Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

"ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ сервиса"

(ФГБОУ ВПО «ПВГУС»)

Кафедра "Информационный и электронный сервис"

Зачет по курсу лабораторных работ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /

подпись ф.и.о.

«\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

**ЖУРНАЛ**

**ОТЧЕТОВ ПО ЛАБОРАТОРНЫМ РАБОТАМ**

Дисциплина Защита информации

Студент

Группа

Преподаватель

Тольятти

**Содержание журнала**

[Лабораторная работа №1 3](#_Toc514071334)

[1.1. Российское законодательство по защите компьютерной информации 3](#_Toc514071335)

[1.2. Компьютерные преступления 6](#_Toc514071336)

[1.3. Законодательство РФ в области информационной безопасности 7](#_Toc514071337)

[Выводы по проделанной работе 10](#_Toc514071338)

[Литература, используемая в работе 10](#_Toc514071339)

[Лабораторная работа №2 11](#_Toc514071340)

[2.1. Криптографические методы защиты информации 11](#_Toc514071341)

[2.2. Алгоритмы шифрования 15](#_Toc514071342)

[УПРАЖНЕНИЕ. Индивидуальное задание 15](#_Toc514071343)

[Выводы по проделанной работе 18](#_Toc514071344)

[Литература, используемая в работе 18](#_Toc514071345)

**Отчет по лабораторной работе**

# Лабораторная работа №1

**Тема:** Политика и стандарты безопасности. Законодательно – правовые и организационные методы защиты компьютерной информации

**Цель:** закрепить знания о Российском законодательстве по защите компьютерной информации. Изучить компьютерные преступления

**Оборудование и материальное обеспечение:** персональный компьютер, доступ в Интернет.

**Учебные вопросы**

1.1. Российское законодательство по защите компьютерной информации.

1.2. Компьютерные преступления.

1.3.Законодательство РФ в области информационной безопасности.

**Ход выполнения:**

## Российское законодательство по защите компьютерной информации

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об ин­формации, информатизации и защите информации" от 20 февраля 1995 номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В нём даются основные определения и намечаются направления развития законодательства в данной области.

Вот некоторые из этих определений:

* **информация** — сведения о лицах, предметах, фактах, событиях, явлениях и процессах **независимо** от формы их представления;
* **документированная информация (документ) –** зафиксированная на материальном носителе информация с реквизитами, позво­ляющими ее идентифицировать;
* **информационные процессы** — процессы сбора, обработки, на­копления, хранения, поиска и распространения информации;
* **информационная система** — организационно упорядоченная со­вокупность документов (массивов документов) и информаци­онных технологий, в том **числе** с использованием средств вы­числительной техники и связи, реализующих информационные процессы;
* **информационные ресурсы** - отдельные документы и отдельные  
  массивы документов, документы и массивы документов в ин­формационных системах (библиотеках, архивах, фондах, бан­ках данных, других информационных системах);
* **информация о гражданах (персональные данные) -** сведения о  
  фактах, событиях и обстоятельствах жизни гражданина, позво­ляющие идентифицировать его личность;
* **конфиденциальная информация** — документированная информа­ция, доступ к которой ограничивается в соответствии с законо­дательством Российской Федерации;
* **пользователь (потребитель) информации** - субъект, обращаю­щийся к информационной системе или посреднику за получе­нием необходимой ему информации и пользующийся ею.
* Закон выделяет следующие цели защиты информации:
* предотвращение утечки, хищения, утраты, искажения, поддел­ки информации;
* предотвращение угроз безопасности личности, общества, госу­дарства;
* предотвращение несанкционированных действий по уничто­жению, модификации, искажению, копированию, блокирова­нию информации;
* предотвращение других форм незаконного вмешательства в ин­формационные ресурсы и информационные системы, обеспе­чение правового режима документированной информации как объекта собственности;
* зашита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имею­щихся в информационных системах;
* сохранение государственной тайны, конфиденциальности до­кументированной информации в соответствии с законодатель­ством;
* обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных  
  систем, технологий и средств их обеспечения.

Как же защищать информацию? В качестве основного закон предла­гает для этой цели мощные универсальные средства: лицензирование и сертификацию.

1.Информационные системы, базы и банки данных, предназначенные  
для информационного обслуживания граждан и организаций, под­лежат сертификации в порядке, установленном Законом Россий­ской Федерации "О сертификации продукции и услуг".

2. Информационные системы органов государственной власти Рос­сийской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организа­ций, которые обрабатывают документированную информацию с ог­раниченным доступом, а также средства защиты этих систем подле­жат обязательной сертификации. Порядок сертификации определя­ется законодательством Российской Федерации.

3.Организации, выполняющие работы в области проектирования  
производства средств зашиты информации и обработки персональ­ных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Фе­дерации.

4.Интересы потребителя информации при использовании импортной  
продукции в информационных системах защищаются таможенными  
органами Российской Федерации на основе международной систе­мы сертификации. Рассмотрим пункты следующей статьи 22.

2. Владелец документов, массива документов, информационных сис­тем обеспечивает уровень защиты информации в соответствии с за­конодательством Российской Федерации.

3. Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике  
(владельце) этих систем и средств. Риск, связанный с использова­нием информации, полученной из несертифицированной системы лежит на потребителе информации.

4.Собственник документов, массива документов, информационных  
систем может обращаться в организации, осуществляющие сертификацию средств зашиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер зашиты его ресурсов и систем и получения консультаций.

5.Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима зашиты информации.

Статья 23 "Защита прав субъектов в сфере информационных процессов и информатизации" содержит следующий пункт:

1. Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.

Очень важными являются пункты статьи 5, касающиеся юридической силы электронного документа и электронной цифровой подписи:

1. Юридическая сила документа, хранимого, обрабатываемого и пере  
даваемого с помощью автоматизированных информационных систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

2. Право удостоверять идентичность электронной цифровой подписи  
осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Таким образом, Закон предлагает действенное средство контроля целостности и решения проблемы "неотказуемости" (невозможности от­казаться от собственной подписи).

Таковы важнейшие, положения Закона "Об инфор­мации, информационных технологиях и о защите информации".

## Компьютерные преступления

Уголовный кодекс Российской Федерации (редакция от 14 марта 2002 года). Глава 28 - "Преступления в сфере компьютерной информа­ции" - содержит три статьи:

статья 272. Неправомерный доступ к компьютерной информа­ции;

статья 273. Создание, использование и распространение вредо­носных программ для ЭВМ;

статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Первая имеет дело с посягательствами на конфиденциальность, вторая – с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представляется нам очень своевременным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности деформациинашли наиболее полное выражение в Законе "О государст­венной тайне" (с изменениями и дополнениями от 6 октября 1997 года). В нём государственная тайна определена как защищаемые государством сведения в обла­сти его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств зашиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализо­ваны, а также средства контроля эффективности защиты информации. Подчеркнем важность последней части определения.

## Законодательство РФ в области информационной безопасности

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информационных технологиях и о защите информации" 2006 года. В нём даются основные определения и намечаются направления развития законодательства в данной области.

Вот некоторые из этих определений:

• информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

• документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

• информационные процессы — процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

• информационная система — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

• информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

• информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

• конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

• пользователь (потребитель) информации - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Закон выделяет следующие цели защиты информации:

• предотвращение утечки, хищения, утраты, искажения, подделки информации;

• предотвращение угроз безопасности личности, общества, государства;

• предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

• предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

• зашита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

• сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

• обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Закон на первое место ставит сохранение конфиденциальности информации. Целостность представлена также достаточно полно, хотя и на втором месте. Режим защиты информации устанавливается:

• в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";

• в отношении конфиденциальной документированной информации — собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;

• в отношении персональных данных - федеральным законом. Здесь выделены три вида защищаемой информации, ко второму из которых принадлежит, в частности, коммерческая информация. Поскольку защите подлежит только документированная информация, необходимым условием является фиксация коммерческой информации на материальном носителе и снабжение ее реквизитами. Отметим, что в данном месте Закона речь идет только о конфиденциальности. Защиту государственной тайны и персональных данных берет на себя государство; за другую конфиденциальную информацию отвечают ее собственники. Как же защищать информацию? В качестве основного закон предлагает для этой цели мощные универсальные средства: лицензирование и сертификацию.

Рассмотрим статью 19.

1.Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".

2. Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.

3.Организации, выполняющие работы в области проектирования производства средств зашиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.

4.Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

Рассмотрим пункты следующей статьи 22.

1. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

2.Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из несертифицированной системы лежит на потребителе информации.

3.Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств зашиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер зашиты его ресурсов и систем и получения консультаций.

4.Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима зашиты информации.

Статья 23 "Защита прав субъектов в сфере информационных процессов и информатизации" содержит следующий пункт:

1.Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.

Очень важными являются пункты статьи 5, касающиеся юридической силы электронного документа и электронной цифровой подписи:

1.Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных систем, может подтверждаться электронной цифровой подписью. Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

2.Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации. Таким образом, Закон предлагает действенное средство контроля целостности и решения проблемы "неотказуемости" (невозможности отказаться от собственной подписи). Таковы важнейшие, положения Закона "Об информации, информационных технологиях и о защите информации".

## Выводы по проделанной работе:

Обеспечение безопасности информации очень консервативная область деятельности. На сегодняшний день стремительно меняется все, что касается способов доставки, обработки и представления информации. Если так же быстро будут меняться и сами средства обеспечения безопасности, то их так же быстро приведет их к краху. В вопросах безопасности нужно рассчитывать на технические и программные решения, которые проверены временем и тысячами квалифицированных специалистов.

Самое современное антивирусное программное обеспечение может оказаться совершенно бесполезным, если не реализована надлежащая политика безопасности, определяющая правила применения компьютеров, сети и данных, а также процедуры, предназначенные для предотвращения нарушения этих правил и реакции на подобные нарушения, если таковые все же возникнут.

Следует отметить, что регулярная работа с системными компонентами, которые обеспечивают безопасность, способствует ее повышению. Необходимо экспериментировать, применять различные средства защиты информации, постоянно модифицировать ключевую информацию, которая используется в этих средствах.

## Литература, используемая в работе:

1. Громов Ю.Ю. Информационная безопасность и защита информации: учебное пособие / Ю.Ю. Громов. – Белгород : ТНТ, 2015. – 539 с.
2. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – М. : ДМК Пресс, 2016. – 702 с.
3. Баранова Е.К. Актуальные вопросы защиты информации / Е.К. Баранова. – М. : Научная мысль, 2017. – 111 с.
4. Краковский Ю.М. Защита информации: учебное пособие / Ю.М. Краковский. – Ростов-на-Дону : Феникс, 2017. – 347 с.

**Отчет по лабораторной работе**

# Лабораторная работа №2

**Тема:** Криптографические методы защиты информации

**Цель:** Освоить основыкриптографических методов защиты информации. Алгоритмы шифрования.

**Оборудование и материальное обеспечение:** тетрадь, ручка, персональный компьютер, доступ в Интернет.

**Учебные вопросы**

2.1. Криптографические методы защиты информации.

2.2.Алгоритмы шифрования.

**Ход выполнения:**

## 2.1. Криптографические методы защиты информации

Криптографические методы защиты информации составляют основу подсистем безопасности современных информационных систем, обеспечивая услуги конфиденциальности, целостности и аутентификации.

риптография – наука о методах и средствах преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею,включающая в себя также методы и средства создания, хранения и распространения ключей – специальных информационных объектов, реализующих эти санкции.

Основным понятием криптографии является понятие шифра. Шифр – совокупность инъективных (обратимых) преобразований множества элементов открытого текста на множество элементов шифротекста, проиндексированных элементами из множества ключей:

{ Fk : X &rarr S, k ∈ K },

где X ∈ X – кодируемое сообщение из множества открытых текстов;

S ∈ S – шифротекст из множества возможных закодированных текстов;

k – ключ шифрования;

F – отображение, выполняемое шифром.

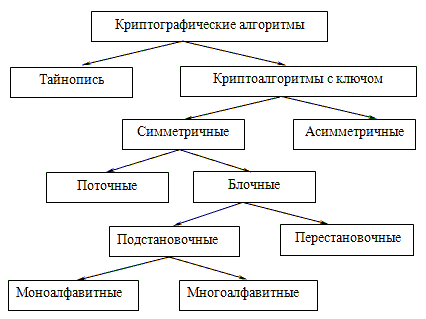
Свойство инъективности шифра означает, что существует отображение F-1 такое, что { Fk-1 : X → S, k ∈ K }

Процесс преобразования открытого текста (передаваемого сообщения) в шифротекст называется шифрованием. Обратное преобразование шифротекста в открытый текст называется дешифрованием.

Криптоанализ - наука (и практика ее применения) о методах и способах вскрытия шифров. Под вскрытием понимается задача получения по известному шифротесту соответствующего открытого текста и/или ключа шифрования.

Криптография и криптоанализ вместе образуют криптологию.

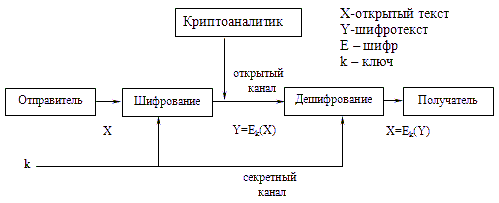
В качестве основного критерия классификации криптографических алгоритмов будем использовать тип выполняемого над исходным текстом преобразования. Классификация по этому критерию представлена на рис. 2.1.

  
Рис. 2.1. Общая классификация криптографических алгоритмов

Тайнопись предполагает, что отправитель и получатель производят над сообщением преобразования, известные только им двоим. Сторонним лицам неизвестны выполняемые алгоритмом изменения над открытым текстом, что и является гарантией нераскрываемости данных на этапе анализа.

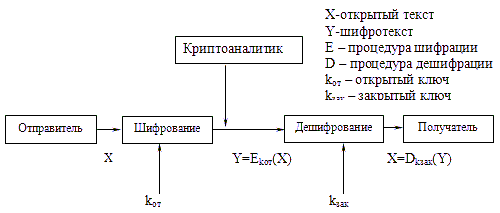
В противовес тайнописи, криптоалгоритмы с ключом построены на том принципе, что алгоритм воздействия на передаваемые данные известен всем сторонним лицам, но он зависит от некоторого параметра, который держится в секрете – «ключа», который известен только двум лицам, участвующим в обмене информацией. Основу такого подхода к шифрованию заложил в конце XIX века голландец Огюст Керкхофф, который предложил, что стойкость шифра должна определяться только секретностью ключа, т.е. криптоаналитику могут быть известны все детали процесса (алгоритма) шифрования и дешифрования, но неизвестно, какой ключ использован для шифрования данного текста. В настоящее время криптография занимается исключительно алгоритмами с ключами. Это обусловлено тем, что защищенность системы не должна зависеть от секретности чего-либо, что невозможно быстро изменить в случае утечки секретной информации, а изменить ключ шифрования на практике гораздо проще, чем весь используемый в системе алгоритм.

Криптосистемы с ключом делятся на симметричные и асимметричные системы шифрования. Модель симметричной системы шифрования представлена на рис. 2.2.

  
Рис. 2.2. Обобщенная модель симметричной системы шифрования

Отличительной чертой симметричных алгоритмов шифрования является наличие одного ключа шифрования (k на рис.2.2), который должен быть известен только отправителю и получателю сообщения. Отправитель на ключе k шифрует сообщение, получатель дешифрует полученный шифротекст ключом k. Криптоаналитик может перехватить шифротекст Y, передаваемый по открытым каналам связи, но, так как он не знает ключа, задача вскрытия шифротекста является очень трудоемкой. Принципиальным моментом является необходимость наличия секретного канала связи между получателем и отправителем для передачи ключа шифрования без возможности его перехвата криптоаналитиком.

Асимметричная система шифрования работает по схеме, представленной на рис. 2.3.

  
Рис. 2.3. Обобщенная модель асимметричной системы шифрования

Отличительной особенностью асимметричных алгоритмов является наличие пары ключей шифрования: открытого kот, который передается второй стороне по незащищенному каналу связи и поэтому может быть известен криптоаналитику,а также закрытого kзак, который известен лишь одному человеку (получателю сообщения) и держится в секрете. Пара ключей обладает тем свойством, что сообщение, зашифрованное на одном из ключей, может быть расшифровано только на другом ключе. Фактически это означает, что секретным каналом передачи информации на схеме рис. 2.3 является направление «отправитель-получатель», поскольку сообщение, зашифрованное на открытом ключе отправителем, может дешифровать своим закрытым ключом только получатель.

В зависимости от размера блока шифруемой информации криптоалгоритмы делятся на блочные и поточные шифры. Единицей кодирования в потоковых шифрах является один бит. Результат кодирования не зависит от прошедшего ранее входного потока. Схема применяется в системах передачи потоков информации, то есть в тех случаях, когда передача информации начинается и заканчивается в произвольные моменты времени и может случайно прерываться. Для блочных шифров единицей кодирования является блок из нескольких байтов. Результат кодирования зависит от всех исходных байтов этого блока. Схема применяется при пакетной передаче информации и кодировании файлов.

Еще одним критерием классификации криптоалгоритмов является тип выполняемых преобразований над блоками открытого текста. По этому критерию криптоалгоритмы разделяют на подстановочные иперестановочные. В перестановочных шифрах блоки информации не изменяются сами по себе, но изменяется их порядок следования, что делает информацию недоступной стороннему наблюдателю. Подстановочные шифры изменяют сами блоки информации по определенным законам.

Деление криптоалгоритмов на моноалфавитные и многоалфавитные характерно для подстановочных шифров. Моноалфавитные криптоалгоритмы заменяют блок входного текста (символ входного алфавита) на один и тот же блок шифротекта (символ выходного алфавита). В многоалфавитных шифрах одному и тому же блоку входного текста могут соответствовать разные блоки шифротекста, что существенно затрудняет криптоанализ.

По степени секретности криптоалгоритмы делятся на абсолютно стойкие и практически стойкие. Абсолютно стойкие шифры невозможно вскрыть. На практике этого можно добиться, только если размер используемого ключа шифрования превышает размер кодируемого сообщения и при этом ключ используется однократно. Практически стойкимназывается шифр, для которого не существует более эффективного способа взлома, кроме как полным перебором всех возможных ключей шифрования.

Говоря об атаках на шифры, можно выделить следующие виды атак: атака на основе шифротекста, атака на основе известного открытого текста, атака на основе выборочного открытого текста.

При атаке на основе шифротекста криптоаналитику известен только закодированный текст и на его основе он должен узнать секретный ключ шифрования.

Атака на основе открытого текста предполагает, что криптоаналитику известны одна или несколько пар «открытый текст/шифротекст», зашифрованных на одном ключе, и на основе этой информации он проводит свой анализ.

Выполняя атаку на основе выборочного открытого текста, злоумышленник имеет возможность подать на вход шифрующего устройства произвольный открытый текст и получить соответствующий ему шифротект. Для того, чтобы называться практически стойким, криптоалгоритм должен успешно противостоять любому из перечисленных типов атак.

## 

## 2.2. Алгоритмы шифрования

Для того, чтобы ваша информация, пройдя шифрование, превратилась в "информационный мусор", бессмысленный набор символов для постороннего, используются специально разработанные методы - алгоритмы шифрования.   
Такие алгоритмы разрабатываются учеными математиками или целыми коллективами сотрудников компаний или научных центров.

Симметричные алгоритмы

Алгоритмы шифрования делятся на два больших класса: симметричные (AES, ГОСТ, Blowfish, CAST, DES) и асимметричные (RSA, El-Gamal). Симметричные алгоритмы шифрования используют один и тот же ключ для зашифровывания информации и для ее расшифровывания, а асимметричные алгоритмы используют два ключа - один для зашифровывания, другой для расшифровывания.

Ключ шифрования

Это случайная или специальным образом созданная по паролю последовательность бит, являющаяся переменным параметром алгоритма шифрования.   
Если зашифровать одни и те же данные одним алгоритмом, но разными ключами, результаты получатся тоже разные.  Обычно в Программах для шифрования (WinRAR, Rohos и т.д.) ключ создается из пароля, который задает пользователь.

Ключ шифрования бывает разной длины, которая, как правило, измеряется в битах. С увеличением длины ключа повышается теоритическая стойкость шифра. На практике это не всегда верно.

Стойкость алгоритма шифрования.

Алгоритм шифрования считается стойким до тех пор, пока не будет доказано обратное. Таким образом, если алгоритм шифрования опубликован, существует более 5 лет, и для него не найдено серьезных уязвимостей, можно считать, что его стойкость подходит для задач защиты секретной информации.

# УПРАЖНЕНИЕ. Индивидуальное задание

**Текст для шифрования:**

МАТРИЧНЫЙ СТРУЙНЫЙ ЛАЗЕРНЫЙ СПЕЦИАЛЬНЫЙ ПРИНТЕРЫ

**Задание 2.1.** Метод шифрования путём замены с использованием алгоритма моноалфавитной замены.

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

МАТРИЧНЫЙ СТРУЙНЫЙ ЛАЗЕРНЫЙ СПЕЦИАЛЬНЫЙ ПРИНТЕРЫ

Ответ: УЯНПЧИТДЦ ОНПМЦТДЦ ФЯЩЬПТДЦ ОРЬЙЧЯФЕТДЦ РПЧТНЬПД

**Задание 2.2.** Метод шифрование путём замены с помощью матрицы Вижинера

Квадрат Виженера представлен на рис.2.4.

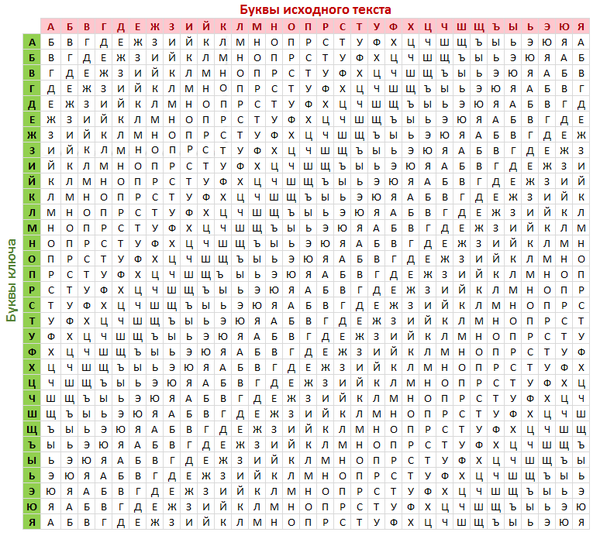


Рисунок 2.4 – Квадрат Виженера

МАТРИЧНЫЙСТРУЙНЫЙЛАЗЕРНЫЙСПЕЦИАЛЬНЫЙПРИНТЕРЫ

ФРАГМЕНТФРАГМЕНТФРАГМЕНТФРАГМЕНТФРАГМЕНТФРАГ

Решение данной задачи оформлено в таблице 2.1.

*Таблица 2.1. Алгоритм шифрования текста по схеме Виженера*

|  |  |  |
| --- | --- | --- |
| Исходный | Ключ | Шифрование |
| М | Ф | Б |
| А | Р | С |
| Т | А | У |
| Р | Г | Ф |
| И | М | Х |
| Ч | Е | Э |
| Н | Н | Ы |
| Ы | Т | О |
| Й | Ф | Ю |
| С | Р | В |
| Т | А | У |
| Р | Г | Ф |
| У | М | А |
| Й | Е | П |
| Н | Н | Ы |
| Ы | Т | О |
| Й | Ф | Ю |
| Л | Р | Ь |
| А | А | Б |
| З | Г | Л |
| Е | М | Т |
| Р | Е | Ц |
| Н | Н | Ы |
| Ы | Т | О |
| Й | Ф | Ю |
| С | Р | В |
| П | А | Р |
| Е | Г | Й |
| Ц | М | Г |
| И | Е | О |
| А | Н | О |
| Л | Т | Ю |
| Ь | Ф | С |
| Н | Р | Ю |
| Ы | А | Ь |
| Й | Г | Н |
| П | М | Ь |
| Р | Е | Ц |
| И | Н | Ц |
| Н | Т | А |
| Т | Ф | З |
| Е | Р | Ц |
| Р | А | С |
| Ы | Г | Я |

Ответ:

БСУФХЭЫОЮВУФАПЫОЮЬБЛТЦЫОЮВРЙГООЮСЮЬНЬЦЦАЗЦСЯ

## Выводы по проделанной работе:

Раскрыть шифр Вижинера, тем же способом, что и шифр одноалфавитной замены, невозможно, так как одни и те же символы открытого текста могут быть заменены различными символами зашифрованного текста. С другой стороны, различные буквы открытого текста могут быть заменены одинаковыми знаками зашифрованного текста.

Особенность данного метода многоалфавитной подстановки заключается в том, что каждый из символов ключа используется для шифрования одного символа исходного сообщения. После использования всех символов ключа, они повторяются в том же порядке. Если используется ключ из десяти букв, то каждая десятая буква сообщения шифруется одним и тем же символом ключа. Этот параметр называется *периодом* шифра. Если ключ шифрования состоит из одного символа, то при шифровании будет использоваться одна строка таблицы Вижинера, следовательно, в этом случае мы получим моноалфавитную подстановку, а именно шифр Цезаря.

С целью повышения надежности шифрования текста можно использовать подряд два или более зашифрования по методу Вижинера с разными ключами (составной шифр Вижинера).

## Литература, используемая в работе:

1. Симонович С.В. Информатика. Базовый курс. Дрофа 2012.
2. Савельев А. Я. Основы информатики: Учебник для вузов. Оникс 2011.
3. Баричев С. Введение в криптографию. Электронный сборник. 2005.