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: Лобанов В.Д.

ФИТ 2 курс 3 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* |
| 11 | 19000 | 17000 | 4 | 800 |

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 занятие №2**

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

Цель: разработать проект политики информационной безопасности бизнес-компании.

# **Введение**

Что такое информационная безопасность?

Информационная безопасность — это различные меры по защите информации от посторонних лиц. В доцифровую эпоху для защиты информации люди запирали важные документы в сейфы, нанимали охранников и шифровали свои сообщения на бумаге. Меры по обеспечению информационной безопасности:

* антивирусная защита
* аутентификация пользователей
* Криптографическая защита данных (шифрование)
* Межсетевые экраны (контроль и фильтрация веб-трафика)
* Резервное копирование
* Специализированные системы обнаружение вторжений

Сейчас чаще защищают не бумажную, а цифровую информацию, но меры, по сути, остались теми же: специалисты по информационной безопасности создают защищенные пространства (виртуальные «сейфы»), устанавливают защитное ПО вроде антивирусов («нанимают охранников») и используют криптографические методы для шифрования цифровой информации.

Однако цифровую информацию тоже нужно защищать не только виртуально, но и физически. Антивирус не поможет, если посторонний похитит сам сервер с важными данными. Поэтому их ставят в охраняемые помещения.

За что отвечает информационная безопасность

Она отвечает за три вещи: конфиденциальность, целостность и доступность информации. В концепции информационной безопасности их называют принципами информационной безопасности.

Конфиденциальность означает, что доступ к информации есть только у того, кто имеет на это право. Например, ваш пароль от электронной почты знаете только вы, и только вы можете читать свои письма. Если кто-то узнает пароль или другим способом получит доступ в почтовый ящик, конфиденциальность будет нарушена.

Целостность означает, что информация сохраняется в полном объеме и не изменяется без ведома владельца. Например, на вашей электронной почте хранятся письма. Если злоумышленник удалит некоторые или изменит текст отдельных писем, то это нарушит целостность.

Доступность означает, что тот, кто имеет право на доступ к информации, может ее получить. Например, вы в любой момент можете войти в свою электронную почту. Если хакеры атакуют серверы, почта будет недоступна, это нарушит доступность.

Какая бывает информация и как ее защищают

Информация бывает общедоступная и конфиденциальная. К общедоступной имеет доступ любой человек, к конфиденциальной — только отдельные лица.

Может показаться, что защищать общедоступную информацию не надо. Но на общедоступную информацию не распространяется только принцип конфиденциальности — она должна оставаться целостности и доступной. Поэтому информационная безопасность занимается и общедоступной информацией.

Например, возьмем интернет-магазин. Карточки товаров, статьи в блоге, контакты продавца — все это общедоступная информация, ее может просматривать любой. Но интернет-магазин все равно нужно защищать, чтобы никто не нарушил его работу, например, не изменил важную информацию в карточках товаров или не «уронил» его сайт.

Главная задача информационной безопасности в IT и не только — защита конфиденциальной информации. Если доступ к ней получит посторонний, это приведет к неприятным последствиям: краже денег, потере прибыли компании, нарушению конституционных прав человека и другим неприятностям.

Основные виды конфиденциальной информации

Персональные данные. Информация о конкретном человеке: ФИО, паспортные данные, номер телефона, физиологические особенности, семейное положение и другие данные. В России действует 152-ФЗ — закон, который обязывает охранять эту информацию. Тот, кто работает с персональными данными, обязан защищать их и не передавать третьим лицам. Информация о клиентах и сотрудниках относится как раз к персональным данным.

Коммерческая тайна. Внутренняя информация о работе компании: технологиях, методах управления, клиентской базе. Если эти данные станут известны посторонним, компания может потерять прибыль.

Компания сама решает, что считать коммерческой тайной, а что выставлять на всеобщее обозрение. При этом не вся информация может быть коммерческой тайной — например, нельзя скрывать имена учредителей юрлица, условия труда или факты нарушения законов. Подробнее о коммерческой тайне рассказывает закон 98-ФЗ.

Профессиональная тайна. Сюда относятся врачебная, нотариальная, адвокатская и другие виды тайны, относящиеся к профессиональной деятельности. С ней связано сразу несколько законов.

Служебная тайна. Информация, которая известна отдельным службам, например, налоговой или ЗАГСу. Эти данные обычно хранят государственные органы, они отвечают за их защиту и предоставляют только по запросу.

Государственная тайна. Сюда относят военные сведения, данные разведки, информацию о состоянии экономики, науки и техники государства, его внешней политики. Эти данные самые конфиденциальные — к безопасности информационных систем, в которых хранится такая информация, предъявляют самые строгие требования.

Если ваша компания хранит персональные данные, коммерческую или профессиональную тайну, то эти данные нужно защищать особым образом. Для этого необходимо ограничить доступ к ней посторонним лицам — установить уровни доступа и пароли, поставить защитное ПО, настроить шифрование.

**Структура риэлторской компании**

Организационная структура агентства недвижимости, определяет способ управления, который будет способствовать максимально эффективному ведению бизнеса и высоким показателям продаж у риэлтора агентства недвижимости.

Организационная структура агентства недвижимости оказывает непосредственное воздействие на отношения риэлтора с компанией и в конечном итоге положительно или отрицательно влияет на результаты его работы.

Часто встречаются риэлторы, которые могли бы работать более продуктивно, но агентство недвижимости не имеет эффективной организационной модели. В таких ситуациях часто считается, что проблема в риэлторе, но таким образом только демонстрируется неспособность к анализу.

Агентство недвижимости — это компания, которая устанавливает краткосрочные цели, а уже после их достижения может разнообразить свою область деятельности, потому что в недвижимости есть четкие ограничения, связанные областью деятельности предприятия.

Однако существуют несколько главных элементов, которые являются ключевыми практически для всех.

Чтобы лучше понимать взаимосвязи этих элементов и понимать, как функционирует агентство недвижимости, рассмотрим две области:

* Административное управление агентством недвижимости.
* Персонал агентства недвижимости.

## Административное управление работой агентства недвижимости.

Административное управление агентством недвижимости не следует путать с концепцией управления предприятием, оно должно быть связано с понятием бюрократии в организации как формы внутренней деятельности.

В организации должны быть четкие формальные правила для всех внутренних процессов. В связи с этим, при управлении внутренними процессами агентства недвижимости необходимо учитывать различные аспекты, которые, как иногда кажется, не сильно связаны:

* Функциональные области агентства недвижимости.
* Подтвержденные компетенции и обязанности.
* Эффективность управления и контроль производительности.
* Специализация риэлтора.
* Пирамида иерархии и лидерства.
* Людские ресурсы и межличностные отношения.
* Принятие решений и разрешение проблем.
* Внутренние и внешние связи агентства недвижимости.

Важным для агентства недвижимости является то, что такая форма внутреннего управления не станет ограничивающим фактором для риэлтора, и, следовательно, не сможет негативно сказаться на производительности труда всей компании.

Методы, используемые для таких целей агентством недвижимости, не только будут регулировать порядок работы и внутренние контакты, но также развивают внешние связи. Эта методика является результатом нескольких методов, реализованных в агентстве недвижимости, как в организации.

Когда области деятельности агентства недвижимости определены правильно, и когда каждый член организации имеет четкие полномочия, не нужно беспокоиться о многих проблемах, которые могут возникнуть, если в агентстве недвижимости нет согласованной работы и не определены точные полномочия его сотрудников.

В случае, если агентство недвижимости имеет четкое разделение на внутренние зоны, оно должно пойти на один шаг дальше для достижения максимального уровня производительности труда.

Определяющим фактором является то, что работники агентства недвижимости работают более эффективно одной командой, если им поставлены общие цели.

Ничего из описанного выше не может строиться без четко определенной иерархической пирамиды в организации, которая из-за особенностей малого и среднего агентства недвижимости, имеет в своей вершине собственника компании.

Когда у малого или среднего агентства недвижимости есть несколько партнеров, очень важно четко определить, кому из них достанется роль лидера; даже если агентство недвижимости имеет только одного владельца, он должен решить, насколько это будет эффективно, если он будет лидером.

Руководитель агентства недвижимости должен иметь определенные навыки для организации и поддержания работы его агентства, он всегда должен быть ориентирован на достижение целей, установленных заранее.

В то же время, руководитель агентства недвижимости должен отслеживать, оценивать, управлять, принимать решения и быть таким же членом команды.

Ценности компании должны быть отражены и в поведении сотрудников, и в поведении руководителя агентства недвижимости. Он — зеркало, где все члены организации должны находить отражение.

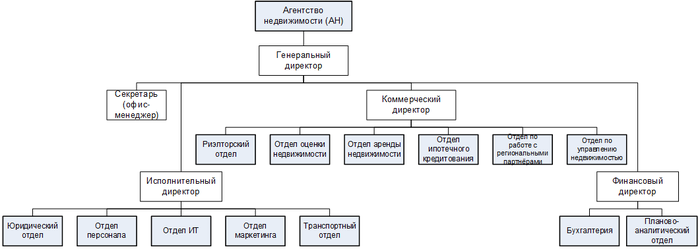
Команда агентства недвижимости должна состоять из всех членов организации без исключения, а их компетенции должны быть четко определены; остается актуальным умение вносить свой вклад согласно своим возможностям, в том числе знания и опыт, в работу команды на организационном уровне.

Лидер организации играет важную роль не только потому, что берет на себя руководство работой команды агентства недвижимости, но и потому, что должен создавать чувство принадлежности каждого члена к организации, а также несет ответственность за создание внутренних положительных связей.

Для формирования команды, как правило, агентству недвижимости требуется постоянный присмотр, следует содействовать организационными ценностями на внутреннем уровне и выработать стратегии, которые облегчат пребывание членов команды внутри компании.

Один из способов достижения наиболее эффективной и функциональной организационной структуры в агентстве недвижимости — через предварительное стратегическое планирование, ориентированное на достижение установленных целей.

Для этого внутреннее управление, организационное лидерство и работа в команде [агентства недвижимости](http://www.costainvest.com/ru/) являются определяющими элементами.



# **Оценка рисков**

1. Определить ценность информационных активов в денежном выражении.

2. Оценить в количественном выражении потенциальный ущерб от реализации каждой угрозы в отношении каждого информационного актива.

Следует получить ответы на вопросы «Какую часть от стоимости актива составит ущерб от реализации каждой угрозы?», «Какова стоимость ущерба в денежном выражении от единичного инцидента при реализации данной угрозы к данному активу?».

3. Определить вероятность реализации каждой из угроз ИБ.

Для этого можно использовать статистические данные, опросы сотрудников и заинтересованных лиц. В процессе определения вероятности рассчитать частоту возникновения инцидентов, связанных с реализацией рассматриваемой угрозы ИБ за контрольный период (например, за один год).

4. Определить общий потенциальный ущерб от каждой угрозы в отношении каждого актива за контрольный период (за один год).

Значение рассчитывается путем умножения разового ущерба от реализации угрозы на частоту реализации угрозы.

5. Провести анализ полученных данных по ущербу для каждой угрозы.

По каждой угрозе необходимо принять решение: принять риск, снизить риск либо перенести риск.

Принять риск — значит осознать его, смириться с его возможностью и продолжить действовать как прежде. Применимо для угроз с малым ущербом и малой вероятностью возникновения.

Снизить риск — значит ввести дополнительные меры и средства защиты, провести обучение персонала и т д. То есть провести намеренную работу по снижению риска. При этом необходимо произвести количественную оценку эффективности дополнительных мер и средств защиты. Все затраты, которые несет организация, начиная от закупки средств защиты до ввода в эксплуатацию (включая установку, настройку, обучение, сопровождение и проч.), не должны превышать размера ущерба от реализации угрозы.

Перенести риск — значит переложить последствия от реализации риска на третье лицо, например с помощью страхования.

В результате количественной оценки рисков должны быть определены:

ценность активов в денежном выражении;

полный список всех угроз ИБ с ущербом от разового инцидента по каждой угрозе;

-частота реализации каждой угрозы;

-потенциальный ущерб от каждой угрозы;

-рекомендуемые меры безопасности, контрмеры и действия по каждой угрозе. Основными объектами защиты в библиотеке являются:

- персонал (так как эти лица допущены к работе с охраняемой законом информацией (коммерческая тайна, персональные данные) либо имеют доступ в помещения, где эта информация обрабатывается).

- объекты информатизации - средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний, заседаний и переговоров с посетителями;

- коммерческая тайна (сведения о посетителях, месте их проживания, контактной информацией);

- персональные данные работников (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия, уровень квалификации, доход, наличие судимостей и некоторая другая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника).

- документированная информация, регламентирующая статус учреждения, права, обязанности и ответственность его работников (Устав, журнал регистрации, учредительный договор, положение о деятельности, положения о структурных подразделениях, должностные инструкции работников)

- материальные носители охраняемой законом информации (личные дела работников, личные дела посетителей, электронные базы данных работников и посетителей, бумажные носители и электронные варианты приказов, постановлений, планов, договоров, отчетов, составляющих коммерческую тайну)

- средства защиты информации (Интернет-шлюз, система сигнализации и др.)

- технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации (личные дела бывших клиентов)

# Предметом защиты информации в библиотеке являются носители информации, на которых зафиксированы, отображены защищаемые сведения:

# - Личные дела посетителей в бумажном и электронном (база данных посетителей) виде;

# - Личные дела работников в бумажном и электронном виде;

# - Приказы, постановления, положения, инструкции, соглашения и обязательства о неразглашении, распоряжения, договоры, планы, отчеты, ведомость ознакомления с Положением о конфиденциальной информации и другие документы, в бумажном и электронном виде.

# Документы, которые имеют конфиденциальный характер и требующие зашиты.

# **Разработка мер защиты**

В настоящее время человечество уверенно вступило в новую высокотехнологичную «информационную эру», характеризующуюся тотальным господством цифровых технологий, невероятно динамичным развитием информационно-коммуникационной сферы и всеобъемлющей информатизацией повседневной деятельности человека (компьютеры, мобильная связь, Интернет, социальные медиа, «умные» дома и города и пр.).

Однако развитие Интернета, открывшего для человечества невиданные ранее возможности в сфере информации и коммуникаций, сопровождается также невиданными ранее рисками, угрозами и вызовами. Основные из них – это появление информационного криминала (киберпреступности), противоправные действия по отношению к объектам информационной инфраструктуры, хакерство, информационный вандализм и терроризм на внутригосударственном и международном уровнях.

Таким образом, массовая цифровизация повлекла за собой начало так называемой «эпохи информационных войн» и появление новых техно биосоциальных угроз, на фоне чего все больше возрастает потребность в защите информации. Любая организация постоянно накапливает определенный объем всевозможной конфиденциальной информации – о своих продуктах, клиентах, сотрудниках, научных исследованиях и др. Попадание этих данных в руки конкурентов или киберпреступников может повлечь для организации и ее клиентов далекоидущие юридические последствия, а также финансовые и репутационные потери.

Риэлторскиесистемы вклю­чают в себя такие общие активы, как базы данных, веб-сайты, устройства и программные приложения, управляемые администраторами систем и сетей. Множество риэлторских организаций организовывают службу платных интерактивных услуг. Этот фактор способствует увеличению требований к безопас­ности. Ни риэлтор, ни клиент не заинтере­сованы в предоставлении «третьей» стороне лич­ных данных. Актуально обеспечение безопасности систем электронного документооборота, электронных платежных систем и личных данных сотрудников, и пользователей.

Риэлторские и другие учреждения подобного плана сталкиваются с большим количеством персональных данных как сотрудников, так и клиентов. Многие документы попадают в категорию коммерческой тайны. Поэтому информационная безопасность переходит на новый уровень.

Увеличение объема конфиденциальной инфор­мации и изменение целей и задач людей, зави­сящие от постоянно развивающихся информаци­онных и коммуникационных технологий, создают новые угрозы для научно-образовательных источ­ников. Это, в свою очередь, усложняет проблему построения единой модели защиты от информа­ционных угроз.

Риэлторские организации переходят на электронный документооборот, автоматизируется ведение электронного учета или личных дел клиентов. Нельзя сказать, что вопросом оптимизации отдела регистрации или безопасности баз данных заинтересовались в системе риэлторских только сейчас. Этот процесс был начат уже достаточно давно. С развитием информационных технологий ускорился и переход организаций на новый уровень обработки и хранения персональных данных.

Для организации эффективной защиты конфиденциальной информации необходимо разработать программу, которая должна позволить достигать следующие цели:

- обеспечить обращение сведений, содержащих различные виды тайн, в заданной сфере;

- предотвратить кражу и утечку, а также любую порчу конфиденциальной информации;

- документировать процесс защиты тайны, чтобы в случае попыток незаконного завладения любой нежелательной информацией для учреждения можно было защитить свои права юридически и наказать нарушителя.

Планируемые мероприятия должны:

- способствовать достижению определенных задач, соответствовать общему замыслу;

- являться оптимальными.

Не должны:

- противоречить законам, требованиям руководителя организации;

- дублировать другие действия.

Правовая защита - специальные правовые правила, процедуры и мероприятия, создаваемые в целях обеспечения информационной безопасности предприятия.

Уголовно-правовые нормы по своему содержанию являются, с одной стороны, запрещающими, то есть они под страхом применения мер уголовного наказания запрещают гражданам нарушать свои обязанности и совершать преступления, а с другой стороны, они обязывают соответствующие органы государства (КГБ, МВД, прокуратуру) привлечь лиц, виновных в совершении преступления, к уголовной ответственности.

Кроме того, нарушения режима секретности, правил сохранения тайны, не являющиеся преступлением, могут повлечь ответственность материального, дисциплинарного или административного характера в соответствии с действующими нормативными актами: отстранение от работы, связанной с секретами, или перевод на другую работу, менее оплачиваемую и тоже не связанную с засекреченной информацией.

Организационная защита - регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, использующей нанесение ущерба.

Организационную защиту обеспечивает:

- Организация режима охраны, работы с кадрами, документами;

- Использование технических средств безопасности;

- Использование информационно-аналитической работы по выявлению угроз.

Организационные меры по защите информации предусматривают, прежде всего, подбор и расстановку кадров, которые будут осуществлять мероприятия по защите информации, обучение сотрудников правилам защиты засекреченной информации, осуществление на практике принципов и методов защиты информации.

Инженерно-техническая защита - использование различных технических средств для обеспечения защиты конфиденциальной информации. Инженерно-техническая защита использует такие средства как:

- Физические - устройства, инженерные сооружения, организационные меры, исключающие или затрудняющие проникновение к источникам конфиденциальной информации (системы ограждения, системы контроля доступа, запирающие устройства и хранилища);

- Аппаратные - устройства, защищающие от утечки, разглашения и от технических средств промышленного шпионажа

- Программные средства.

# **Вывод**

Важно помнить, что прежде, чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот.

Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Опыт показывает, что для достижения удачных решений по защите информации кампаний необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. В общем случае технические меры безопасности составляют незначительную часть от общих мер защиты (правовых и организационных). Однако ни одну из них упускать нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведёт к нарушению защищённости.

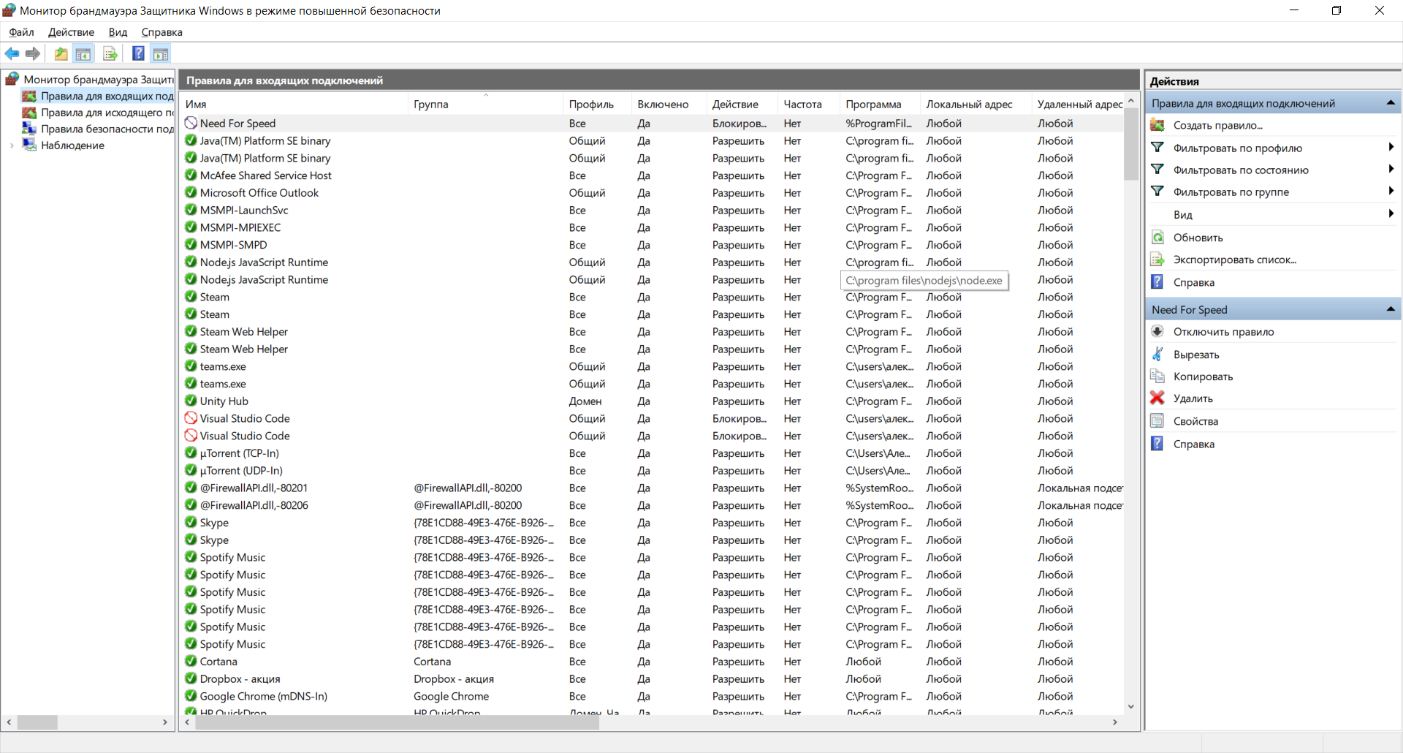
Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надёжность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надёжности технических средств обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надёжности технических средств.

**Практическое занятие №3**

**Тема «Настройка Брандмауэра Windows»**

1. Правила для входящих подключений

Правило на блокировку подключения:



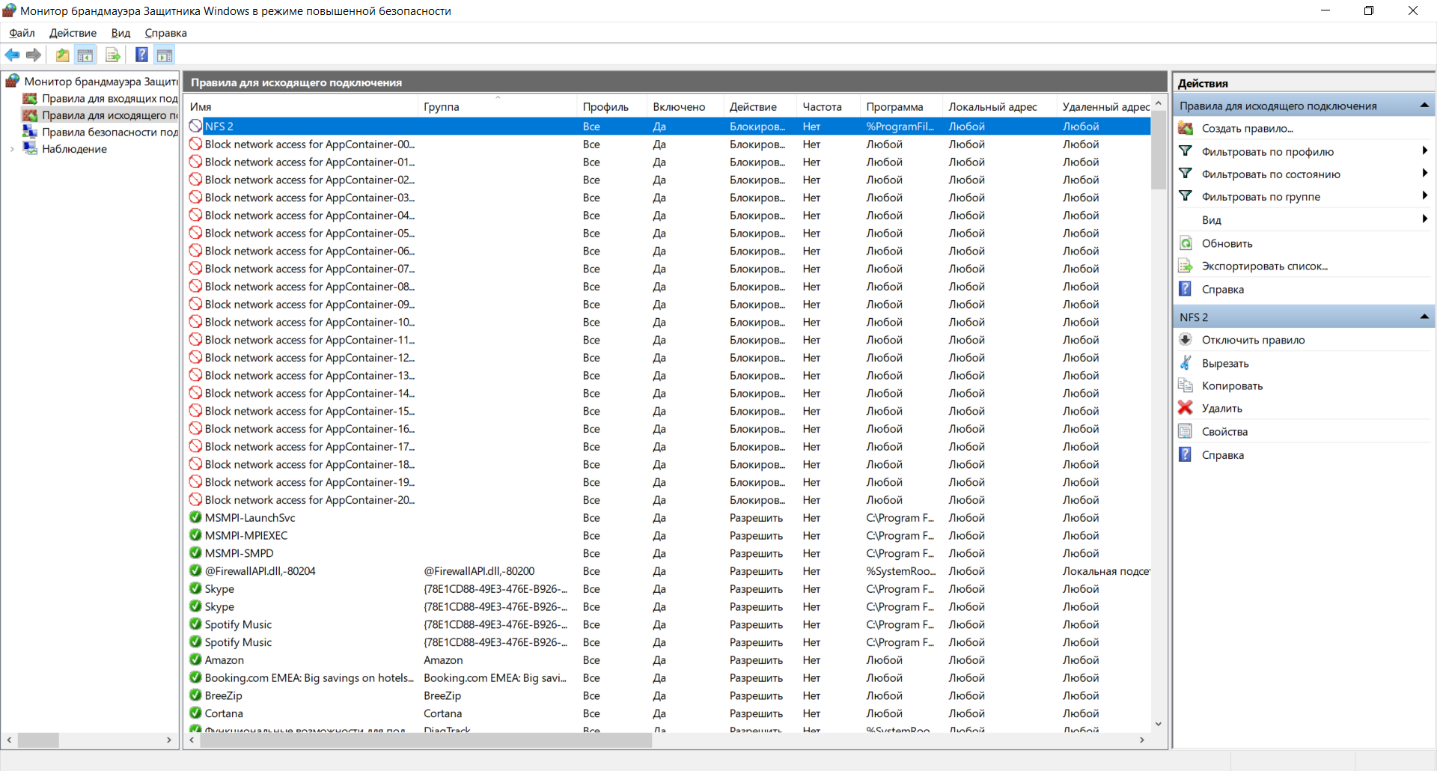
Правило на разрешение подключения:

Изображение выглядит как стол

Автоматически созданное описание

Правила для исходящих подключений

Правило на блокировку подключения:

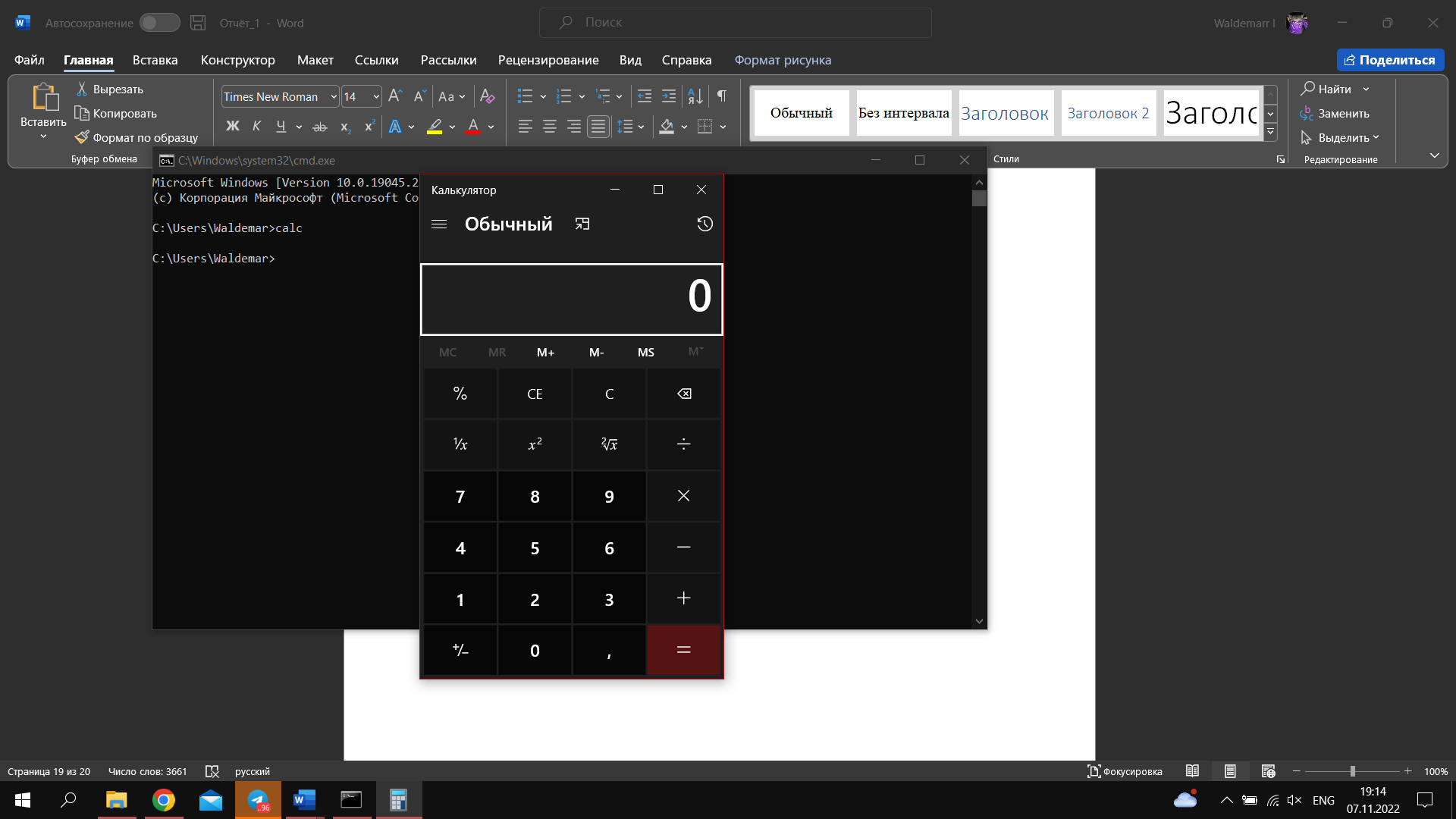


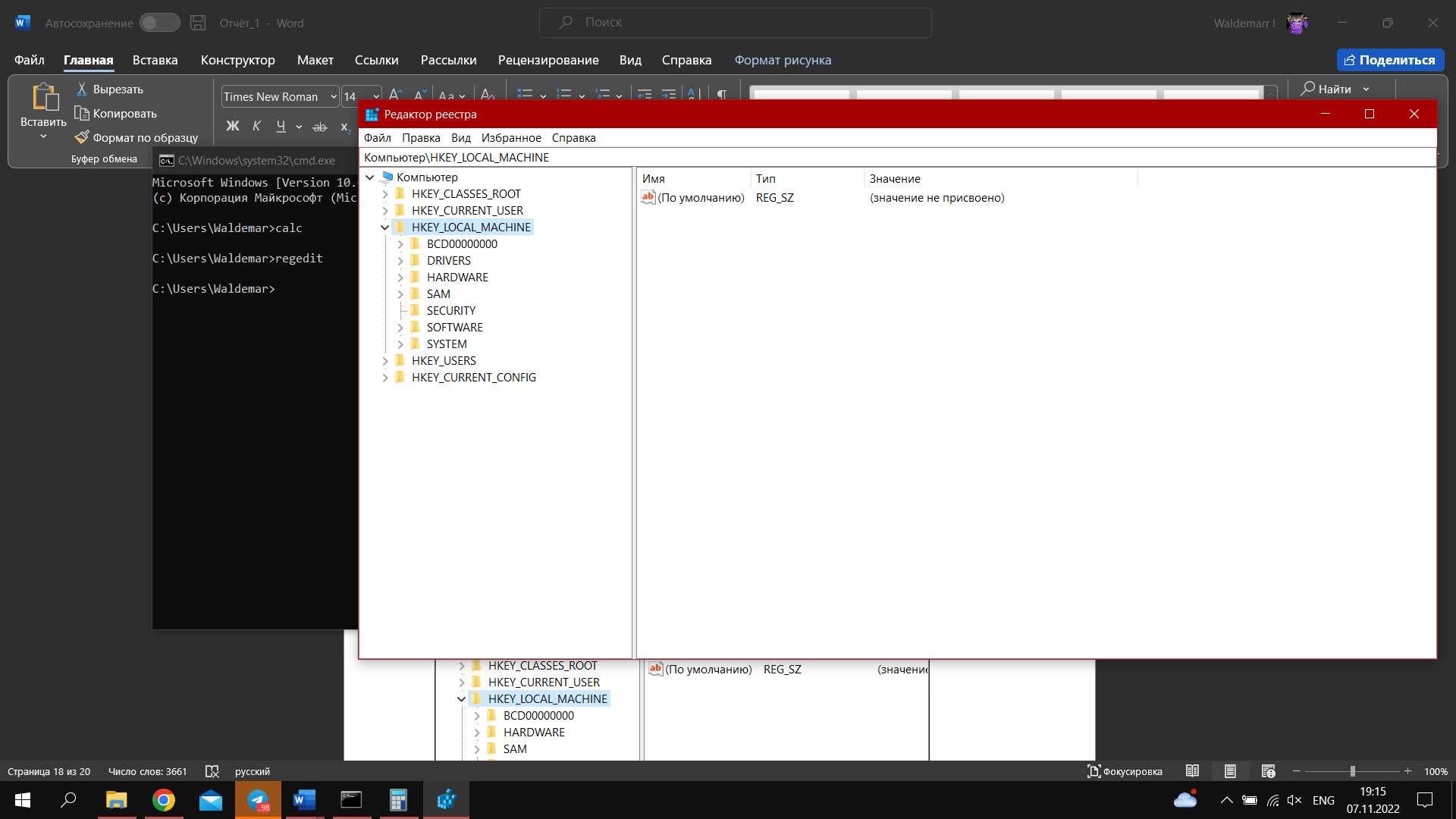
Правило на разрешение подключения:

Изображение выглядит как стол

Автоматически созданное описание

4. Действие команд





**Практическое занятие №4.1**

**Тема «Криптографическая защита информации»**

**Теоретическое введение**

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

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

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

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

В англоязычной литературе зашифрование / расшифрование – enciphering / deciphering.

Классификация алгоритмов шифрования

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

1.1. Потоковые:

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

· с конечным ключом;

· на основе генератора псевдослучайных чисел.

1.2. Блочные:

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

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

· моноалфавитные;

· полиалфавитные;

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

· Диффи-Хеллман DH (Diffie, Hellman);

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

· Эль-Гамаль (ElGamal).

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

Обмен информацией осуществляется в 3 этапа:

– отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);

– отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;

– получатель получает сообщение и расшифровывает его.

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

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

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

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

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

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

– моноалфавитные (код Цезаря);

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

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



Рисунок 5.1 – Принцип замены

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

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

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

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

Схема обмена информацией такова:

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

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

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

**Шифрование с использованием системы Цезаря:**

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки.

Математическая модель

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

http://kriptografea.narod.ru/13.png

http://kriptografea.narod.ru/14.png

где x — символ открытого текста

y — символ шифрованного текста

n — мощность алфавита (кол-во символов)

k — ключ.



Рисунок 5.2 – Алфавит

Пример:

Таблица 5.1 Шифр Цезаря

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Сообщение** | **Л** | **О** | **Б** | **A** | **Н** | **О** | **В** | **В** | **Л** | **А** | **Д** | **И** | **М** | **И** | **Р** |
| **Номер 1** | **13** | **16** | **2** | **1** | **15** | **16** | **3** | **3** | **13** | **1** | **5** | **10** | **14** | **10** | **18** |
| **Номер 1 +4** | **17** | **20** | **6** | **5** | **19** | **20** | **7** | **7** | **17** | **5** | **9** | **14** | **18** | **14** | **22** |
| **Шифр** | **П** | **Т** | **Е** | **Д** | **С** | **Т** | **Ё** | **Ё** | **П** | **Д** | **З** | **М** | **Р** | **М** | **Ф** |

Ответ: «Зфтлз Дриохин», ключ 4

**Шифрование с использованием системы Трисемуса:**

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.5.2 изображена таблица с ключевым словом «ЗАЩИТА».

Изображение выглядит как текст, кроссворд, электроника, телефон

Автоматически созданное описание

Рисунок 5.2 – Таблица шифрозамен для шифра Трисемуса с ключевым словом «ЗАЩИТА»

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

Например, исходное сообщение «ЛОБАНОВ ВЛАДИМИР», зашифрованное – «ПУЕБСУЖ ЖПБКГРГХ».

**Шифрование с использованием системы Виженера:**

В [шифре Цезаря](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F) каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 32 символа, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 32 различных шифра Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет вид:

ЛОБАНОВВЛАДИМИР

Человек, посылающий сообщение, записывает ключевое слово («ЗАЩИТА») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

ЗАЩИТАЗАЩИТАЗАЩ

Изображение выглядит как стол

Автоматически созданное описание

Рисунок 5.3 – Таблица Виженера для русского алфавита

Первый символ исходного текста Ш зашифрован последовательностью З, которая является первым символом ключа. Первый символ З шифрованного текста находится на пересечении строки З и столбца Ш в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста К получается на пересечении строки А и столбца К. Остальная часть исходного текста шифруется подобным способом.

*Исходный текст: ЛОБАНОВЛАДИМИР*

*Ключ: ЗАЩИТАЗАЩИТАЗАЩ*

*Зашифрованный текст:* дозчыоъвтчсиеич

**Шифрование с использованием системы Плейфера:**

Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4х8), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в русских текстах обычно «Е» и «Ё» объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом, составляет матрицу 4х8 и является ключом шифра.

Для того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Лобанов Владимир» становится «ЛО БА НО ВВ ЛА ДИ МИ Р», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем, руководствуясь следующими 4 правилами, зашифровываем пары символов исходного текста:

1. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «Х» используется «Q».

2. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

3. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

4. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «Х» (или «Q»), если они не несут смысла в исходном сообщении.

Пример: используем ключ «ЗАЩИТА», тогда матрица примет вид:

Изображение выглядит как текст, кроссворд, электроника, телефон

Автоматически созданное описание

Рисунок 5.4 – Таблица шифрозамен для шифра Плейфера с ключевым словом «ЗАЩИТА»

Зашифруем сообщение «ЛОБАНОВ ВЛАДИМИР»

ЛО БА НО ВВ ЛА ДИ МИ Р

1. Биграмма ЛО формирует прямоугольник, заменяем её на КП.  
   2. Биграмма БА расположена в одном столбце, заменяем её на ЕБ.  
   3. Биграмма НО формирует прямоугольник, заменяем её на СК.  
   4. Биграмма ВВ расположена в одном столбце, заменяем её на ЖЖ.  
   5. Биграмма ЛА расположена в одной строке, заменяем её на ПБ.  
   6. Биграмма ДИ формирует прямоугольник, заменяем её на ЙЗ.
2. Биграмма МИ формирует прямоугольник, заменяем её на НЩ
3. Биграмма РХ формирует прямоугольник, заменяем её на ХЪ  
   Получаем зашифрованный текст « КП ЕБ СК ЖЖ ПБ ЙЗ НЩ ХЪ»

Таким образом сообщение «ЛОБАНОВ ВЛАДИМИР» преобразуется в «КПЕБ СКЖЖ ПБЙЗНЩХЪ»

**ЗАДАНИЕ**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **гг\_ \_ ип-оомитрдр\_ос,яубогп\_**  **мбадираоитнла\_гноаавуоа** | | | | | | | | |
| г | г | \_ | \_ | и | п | - |
| о | о | м | и | т | р | д |
| р | \_ | о | с | , | я | у |
| б | о | г | п | \_ | м | б |
| а | д | и | р | а | о | и |
| т | н | л | а | \_ | г | н |
| о | а | а | в | у | о | а |

**Практическое задание №4.2**

**Тема «Криптографическая защита информации»**

**Теоретические сведения**

# Реализация элементов криптосистемы RSA

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

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

Весь алгоритм расписан в таблице:

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

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

## **Расшифрование**

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

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

При этом нетрудно проверить, что

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

и поэтому

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

Для практических вычислений больше подходит следующая формула:

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

## **Пример**

**Шифрование**

Допустим, что нужно зашифровать сообщение ~M=5.

Произведем генерацию ключей :

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

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

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

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

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

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

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

**Расшифрование**

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

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

Получили исходное сообщение ~M=5.

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

## **Генерация ключей**

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

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

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

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

1. Два участника обмена договариваются о двух числах. Один выбирает большое простое число, а другой – целое число, меньшее числа первого участника. Переговоры они могут вести открыто, и это никак не отразится на безопасности.
2. Каждый из двух участников, независимо друг от друга, генерирует другое число, которое они будут хранить в тайне. Эти числа выполняют роль секретного ключа. Далее в вычислениях используются секретный ключ и два предыдущих целых числа. Результат вычислений посылается участнику обмена, и он играет роль открытого ключа.
3. Участники обмена обмениваются открытыми ключами. Далее они, используя собственный секретный ключ и открытый ключ партнера, конфиденциально вычисляют ключ сессии. Каждый партер вычисляет один и тот же ключ сессии.
4. Ключ сессии может использоваться как секретный ключ для другого алгоритма шифрования, например DES. Никакое третье лицо, контролирующее обмен, не сможет вычислить ключ сессии, не зная один из секретных ключей.

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

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

**Пример**

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

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



**Практическое занятие №5**

**Тема «Криптографическая защита информации»**

ЭЦП — это реквизит [электронного документа](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82), полученный в результате криптографического преобразования [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) с использованием [закрытого ключа](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%B9_%D0%BA%D0%BB%D1%8E%D1%87) подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу [сертификата ключа подписи](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%82_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D0%BE%D0%B3%D0%BE_%D0%BA%D0%BB%D1%8E%D1%87%D0%B0) (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

Электронная цифровая подпись (ЭЦП) позволяет подтвердить авторство электронного документа (будь то реальное лицо или, например, аккаунт в [криптовалютной](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%8E%D1%82%D0%B0" \o "Криптовалюта) системе). Подпись связана как с автором, так и с самим документом с помощью криптографических методов и не может быть подделана с помощью обычного копирования.

**RSA** (аббревиатура от фамилий Rivest, Shamir и Adleman) — [криптографический алгоритм с открытым ключом](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC), основывающийся на [вычислительной сложности](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%BB%D0%BE%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D1%8C) [задачи факторизации](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%86%D0%B5%D0%BB%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB) больших [целых чисел](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE).

Криптосистема RSA стала первой системой, пригодной и для [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), и для [цифровой подписи](https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C). Алгоритм используется в большом числе криптографических приложений, включая [PGP](https://ru.wikipedia.org/wiki/PGP), [S/MIME](https://ru.wikipedia.org/wiki/S/MIME), [TLS](https://ru.wikipedia.org/wiki/TLS)/[SSL](https://ru.wikipedia.org/wiki/SSL), [IPSEC](https://ru.wikipedia.org/wiki/IPSEC)/[IKE](https://ru.wikipedia.org/wiki/IKE) и других[[3]](https://ru.wikipedia.org/wiki/RSA#cite_note-_7363aa0714d3f6f6-3).

**Разновидности ЭЦП**

Кроме классической схемы ЭЦП различают еще несколько специальных:

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

**Этап 1.** Выработка ключей (выполняет отправитель **А**) - см. практическую работу "Шифрование методом RSA".

**Этап 2.** Отправка сообщения и электронной подписи (выполняет отправитель **А**).

Отправка сообщения и ЭЦП на базе алгоритма RSA



**Этап 3.** Получение сообщения и проверка электронной подписи (выполняет получатель **B**).

Получение сообщения и проверка ЭЦП на базе алгоритма RSA



**Использованные источники:**

[https://ru.wikipedia.org/wiki/](https://ru.wikipedia.org/wiki/RSA)

<http://www.michurin.net/>

<https://e-nigma.ru/stat/>

|  |
| --- |
| **Практическое задание № 6** |
| **Тема «Теория чисел»** |

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 .

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

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 на 1 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, если НОД .

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, когда НОД  и НОД .

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

.

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  или  и 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.** Рефлективность:  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 . Тогда .

**Условие задания**

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

a) алгоритмом Евклида,

б) разложением чисел на простые множители.

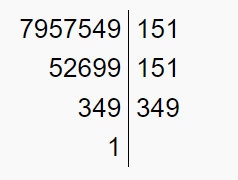
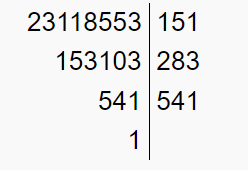
1. С помощью расширенного алгоритма Евклида найти целые u, v, удовлетворяющие соотношению Безу: au + bv = НОД .
2. Найти остаток от деления данного числа на простое.

|  |  |
| --- | --- |
| 11. | 1-3. а = 7957549, b = 23118553.  4. Найти остаток от деления  на 19. |

**Исполнительская часть**

**Задание 1.** Найти канонические разложения чисел

**Решение.**

Следовательно, 7957549 =151∙151∙349

23118553 = 151∙283∙541

**Задание 2.** Найти НОД (7957549, 23118553) пользуясь а) алгоритмом Евклида, б) разложением чисел на простые множители.

**Решение.**

А) Применим алгоритм Евклида.

1) 23118553:7957549=2(остаток7203455), так как 23118553 = 7957549 ∙ 2 + 7203455, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 7957549 на 7203455  
  
2) 7957549:7203455=1(остаток754094),так как 7957549 = 7203455 ∙ 1 + 754094, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 7203455 на 754094  
  
3) 7203455:754094=9(остаток416609),так как 7203455 = 754094 ∙ 9 + 416609, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 754094 на 416609  
  
4) 754094:416609=1(остаток337485),так как 754094 = 416609 ∙ 1 + 337485, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 416609 на 337485  
  
5) 416609:337485=1(остаток79124),так как 416609 = 337485 ∙ 1 + 79124, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 337485 на 79124  
  
6) 337485:79124=4(остаток20989),так как 337485 = 79124 ∙ 4 + 20989, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 79124 на 20989

7) 79124:20989=3(остаток16157),так как 79124 = 20989 ∙ 3 + 16157, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 20989 на 16157  
  
8) 20989:16157=1(остаток4832),так как 20989 = 16157 ∙ 1 + 4832, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 16157 на4832  
  
9)16157:4832=3(остаток1661),так как 16157 = 4832 ∙ 3 + 1661, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 4832 на1661  
  
10)4832:1661=2(остаток1510),так как 4832 = 1661 ∙ 2 + 1510, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 1661 на 1510

11) 1661:15101(остаток151),так как 1661 = 1510 ∙ 1 + 151, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 1510 на 151  
  
1510 : 151 = 10 (остаток 0), так как 1510 = 151 ∙ 10 + 0, равен нулю, значит НОД равен предыдущему остатку от деления

Ответ: НОД (7957549; 23118553) = 151.

Б) С помощью алгоритма разложения на простые моножители

7957549 =151∙151∙349

23118553 = 151∙283∙541

Общие множители чисел: 151

НОД (7957549; 23118553) = 151

**Задание 3.** С помощью расширенного алгоритма Евклида найти целые числа u, v, удовлетворяющие соотношению Безу:  для целых чисел a = 7957549; b = 23118553

**Решение.**

НОД (7957549, 23118553) = 151.

Построим соотношение Безу для данных a и b.

23118553 = 7957549 ∙ 2 + 7203455; поэтому 7203455= 23118553+ 7957549 ∙ (-2)

 7957549 = 7203455 ∙ 1 + 754094; поэтому 754094= 7957549 + 7203455 ∙ (-1)

7203455 = 754094 ∙ 9 + 416609; поэтому 416609= 7203455 + 754094 ∙ (-9)

754094 = 416609 ∙ 1 + 337485; поэтому 337485= 754094 + 416609 ∙ (-1)

416609 = 337485 ∙ 1 + 79124; поэтому 79124= 416609 + 337485 ∙ (-1);

337485 = 79124 ∙ 4 + 20989; поэтому 20989= 337485 + 79124 ∙ (-4)

79124 = 20989 ∙ 3 + 16157; поэтому 16157= 79124 + 20989 ∙ (-3)

20989 = 16157 ∙ 1 + 4832; поэтому 4832= 20989 + 16157 ∙ (-1)

16157 = 4832 ∙ 3 + 1661; поэтому 1661= 16157 + 4832 ∙ (-3)

4832 = 1661 ∙ 2 + 1510; поэтому 1510= 4832 + 1661 ∙ (-2)

1661 = 1510 ∙ 1 + 151; поэтому 151= 1661 + 1510 ∙ (-1)

1510: 151 = 10 (остаток 0), так как 1510 = 151 ∙ 10 + 0

В это равенство подставим выше полученное выражение для 1 и приведем подобные относительно чисел 1661 и 4832. Итак, 0 = 1661 + 1∙(-1661) = 1661 + (4832 + 1661 ∙(-1))(- 1661) = 1661 ∙4832 + 4832 ∙(-1661). В полученное выражение для НОД (7957549, 23118553) = 151 подставим вышеприведенное выражение числа 14. Получим окончательно

0 = 1661 ∙4832 + 4832 ∙ (-1661) = (16157 + 4832 ∙ (-3)) 4832 +4832 ∙ (-7) =16157 ∙4832 +4832 ∙ (-16157) = 0.

    .

**Задание 4.**

а)Найти остаток от деления 20051999 на 19.

**Решение.** 2005 делится на 19 с остатком 10, 20052 делится на 19 с остатком 5. При дальнейшем возведении 2005 в степень остатки от деления будут чередоваться 10, 5, 10, 5, 10, …. Значит, в силу четности степени 1999 остаток от деления требуемого числа на 19 будет равен 10.

20051999=xmod(19)

x = 10

**Практическое задание № 7**

**Тема «Настройка антивирусов»**

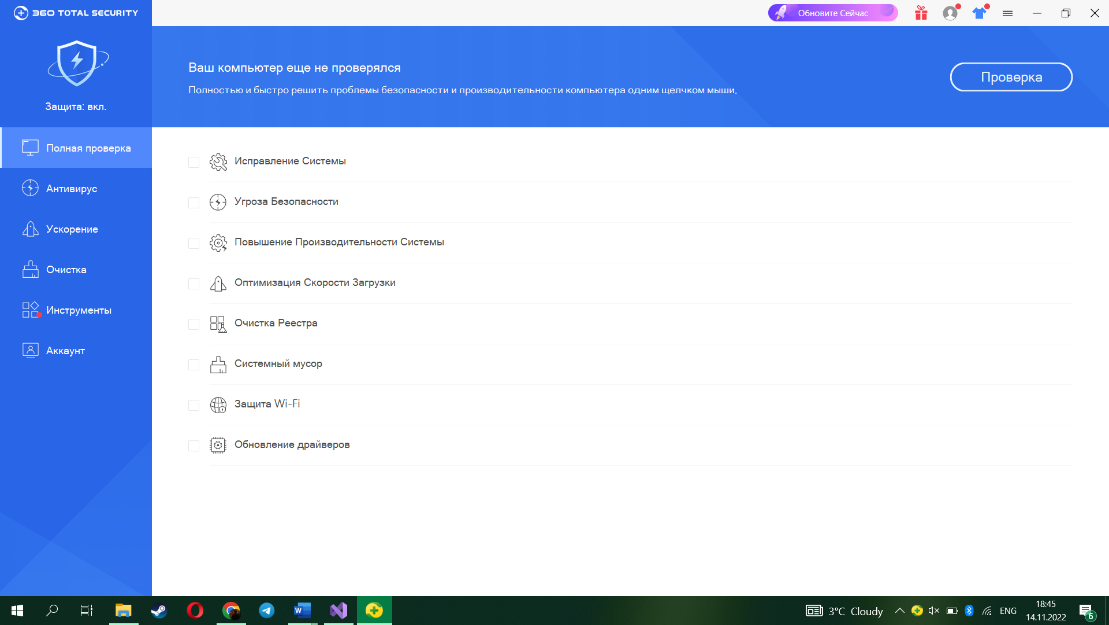


Рисунок 1 – Установка и настройка антивирусной программы 360 TOTAL SECURITY

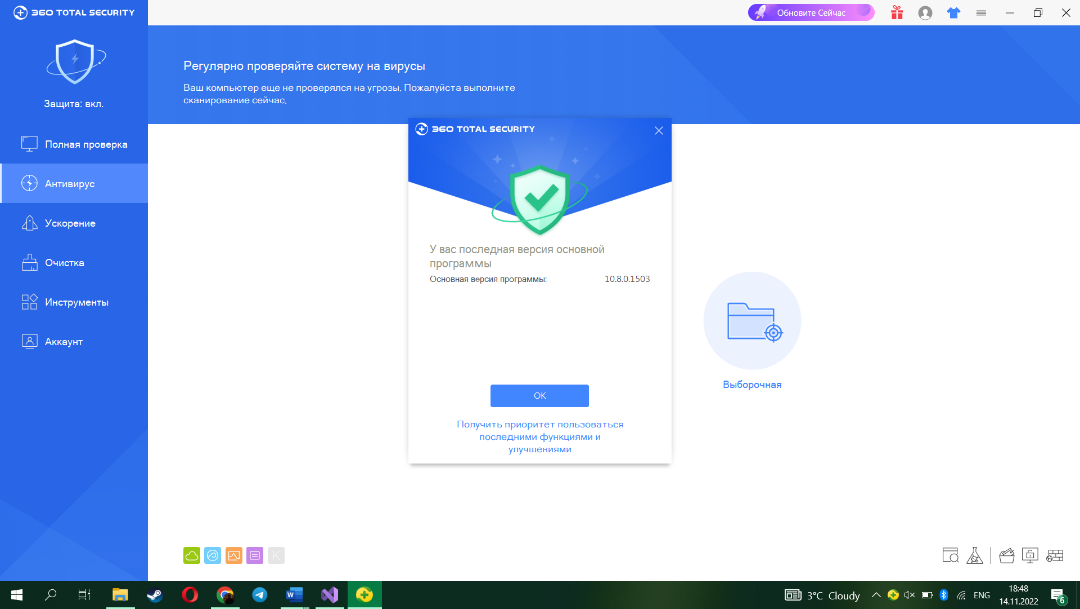


Рисунок 2 – Обновить базу данных сигнатур вирусов

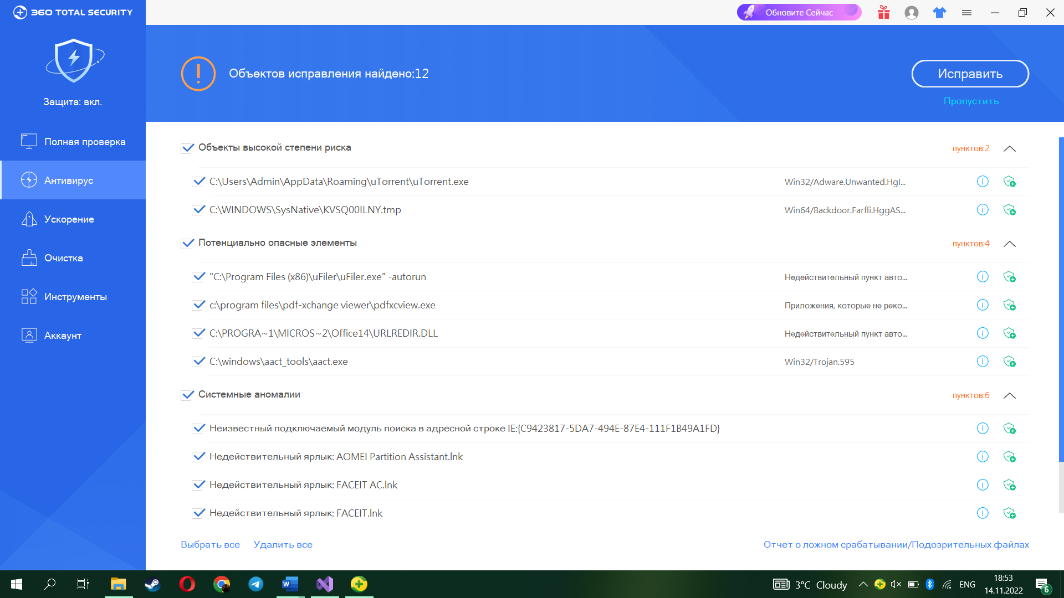


Рисунок 3 – Выполнение сканирования дисков

|  |
| --- |
| **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)**»** |