Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Дисциплина «Основы защиты информации»

Отчёт по практическому занятию №1

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

Студент: Корело К.А.

ФИТ 2 курс 2 группа

Преподаватель: Ржеутская Н.В.

**Практическое занятие №1**

**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 объекта ‑ через К, тогда:

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

где К≥1.

Выражения (2.1) – (2.2) 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 | *E*0 | *E* | *K* | *C* |
| 12 | 21000 | 18000 | 3 | 900 |

Согласно формуле (2.1), эффективность функционирования объекта с учетом воздействия несанкционированного доступа:

Согласно формуле (2.2), относительная эффективность:

Согласно формуле (2.4), снижение эффективности функциональности объекта при наличии средств защиты равно:

Согласно формуле (2.5), выражение для эффективности и относительной эффективности примут вид:

Согласно формуле (2.9), непосредственно изменяет эффективность:

Вычитая , мы узнаем знак разности этих эффективностей:

Поскольку знак разности положительный, то число, от которого вычитали, больше (а следовательно эффективность функционирования объекта при наличии средств защиты выше, чем эффективность функционирования объекта с учетом воздействия несанкционированного доступа при отсутствии средств защиты).

**Вывод:**

По итогам проведённых вычислений было получено, что >Е, а это значит, что для обеспечения максимальной эффективности объекта защита эффективна.

**Практическое задание №2**

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

Цель: Разработать проект политики информационной безопасности бизнес-компании.

**Задание для выполнения.**

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

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

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

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

Индивидуальное задание:

|  |  |
| --- | --- |
| 12. | Туристическая компания |

**Введение**

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

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

Основные этапы разработки политики информационной безопасности следующие:

* Исследование текущего состояния информационной среды и информационной безопасности организации;
* Анализ полученных сведений по результатам исследования;
* Формирование плана работ по разработке политики информационной безопасности;
* Разработка политика информационной безопасности организации.

Безопасность информационной инфраструктуры компании подразумевает защиту от случайных или умышленных действий, которые могут нанести вред владельцам данных или их пользователям.

Действия лиц, несущих ответственность за какую-либо сферу, должны быть направлены на создание защиты, препятствующей утечкам данных, а не борьбу с их последствиями. Но при этом важно сохранять простой доступ к информации тем людям, которые на законных основаниях пользуются базами данных.

Отсутствие правильно разработанной и внедренной политики информационной безопасности чаще всего становится большой удачей для злоумышленников в случаях кибератак.

В большинстве случаев краже подлежат следующие данные:

* Информация о реальном финансовом состоянии компании;
* Инновационные разработки научно-технических отделов;
* Регистрационные данные для доступа к защищенным серверам;
* Персональные данные работников.

Утечка этих сведений с использованием любых каналов незаконного перехвата информации приводит к следующим видам ущерба:

* Ухудшение деловой репутации компании;
* Отзыв лицензии или иного допуска к сведениям, которые охраняются особым образом;
* Потеря клиентов, снижение интенсивности денежного потока;
* Потеря собственных разработок, маркетинговых исследований, приоритета при выпуске нового продукта;
* Утрата влияния на рынке, отдельных секторов рынка;
* Прямые иски о возмещении вреда, вызванного утратой коммерческой тайны контрагентов, или морального вреда.

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.

**1.1 Описание структуры бизнес-компании (туристическое агентство)**

Под **структурой управления** туристской фирмы понимается упорядоченная совокупность взаимосвязанных элементов, находящихся в устойчивых взаимоотношениях, обеспечивающих их функционирование и развитие как единого целого.

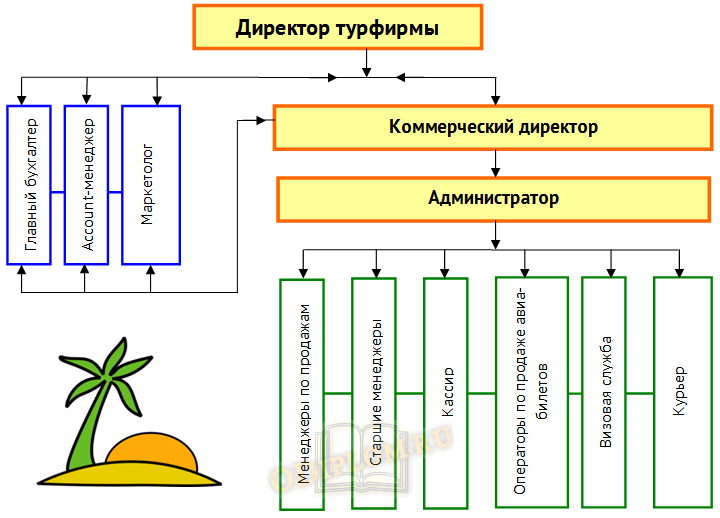
Элементами структуры являются отдельные работники, службы и другие звенья, задействованные в деятельности фирмы.

Типовой набор услуг турфирмы:

* Услуги в области туризма, организация и участие в организации и эксплуатации отелей, турбаз, мотелей, услуги по организации экскурсий, обслуживание частных и деловых поездок, культурных, гастрольных, благотворительных и других мероприятий;
* Организация туристических поездок, командировок специалистов;
* Осуществление международной туристической деятельности в ближнем и дальнем зарубежье;
* Продажа авиабилетов на внутренние и зарубежные рейсы авиакомпаний различных стран;
* Реализация путевок в здравницы и дома отдыха.

Функции турфирмы вытекают из сферы её деятельности: предоставление населению возможностей отдохнуть во время отпуска.

*Пример структуры турфирмы:*



В соответствии с типовой организационной структурой в турфирме существует 3 уровня управления:

1. Генеральный директор – обеспечивает общий контроль и управление всеми отделами. Также непосредственно ему подчиняются главный бухгалтер, который доводит до его сведения всю финансовую информацию, account-менеджер и маркетолог, которые работают по утвержденным директором стратегическим планам на определенный период.
2. Коммерческий директор – в его задачи входит доведение управленческой информации от директора к администратору, текущее управление работой маркетолога и account-менеджера, взаимодействие с главным бухгалтером сбор ежедневной выручки, работа с партнерами турагентства за рубежом, определение цен на предлагаемые услуги и утверждение цен с генеральным директором, осуществление контактов с организациями, осуществляющими внешний контроль за работой агентства.
3. Администратора – основной функцией является общее координирование работы офиса, т.е. он отвечает за организацию непосредственно процесса работы, он является передаточным звеном между коммерческим директором и сотрудниками офиса. Также он занимается распределением клиентов между менеджерами, чтобы не допустить избыточной загруженности одного их них и в то же время не допустить, чтобы неопытный менеджер стал работать с слишком требовательным клиентом.

В понятие информационной безопасности туристической фирмы входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы.

Вторым аспектом понятия станет безопасная обработка банковских данных и реализация всех требований PCI DSS (стандарта защиты данных в индустрии платежных карт). Ведь туризм – одна из отраслей, наиболее часто использующих платежи через интернет. Бронирование номеров в гостиницах, резервирование авиабилетов и другой инфраструктуры с оплатой через всемирную сеть – самое обычное явление в сфере путешествий и туризма.

**1.2 Оценка рисков**

Проблемы информационной безопасности постоянно усугубляется процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем. Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением.

Виды угроз информационной безопасности предприятия

Существует несколько причин, по которым становится возможным незаконный доступ до конфиденциальной информации злоумышленниками. Среди них особенно опасными являются следующие:

**1)** Халатное отношение сотрудников компании к защите цифровых данных.

Основные причины нарушения безопасности со стороны сотрудников:

* Переход по фишинговой ссылке с рабочего компьютера и заражение вредоносной программой корпоративной сети;
* Хранение конфиденциальных данных на сменных носителях информации;
* Пересылка информации с секретными данными по обычной электронной почте или через незащищенный мессенджер.

**2)** Использование нелицензионных программ

Коммерческие компании часто экономят средства на приобретении ПО и позволяют сотрудникам пользоваться пиратскими версиями офисных приложений и профессиональных программ. Однако при этом возникает опасность внедрения в сеть вирусов и других вредоносных программ.

Кроме того, использование пиратского ПО влечет за собой дополнительные минусы:

* Отсутствие периодических обновлений, которые «латают дыры» в системе защиты;
* Отсутствие технической поддержки со стороны разработчиков;
* Невозможность проверки подлинности кода приложения.

**3)** Работа вредоносных программ

Компьютерные вирусы – распространенная угроза безопасности IT-инфраструктуры компании. Ущерб, нанесенный вредоносными программами, исчисляется миллионами долларов. В последние 3-5 лет наблюдается увеличения числа вредоносных программ и атак с их стороны, а также сумм понесенных компаниями потерь.

Дополнительная опасность в том, что помимо компьютеров пользователей и серверов, сейчас заражению подвергаются и другие элементы сетевой инфраструктуры:

* Коммутаторы и маршрутизаторы;
* Мобильные устройства для доступа в сеть – компьютеры, планшеты;
* Элементы «умного дома».

Наибольший ущерб причиняют вирусы, которые шифруют данные на компьютере пользователя и требуют от него денежного перевода за расшифровку.

**4)** Действия правоохранительных органов

В ходе расследования уголовных дел и при проведении некоторых видов проверок представители контролирующих и правоохранительных органов могут изымать компьютерную технику и документы, в том числе с конфиденциальной информацией.

Это приводит сразу к двум негативным последствиям:

* Из-за изъятия компьютеров и серверного оборудования деятельность компании может полностью прекратиться;
* Информация с изъятых носителей и документов может распространиться далее, несмотря на ответственность работников следствия.

Ущерб, причиняемый утечкой информации, невозможно спрогнозировать заранее. Он может выражаться в незначительной сумме, но в некоторых случаях приводит к полной неспособности компании заниматься хозяйственной деятельностью.

**1.3 Разработка мер защиты**

На сегодняшний день информационная безопасность туристической фирмы требует более пристального внимания со стороны руководства и грамотной программы по обеспечению информационной безопасности фирмы, потому что появилось достаточно много конкурентов, которые вряд ли упустят возможность воспользоваться, например, клиентской базой.

Для того, чтобы оградить себя от утечки конфиденциальной информации, турфирма может осуществить следующую политику информационной безопасности:

1) установка на всех компьютерах антивирусного программного обеспечения и регулярное его обновление;

2) использование межсетевого экрана - программного или аппаратного маршрутизатора, который не пропускает наружу внутренние пакеты локальной сети предприятия и блокирует доступ к ней чужих компьютеров;

3) защита электронной почты (поставлен антивирус на корпоративный сервер электронной почты);

4) использование Proxy-сервера. Во-первых, это позволит незначительно сократить интернет-трафик. Во-вторых, это позволит скрыть от посторонних глаз внутренние имена и адреса компьютеров. И, в-третьих, это позволит выявлять нарушителей, подключившихся к сети предприятия с целью получения доступа в Интернет;

К сожалению, предоставленные средства не могут обеспечить информационную безопасность в полной мере, межсетевой экран не в состоянии решить все проблемы безопасности корпоративной сети, а также существуют угрозы безопасности, от которых межсетевые экраны не могут защитить. Прокси-сервер уменьшает скорость передачи данных.

На сегодняшний день существует большой арсенал методов обеспечения информационной безопасности, предлагается осуществить следующие действия:

1) установить средства идентификации и аутентификации пользователей (так называемый комплекс 3А);

2) установить средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;

3)  установить средства восстановления системы защиты информации;

4) обеспечить физическую охрану средств вычислительной техники и магнитных носителей;

5)  установить аппарат для уничтожения ненужных документов.

«Комплекс 3А» включает аутентификацию (или идентификацию), авторизацию и администрирование.

Идентификация и авторизация - это ключевые элементы информационной безопасности. При попытке доступа к информационным активам функция идентификации дает ответ на вопрос: «Кто вы?» и «Где вы?», а также являетесь ли вы авторизованным пользователем сети.

Функция авторизации отвечает за возможность доступа конкретного пользователя к различным ресурсам.

Функция администрирования заключается в наделении пользователя определенными идентификационными особенностями в рамках данной сети и определении объема допустимых для него действий.

Системы шифрования позволяют минимизировать потери в случае несанкционированного доступа к данным, хранящимся на жестком диске или ином носителе, а также перехвата информации при ее пересылке по электронной почте или передаче по сетевым протоколам.

Задача данного средства защиты – обеспечение конфиденциальности. Основные требования, предъявляемые к системам шифрования – высокий уровень крипто стойкости и легальность использования.

Описанные способы обеспечения информации предприятия являются мало затратными и достаточно эффективными, в целях обеспечения безопасности предприятия от множества угроз информационной безопасности как извне, так и изнутри.

Хотя существуют и другие способы, вроде тотальной слежки за сотрудниками, их эффективность значительно ниже и не попадает под категорию простых средств. Кроме того, не стоит забывать, что обеспечение информационной безопасности не должно наносить вред деятельности предприятия или создавать помехи для работы сотрудников, ведь, в конечном счёте, любые бизнес-процессы предприятия должны быть направлены на обеспечение основной деятельности, а не вспомогательных служб.

**Вывод**

Политика информационной безопасности — это набор требований, правил, ограничений и рекомендаций, регламентирующих порядок информационной деятельности в организации, направленных на достижение и поддержание состояния информационной безопасности организации.

Защита информации как некогда актуальна на сегодняшний момент. Мы живем в информационном обществе и поглощаем её ежедневно. Информация порой становится дороже самих материальных благ. Соответственно возникает необходимость в защите.

К решению этого вопроса необходимо подходить комплексно и с привлечением сторонних специалистов. Только такой подход позволит предотвратить утечку данных, а не бороться с ее последствиями.

**Практическое задание № 3**

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

Цель: Овладение навыками настройки и использования Брандмауэра Windows.

**Теоретическое введение**

Брандмауэр (Межсетевой экран) - это аппаратный или программный комплекс, позволяющий проверять (фильтровать) входные и выходные потоки данных, проходящие через интернет или сеть.

Межсетевой экран является одним из важнейших средств защиты, осуществляя надежную аутентификацию пользователей и защиту от несанкционированного доступа.

**Создание правила по ограничению доступа программ к сети**

При создании правила указывается какое именно действие вы хотите применить. В данном случае необходимо блокировать подключение (рис. 1).

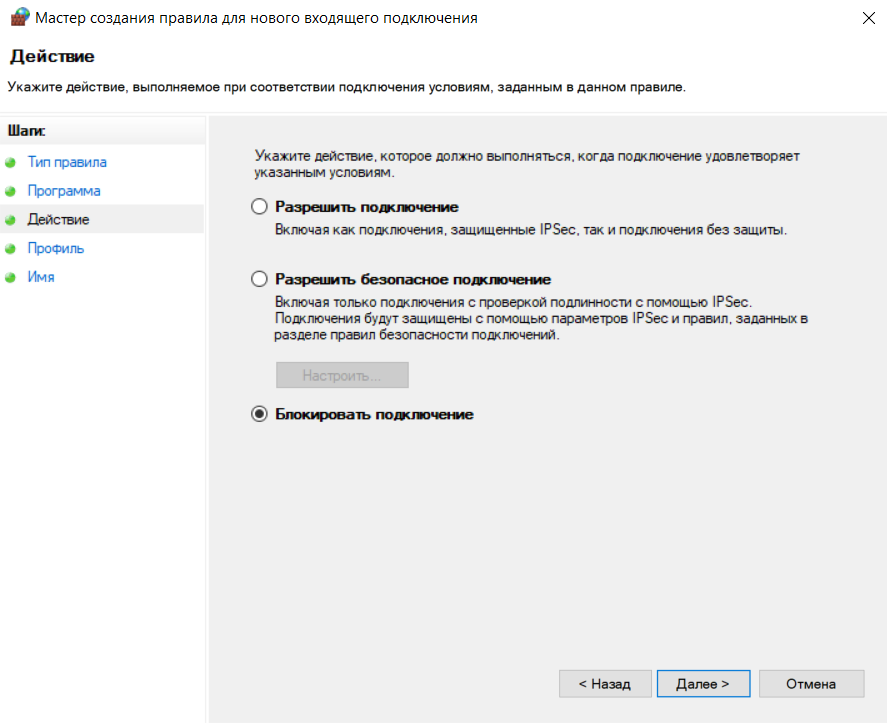


Рисунок 1–Выбор действия

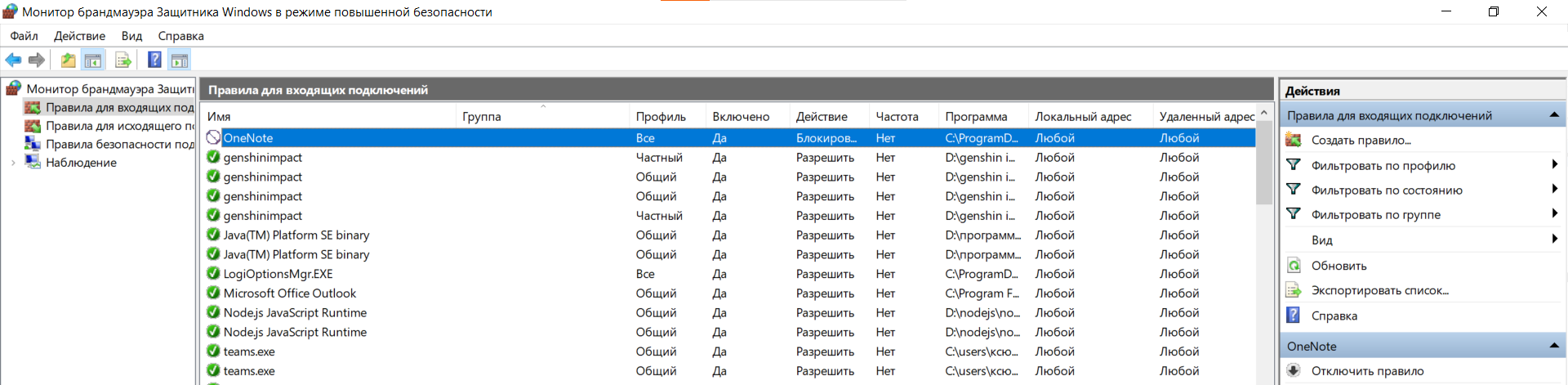


Рисунок 2 – Созданное правило

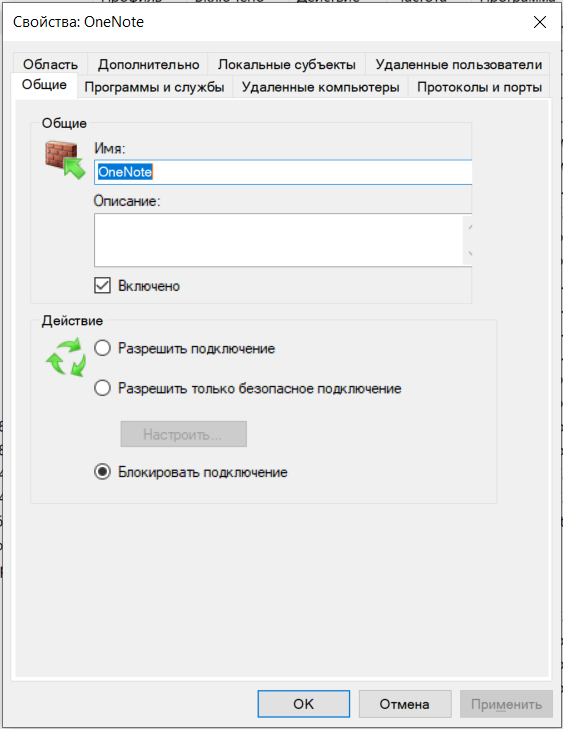


Рисунок 3– Свойства правила

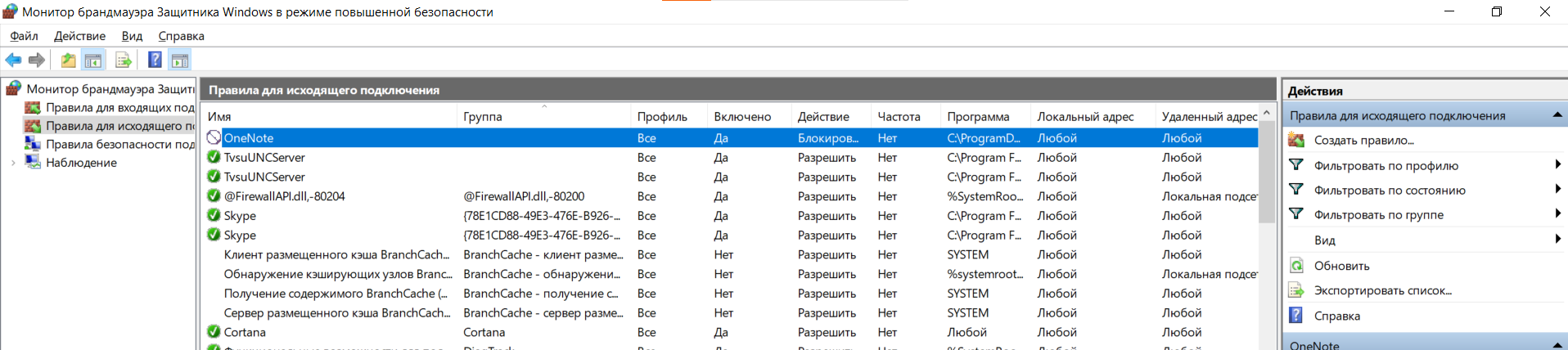


Рисунок 4 – Созданное правило

Запуск программы через командную строку:

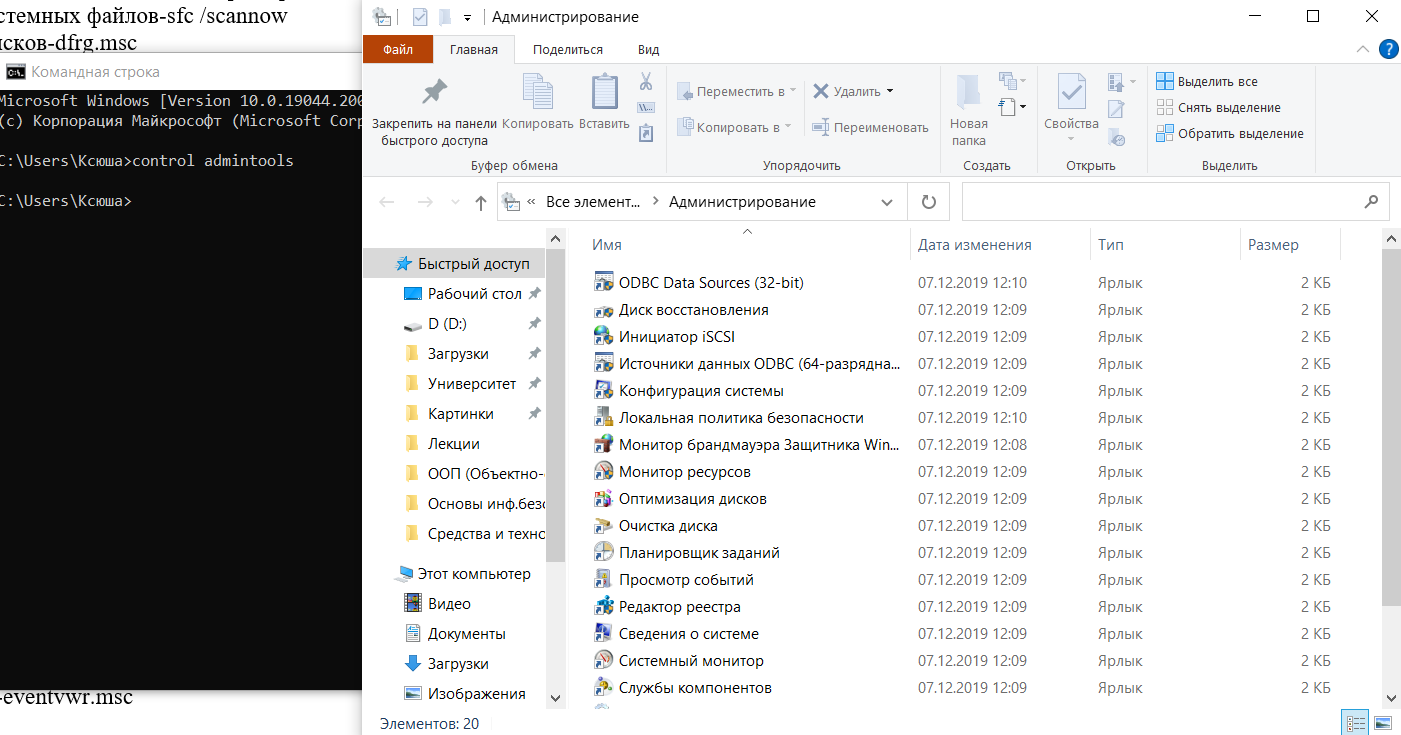


Рисунок 5 – Команда admintools (администрирование)

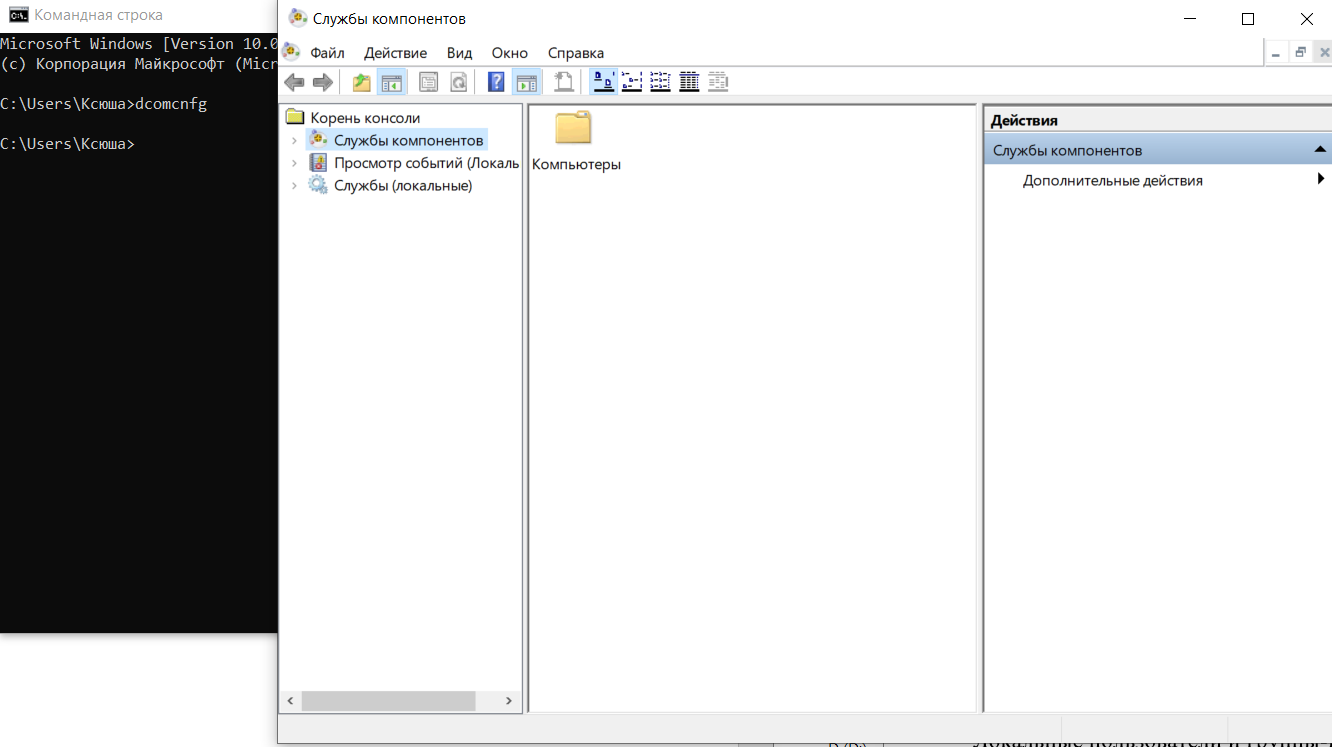


Рисунок 6 – Команда dcomcnfg (консоль управления)

**Практическое задание №4.1**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами симметричного шифрования.

**Теоретическое введение**

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

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

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.

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.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу

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.



В полиалфавитных подстановках для замены некоторого символа исходного сообщения в каждом случае его появления последовательно используются различные символы из некоторого набора.

**Задание к выполнению**

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.

Шифр Цезаря:

Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Следовательно, так как номер моего варианта равен 12, значит и сдвиг будет на 12 элементов.

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

Рисунок 7 – Таблица шифрозамен для шифра Цезаря

Зашифрованное сообщение – Цъьрчъ Цэрщфк Лчрцэлщпьънщл (Корело Ксения Александровна)

Шифр Трисемуса:

В таблицу сначала вписывается по строкам ключевое слово, причем повторяющиеся буквы отбрасываются. Затем эта таблица дополняется не вошедшими в нее буквами алфавита по порядку. Данная таблица имеет размер 8×4. Ключевое слово – Защита

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

Рисунок 8 – Таблица шифрозамен для шифра Трисемуса

Зашифрованное сообщение – Оухлпу Оцлсги Бплоцбскхужсб (Корело Ксения Александровна)

Шифр Плейфейра:

Структура шифрующей таблицы системы Плейфейра полностью аналогична структуре шифрующей таблицы Трисемуса. Поэтому воспользуемся таблицей из предыдущего задания.

Открытый текст исходного сообщения разбивается на пары букв (биграммы). Текст должен иметь четное количество букв и в нем не должно быть биграмм, содержащих две одинаковые буквы.

Следовательно, сообщение будет иметь вид: ко ре ло кс ен ия ал ек са нд ро вн

Зашифрованное сообщение – оу жп кп но йл ги бп дл ип йк сп гм

Шифр Вижинера:

Шифр Виженера — это последовательность шифров Цезаря с различными значениями сдвига.

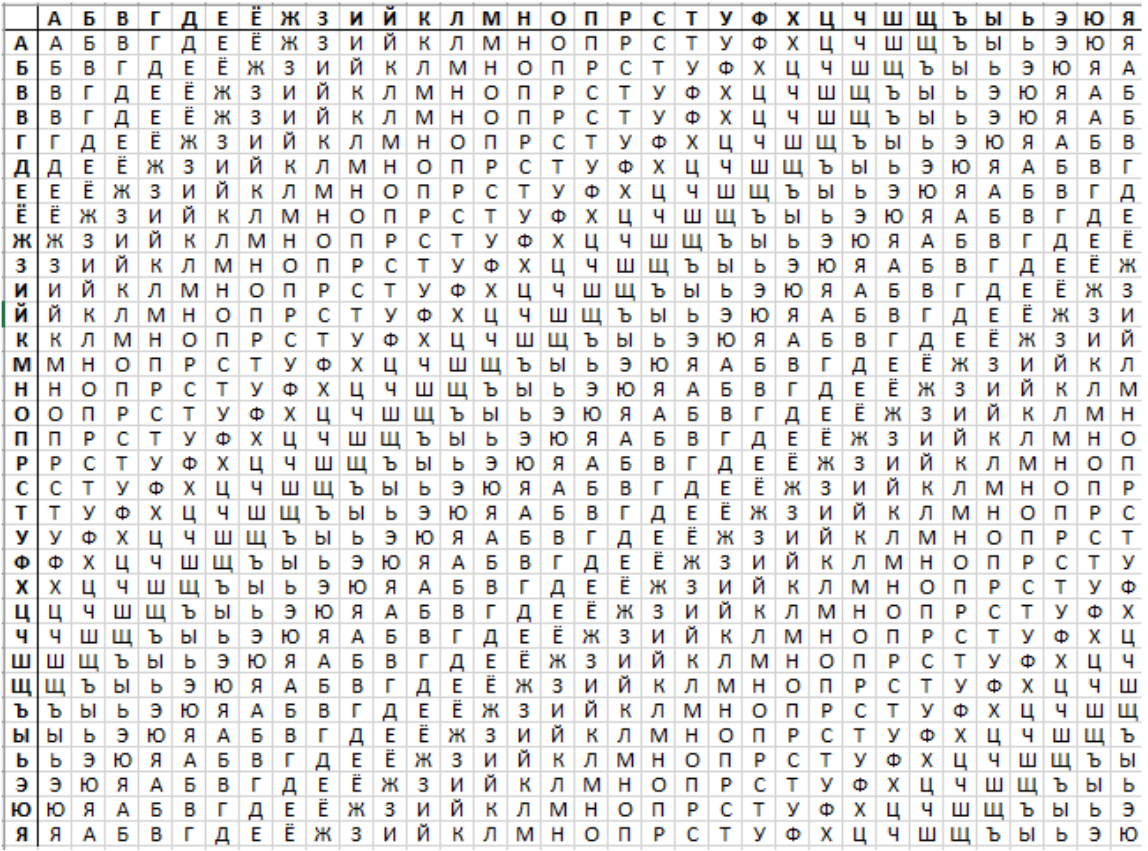


Рисунок 8 – Таблица Виженера

Чтобы зашифровать текст необходимо записать ключевое слово «Защита» циклически до тех пор, пока его длина не будет соответствовать длине исходного текста.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| К | О | Р | Е | Л | О | К | С | Е | Н | И | Я | А | Л | Е | К | С | А | Н | Д | Р | О | В | Н | А |
| З | А | Щ | И | Т | А | З | А | Щ | И | Т | А | З | А | Щ | И | Т | А | З | А | Щ | И | Т | А | З |
| Т | О | Й | Н | Ю | О | Т | С | Ю | Ц | Ы | Я | З | Л | Ю | У | Д | А | Х | Д | Й | Ч | Ф | Н | З |

2) Расшифровать следующие сообщения:

|  |  |  |
| --- | --- | --- |
| 12. | **нотеч\_е\_ \_кем\_кчалемре,осеал\_втссоаеотив\_к\_** | Расшифровать с помощью **Метода простой перестановки Таблица 6х7** |

Расшифровка:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| н | о | т | е | ч |  |
| е |  |  | к | е | м |
|  | к | ч | а | л | е |
| м | р | е | , | о | с |
| е | а | л |  | в | т |
| с | с | о | а | е | о |
| т | и | в |  | к |  |

Расшифрованный текст – Не место красит человека, а человек место.

**Практическое задание №4.2**

**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.

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

# **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 

# **Реализация элементов схемы шифрования Дифи-Хеллмана**

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.

**Практическое занятие №5**

**Практическое задание № 5**

**Тема «Криптографическая защита информации»**

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

**Теоретические сведения:**

ЭЦП (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").

Разновидности ЭЦП

Кроме классической схемы ЭЦП различают еще несколько специальных:

• схема "конфиденциальной" (не отвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;

• схема подписи "вслепую" ("затемненной" подписи) - отправитель не знает подписанного им сообщения;

• схема "мульти подписи" - 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;

**Практические задания:**

1) последовательность выполнения процедур генерации и проверки ЭЦП:

При создании цифровой подписи по классической схеме отправитель:

Генерация ЭЦП:

* применяем к исходному сообщению хеш-функцию и получаем хеш-образ сообщения;
* вычисляем цифровую подпись по хеш-образу с использованием своего закрытого ключа;

Проверка ЭЦП:

* Применяем к полученному сообщению хеш-функцию и получаем хеш-образ сообщения;
* расшифровываем хеш-образ из цифровой подписи с использованием открытого ключа отправителя;
* проверяем соответствие хеш-образов и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

2) При создании цифровой подписи по классической схеме отправитель:

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

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

* применяет к полученному сообщению хеш-функцию и получает хеш-образ сообщения;
* расшифровывает хеш-образ из цифровой подписи с использованием открытого ключа отправителя;
* проверяет соответствие хеш-образов и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

3) Схема протокола ЭЦП на основе алгоритма RSA

На первом этапе создания электронной подписи с помощью алгоритма RSA генерируются открытый и секретный ключи по следующему алгоритму. Сначала выбираются два больших простых числа p и q и вычисляется их произведение n = p∗q, после чего, с помощью функции Эйлера для числа n (ϕ(n) = (p − 1) ∗ (q − 1)), вычисляются секретная и открытая экспоненты, являющиеся частями секретного и открытого ключей соответственно.

Для вычисления открытой экспоненты необходимо выбрать число e, удовлетворяющее неравенствам 1 <e <ϕ(n) и взаимно простое с ϕ(n). Далее мы вычисляем число d, обратное к числу e по модулю ϕ(n), то есть удовлетворяющее уравнению d∗e ≡ 1(modϕ(n)). Полученное число d и является секретной экспонентой. Теперь в качестве открытого ключа мы берем (n, e), а в качестве секретного ключа: (n, d).

Криптосистема RSA позволяет шифровать сообщения, имеющие вид целого числа, большего 0, но меньшего n−1. Для него создается подпись с использованием секретного ключа (n, d) по формуле s = m^d (mod n). В результате, вместо нашего сообщения m, передается сообщение с подписью (m, s). При приеме сообщения с подписью (m, s) для проверки истинности содержания и автора сначала с помощью открытого ключа (n, e) вычисляется прообраз m′ по формуле m′ = s^e (mod n). И во конце истинность проверяется путем сравнения m и m′. Именно здесь используется сложность задачи факторизации, а именно, если приниматель не знает открытую экспоненту, ему придется вычислять значение ϕ(n), что требует знания разложения числа n на простые множители.

|  |
| --- |
| **Практическое задание № 6** |
| **Тема «Теория чисел»** |
| Цель**:**  получение основных сведений из курса теории чисел |
| **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).*

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

**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.

*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: .

*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.

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 .*

**Задание для выполнения:**

1. Найти канонические разложения чисел а и b.
2. Найти НОД  пользуясь:

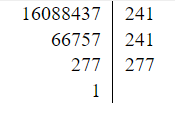
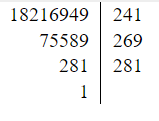
a) алгоритмом Евклида,

б) разложением чисел на простые множители.

1. С помощью расширенного алгоритма Евклида найти целые u, v, удовлетворяющие соотношению Безу: au + bv = НОД .
2. Найти остаток от деления данного числа на простое.

|  |  |
| --- | --- |
|  | 1-3. *а* = 160884371, *b* = 18216949.  4. Найти остаток от деления  на 16. |

№1, а) б)

№2, НОД (а, b)

А) Алгоритм Евклида

18216949 : 16088437 = 1 (остаток 2128512),

16088437 : 2128512 = 7 (остаток 1188853),

2128512 : 1188853 = 1 (остаток 939659),

1188853 : 939659 = 1 (остаток 249194),

939659 : 249194 = 3 (остаток 192077),

249194 : 192077 = 1 (остаток 57117),

192077 : 57117 = 3 (остаток 20726),

57117 : 20726 = 2 (остаток 15665),

20726 : 15665 = 1 (остаток 5061),

15665 : 5061 = 3 (остаток 482),

5061 : 482 = 10 (остаток 241),

482 : 241 = 2 (остаток 0),

НОД (16088437; 18216949) = 241

Б) Разложение на простые множители

16088437 = 241•241•277  
18216949 = 241•269•281

Общий множитель 241, следовательно НОД(16088437; 18216949) = 241

№3, С помощью расширенного алгоритма Евклида найти целые числа *u*,*v*, удовлетворяющие соотношению Безу: 

18216949 : 16088437 = -1 (остаток 2128512),

…

Коэффициент перед большим числом:

y = 31829

Коэффициент перед меньшим числом:

u = -36040

16088437 \*-36040+18216949 \*31829= 241

№4 Найти остаток от деления  на 16

1995:16 = 124 остаток 11

1995^2:16 = 248751 остаток 9

1995^3: 16 = 496259367 остаток 3

1995^4: 16 = 990037437539 остаток 1

1995^5: 16 остаток 11

1995^6: 16 остаток 9

1995^6: 16 остаток 3

1995^6: 16 остаток 1

1995^6: 16 остаток 11

1995^6: 16 остаток 9

1995^6: 16 остаток 3

1995^6: 16 остаток 1,

Следовательно, остаток от деления равен 1

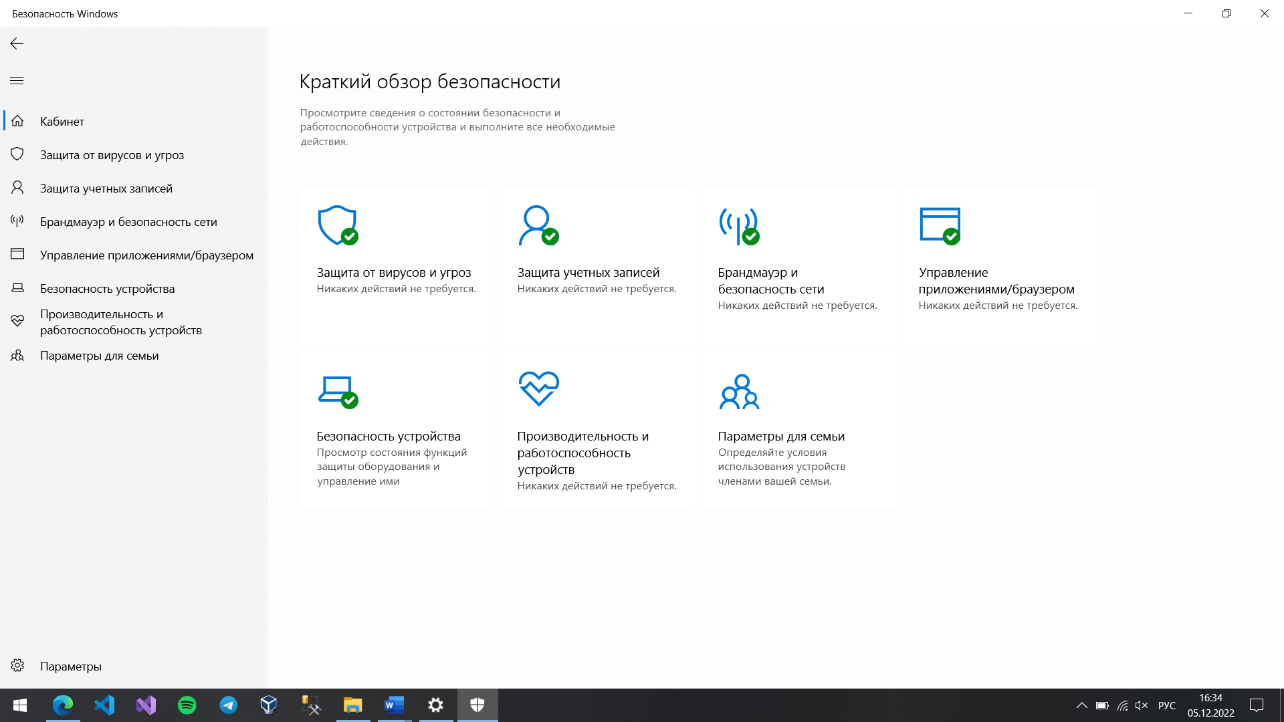
**Практическое задание № 7**

**Тема «**Настройка антивирусов**»**

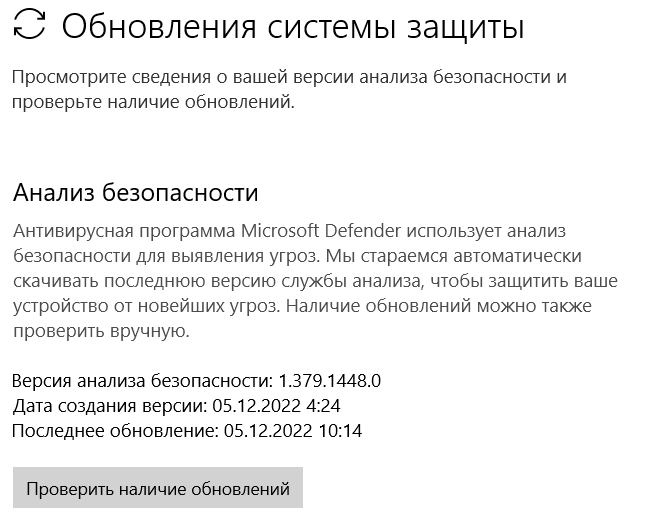
Цель: Овладение навыками настройки и использования различных антивирусов.

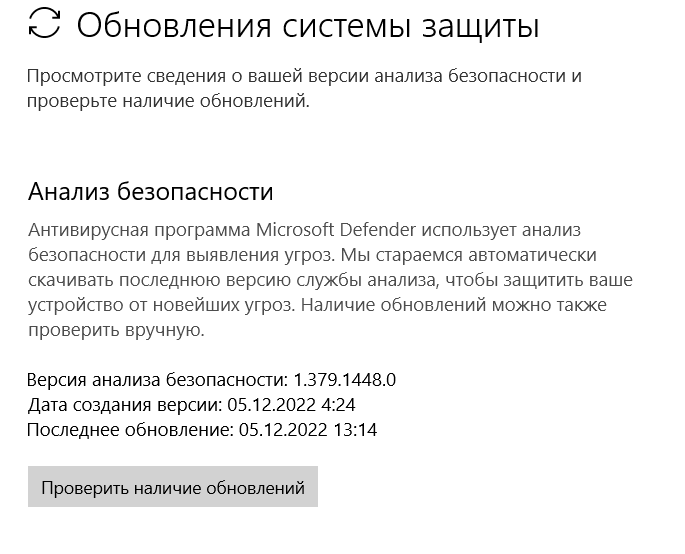
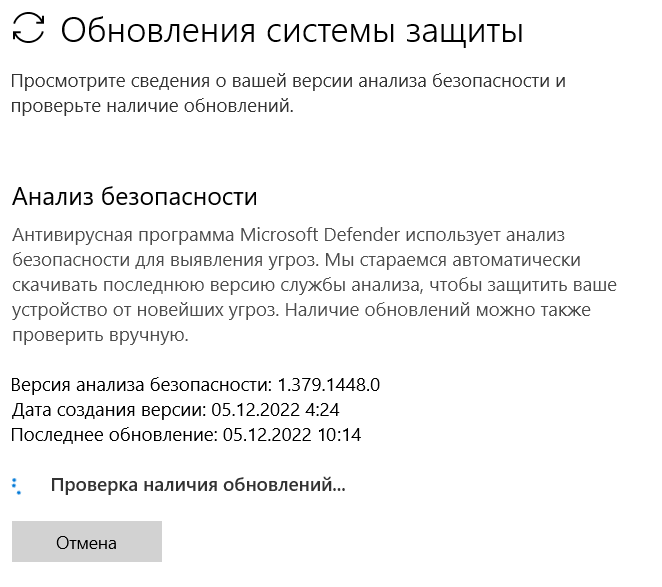
**Задание к выполнению**

1. Установить и настроить антивирусную программу.

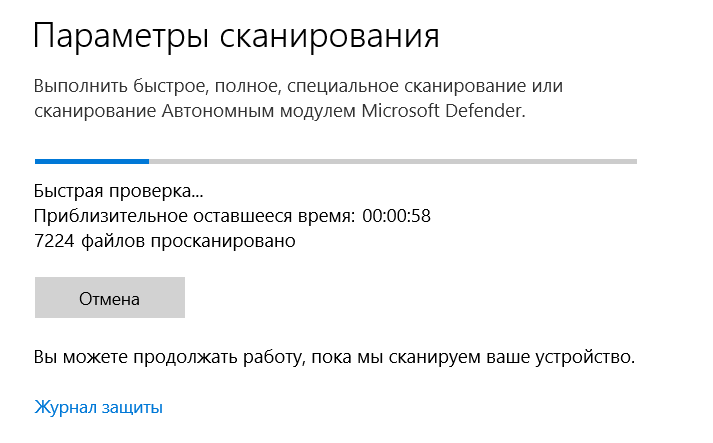


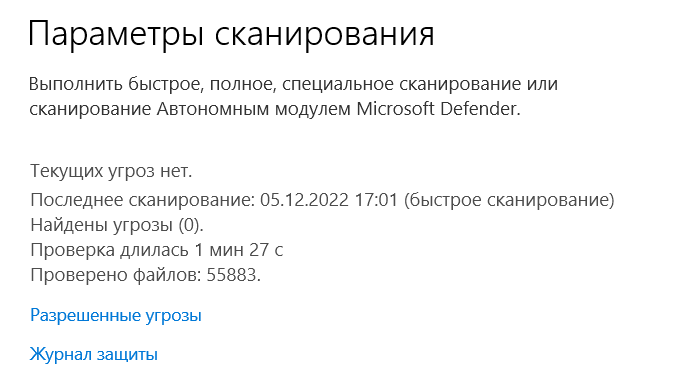
2. Обновить базу данных сигнатур вирусов.





3. Выполнить сканирование дисков.





|  |
| --- |
| **Практическое занятие №8** |
| **Тема «Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование с использованием библиотеки** [**System.Security.Cryptography**](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography)**»** |
| Цель: Изучить модель криптографии .NET Framework, основные классы и структуры данных, разработать приложение для шифрования файлов использующих симметричные и ассиметричные алгоритмы шифрования |

**Задание для выполнения:**

1. Ознакомиться с созданием криптографического приложения;
2. Выполнить шифрование, дешифрование и хеширование своей фамилии по указанным алгоритмам. Используя функции работы с файлами сохранить ключи шифрования, результаты шифрования и хеширования.
3. Для выше указанных алгоритмов используя Hex-редактор продемонстрировать ключи шифрования, зашифрованные и захешированные данные.

|  |  |
| --- | --- |
| RSA (640bit) | SHA384 |

**Практическое задание № 9**

**Тема «Изучение стандартных средств для реализации симметричного и ассиметричного шифрование с использованием SubtleCrypto в js»**

Цель: Изучить интерфейс **SubtleCrypto**, Основные классы и структуры данных, разработать приложение для шифрования файлов использующих симметричные и ассиметричные алгоритмы шифрования

**Задание к выполнению:**

1. Ознакомиться с созданием криптографического приложения
2. Выполнить генерацию и вывод в консоль случайный чисел.
3. Выполнить шифрование, дешифрование и хеширование своей фамилии по указанным алгоритмам.
4. Продемонстрировать упаковку и распаковку ключа, полученного в предыдущем задании используя алгоритм AES-KW.
5. Выполнить процедуру подписи сообщения и проверку подлинности с использованием RSA-PSS или ECDSA на выбор.

|  |  |
| --- | --- |
| AES-GCM | SHA-256 |