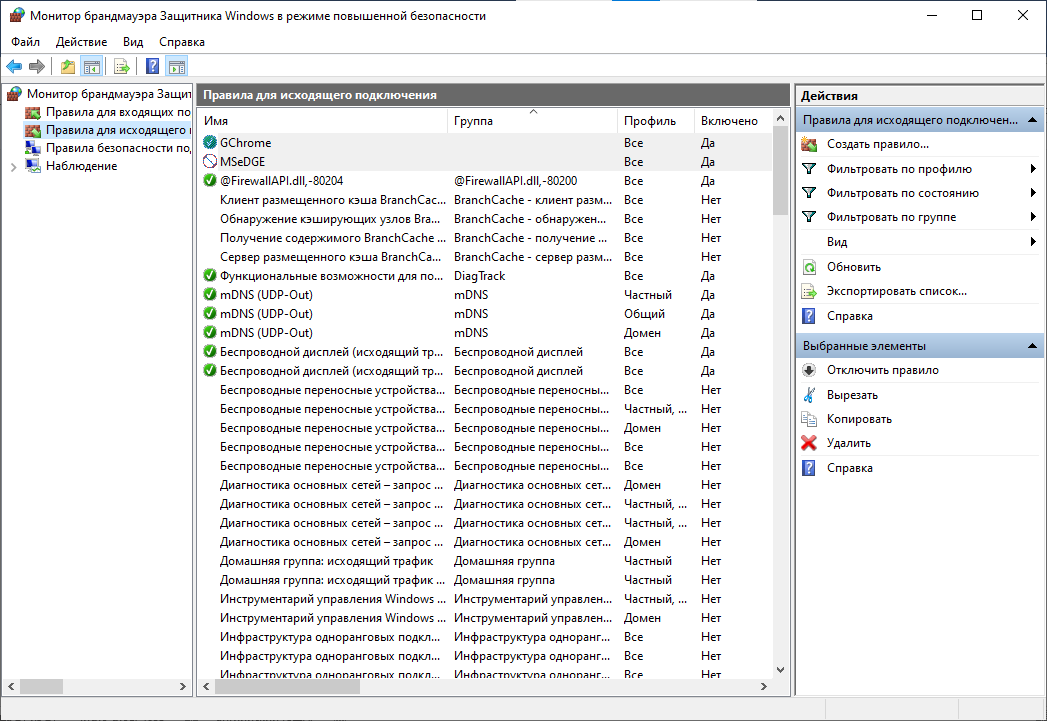
**Рисунок 4.4 −** Создание блокирующего правила MSEdge(Block) и разрешающего правила GoogleChrome(Connect)

**Задание 2.** Создать правила для исходящих подключений (с помещением в электронный конспект копий экрана с пояснениями промежуточных действий)

Для создания нового правила на исходящее подключение «слева» выбираем Правила для исходящих подключений − Создать правило. Откроется мастер создания правил для новых входящих подключений. В открывшемся окне выбираем «Для программы», так как необходимо перекрыть доступ к сети конкретной программе. Создадим блокирующее правило для Microsoft Edge. Следуя методическим указаниям создалось правило на блокировку. Выполняя аналогичные действия создадим разрешающее правило для программы Google Chrome (Рис. 4.5). Создание исходящих подключений закончено.

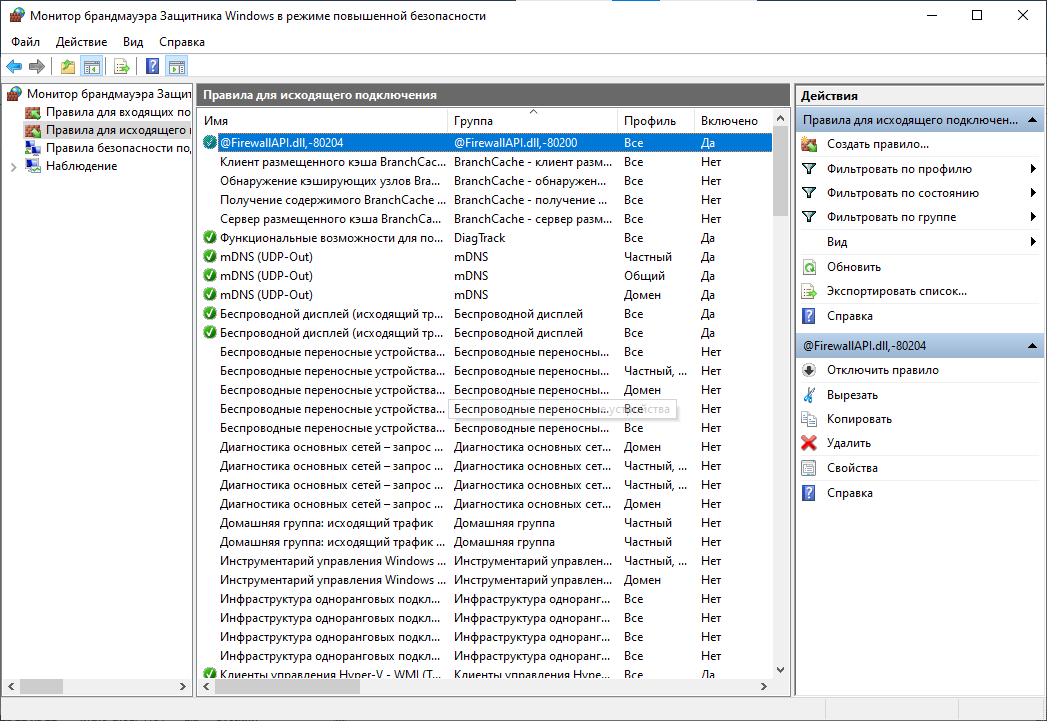
**Задание 3.** Вернуть настройки Брандмауэра в исходное состояние до начала выполнения практического задания.

Для того, чтобы ернуть настройки в первоначальное положение, удаляем созданные правила в колонке «слева». Так как брандмауэр был включен и до этого, то дополнительных действий больше не требуется (Рис. 4.6).

****

**Рисунок 4.5 −** Создание блокирующего правила MSeDGE и разрешающего правила GChrome

Для того, чтобы ернуть настройки в первоначальное положение, удаляем созданные правила в колонке «слева». Так как брандмауэр был включен и до этого, то дополнительных действий больше не требуется (Рис. 4.6).

****

**Рисунок 4.6 −** Возврат настроек к первоначальному состоянию

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

**Практическое занятие №5**

**Тема «Криптографическая защита информации»**

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

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

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

ФИО: Дрожжа Анастасия Дмитриевна;

Используя шифр **Цезаря** используем алфавит и определенное значение ключа. Номер варианта 8, значит ключ для шифрования будет равен 8.

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 У00** б, в, г,д, е, ё, ж, й, к, л, м, н, о, п, р, с, ф, х, ц,

**Ответ:**

Дрожжа=ьдвяяч,

АНАСТАСИЯ=чбчеёчеац

ДМИТРИЕВНА=ьуаёдаэъбч

**Шифровка текста с помощью метода Трисемуса**:

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

**Ответ:**

Дрожжа=ЛЩЦООВ,

АНАСТАСИЯ=ВХВЪЕВЪДЩ

ДМИТРИЕВНА=ЛФДЕЩДМЙХВ

**Шифровка текста с помощью метода Плейфейра**:

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

Делим исходный текст на биграммы: др-ож-жа, ан-ас-та-си-яъ, дм-ит-ри-ев-на

**Ответ:**

Дрожжа=ож-др-ди,

АНАСТАСИЯ=зо-фз-уз-цз-юы

ДМИТРИЕВНА= КЖ-ВЗ-ЦВ-БЖ-ОЗ

**Шифровка текста с помощью метода Вижинера**:

Шифр Виженера состоит из последовательности нескольких [шифров Цезаря](https://questhint.ru/shifr-tsezarya/) с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера.

**Ответ:**

Дрожжа= лрзпщу,

АНАСТАСИЯ= знщъеущиш

ДМИТРИЕВНА= мяьървнфбз

**Задание 2.** Расшифровать следующие сообщения:

Таблица 5−Данные для лабораторной работы

|  |  |  |
| --- | --- | --- |
| **№** | **Сообщение** | **Способ** |
|  | Ие михежцчжшйч сшихуцчб | Расшифровать с помощью шифра Цезаря. Ключ 5 |
|  | съчпщг окхчхиге ичлкпщг | Расшифровать с помощью шифра Цезаря. Ключ 7 |
|  | ьоъщочто т лечшыхтлшыьё | Расшифровать с помощью шифра Цезаря. Ключ 10 |
|  | Лжбзеииеизиачзнр | Расшифровать с помощью **Магического квадрата**   |  |  |  |  | | --- | --- | --- | --- | | 7 | 12 | 1 | 14 | | 2 | 13 | 8 | 11 | | 16 | 3 | 10 | 5 | | 9 | 6 | 15 | 4 | |
|  | тяеонаыбиьсрль\_т | Расшифровать с помощью **Магического квадрата**   |  |  |  |  | | --- | --- | --- | --- | | 9 | 16 | 2 | 7 | | 6 | 3 | 13 | 12 | | 15 | 10 | 8 | 1 | | 4 | 5 | 11 | 14 | |
|  | иоарткдпвл\_натоа | Расшифровать с помощью **Магического квадрата**   |  |  |  |  | | --- | --- | --- | --- | | 7 | 12 | 1 | 14 | | 2 | 13 | 8 | 11 | | 16 | 3 | 10 | 5 | | 9 | 6 | 15 | 4 | |
|  | гэ ишн зижшпэг оюжи | Расшифровать с помощью шифра Цезаря.  Ключ 8.  Ключевое слово ВЕСНА |
|  | дороюё дъ нозбъвё жодщйц | Расшифровать с помощью шифра Цезаря.  Ключ 5.  Ключевое слово ОСЕНЬ |

Ключевое слово: Осень;

Ключ:5;

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,

**Исходный текст**: дороюё дъ нозбъвё жодщйц

**Первоначальный текст**: нечего на зеркало пенять

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

**Практическое занятие №6**

**Тема «Криптографическая защита информации»**

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

**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.

|  |
| --- |
| static void DiffieHellman (int p, int g)  {  //Alice and Bob Key Gen  int AliceSK = r.Next(1, 11); // Алиса генерирует свой закрытый ключ  int BobSK = r.Next(1, 11); // Боб генерирует свой закрытый ключ  int AliceOK =  power(g, AliceSK, p); // С помощью своего числа, закрытого ключа и ключа Алиса генерирует открытый ключ  int BobOK = power(g, BobSK, p); // С помощью своего числа, закрытого ключа и ключа Боб генерирует открытый ключ  int AliceSessionKey = power(BobOK, AliceSK, p); //Алиса, получив открытый ключ Боба, генерирует ключ сессии  int BobSessionKey = power(AliceOK, BobSK, p); //Боб, получив открытый ключ Алисы, генерирует ключ сессии  if (AliceSessionKey == BobSessionKey)  {  Console.WriteLine($"Закрытый ключ Алисы: {AliceSK}");  Console.WriteLine($"Открытый ключ Алисы: {AliceOK}");  Console.WriteLine($"Закрытый ключ Боба: {BobSK}");  Console.WriteLine($"Открытый ключ Боба: {BobOK}");  Console.WriteLine($"Ключи сессии совпадают: {AliceSessionKey}");  }  else  {  Console.WriteLine("Ключи сессии не совпадают");  } |
|  |

**Задание 2**

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

|  |
| --- |
| static void RSA(string message)  {  int e = 13, n = 1073, d = 853;  int[] encryptedMessage = new int[message. Length];  for (int i = 0; i < message.Length; i++)  {  encryptedMessage[i] = modpow(message[i], e, n);  }  Console.WriteLine("--Зашифрованное сообщение--");  for (int i = 0; i < encryptedMessage.Length; i++)  {  Console.Write(encryptedMessage[i]);  }  Console.WriteLine();  char[] decryptedMessage = new char[encryptedMessage.Length];  for (int i = 0; i < message.Length; i++)  {  decryptedMessage[i] = Convert.ToChar(modpow(encryptedMessage[i], d, n));  }  Console.WriteLine("--Расшифрованное сообщение--");  Console.WriteLine(decryptedMessage);  } |
|  |

**Задание 3**

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

|  |
| --- |
| int y = power(g, x, p);  Console.WriteLine($"Открытый ключ (p,g,y) = {p}, {g}, {y}");  Console.WriteLine($"Закрытый ключ x = {x}");  int k = r.Next(1, p); // 1 < k < (p-1)  int a = power(g, k, p);  int M = Convert.ToInt32(message);  int b = mul(power(y, k, p), M, p);    Console.Write($"Шифротекст: \na:{a}\nb:{b}");  Console.WriteLine();  decrypt(a, p, x, b);  }  static void decrypt(int a, int p, int x, int b)  {  Console.WriteLine("--Расшированный текст--");  Console.WriteLine($"{b \* Math.Pow(a, p-1-x) % p}");  } |
|  |

**Вывод**: были изучены ассиметричные криптографические методы шифрования и решены практические задачи.

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

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

**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").

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

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

**Практическое занятие №9**

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

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

**Практическое занятие №10**

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

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

1. Основные составляющие описания изобретения?
2. Правила оформления описания изобретения?
3. Какие основные пункты должна содержать заявка на изобретение?
4. Основные документы, необходимые для подачи заявки на изобретения?
5. ОТЛИЧИЯ заявок на охранные документы различных объектов промышленной собственности?
6. На какие ОПС выдаются патенты?
7. На какие ОПС выдаются свидетельства?

**Практическое занятие №11**

**Тема «Патентные исследования»**

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

**Практическое занятие №11**

**Тема «Патентный поиск»**

**Цель:** освоить навыки проведения патентного поиска по заданной тематике.

**Практическое занятие №13**

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

**Цель:** Овладеть навыками подготовки документации для регистрации компьютерных программ.