**КОНТРОЛЬНАЯ РАБОТА**

по Основам Защиты Информации (ОЗИ)

для студентов ИИТ

**1 Теоретические сведения**

**1.1 Угрозы информационной безопасности, их приоритет и методы парирования. 1.1.1. Основные понятия и термины науки о защите информации**. Под **информацией** (И) понимают [1] сведения о лицах, предметах, фактах, событиях, явлениях и процессах. **И** может существовать в виде бумажного документа, физических полей и сигналов (электромагнитных, акустических, тепловых и т.д.), биологических полей (память человека). В дальнейшем будем рассматривать **И** в документированной (на бумаге, дискете и т. д.) форме и в форме физических полей (радиосигналы, акустические сигналы). Среду, в которой **И** создается, передается, обрабатывается или хранится, будем называть **информационным объектом** (ИО) [1].

В контрольной работе из множества ИО будем рассматривать только информационные системы (ИС), частными видами которых является компьютер, компьютерная сеть (локальная и интернет), мобильное устройство (телефон и другие гаджеты), кассовый суммирующий аппарат (КСА), пластиковая интеллектуальная карта (кредитная, телефонная или другая) и т. д.

**Информационная безопасность** (**ИБ**) – это защищенность информации и поддерживающей инфраструктуры (ИС и др.) от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. К случайным (непреднамеренным) воздействиям на ИО относятся стихийные бедствия, отказы оборудования, ошибки персонала и т.д.), к преднамеренным – действия злоумышленников. Все воздействия могут привести к **последствиям (ущербу)** трех видов: **нарушению конфиденциальности, целостности, доступности**.

**Нарушение конфиденциальности** — нарушение свойства информации быть известной только определенным субъектам. **Нарушение целостности** — несанкционированное изменение, искажение, уничтожение информации.

**Нарушение доступности** (отказ в обслуживании) — нарушаются доступ к информации, работоспособность объекта, доступ в который получил злоумышленник. В отличие от разрешенного (санкционированного) доступа к информации в результате преднамеренных действий злоумышленник получает несанкционированный доступ. Суть несанкционированного доступа состоит в получении нарушителем доступа к объекту в нарушение установленных правил [1].

Под **угрозой** ИБ ИО будем понимать возможные воздействия на него, приводящие к ущербу. Некоторое свойство объекта, делающее возможным возникновение и реализацию угрозы, будем называть **уязвимостью**. Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку, — **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы**. **Цель** ИБ – обеспечить непрерывность бизнеса организации, по возможности предотвратить и/или минимизировать ущерб от нарушений безопасности. **Защита информации** – это комплекс мероприятий, направленных на обеспечение ИБ. **Управление ИБ** позволяет эффективно использовать данные, одновременно обеспечивая их защиту и защиту вычислительных ресурсов. **Политика безопасности** — совокупность норм, правил, рекомендаций, регламентирующих работу средств защиты ИО от заданного множества угроз безопасности.

Приоритéт (лат. prior — первый, старший) — понятие, показывающее важность, первенство. **Приоритет угрозы ИБ** – важность её. Наиболее приоритетная (самая важная) угроза – угроза ИБ, наносящая максимальный ущерб ИО при нарушении его безопасности.

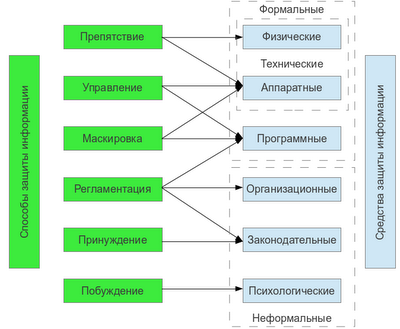
**1.1.2 Классификация угроз** проводится по следующим **критериям:**

* **по аспекту ИБ**, против которого угрозы направлены в первую очередь (доступность, целостность, конфиденциальность, собственность);
* **по компонентам ИС,** на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура (компьютеры, обслуживающий персонал, помещения, системы связи, электропитания, водо- и/или теплоснабжения, кондиционирования и др.));
* **по способу осуществления** (случайные/преднамеренные, природные/ техногенного характера);
* **по расположению** источника угроз (внутренние/внешние) и др.

Примеры угроз:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Вид угроз | | |
| доступности | целостности | конфиденциальности |
| Приме-ры угроз | отказ пользователей [4] | ввод неверных данных | перехват паролей |
| непреднамеренные ошибки штатных пользователей, системных админист-раторов и других лиц, обслуживающих ИС | изменение данных | размещение и передача конфиденциальных дан-ных в небезопасной среде |
| внутренний отказ ИС | нарушение атомарности транзакций | и др. |
| отказ поддерживающей инфраструктуры | переупорядочение |  |
| природные угрозы (стихийные бедствия, электромагнитные бури, радиоактивные излучения и осадки и др. | дублирование или внесение дополни-тельных сообщений |  |
| и др. | кража и др. |  |

**1.1.3 Методы парирования угроз ИБ** (способы защиты информации в ИО [7]).



**Способы (методы)** защиты информации (парирования угроз ИБ):

* Препятствие – создание на пути угрозы преграды, преодоление которой сопряжено с возникновением сложностей для злоумышленника или дестабилизирующего фактора.
* Управление – оказание управляющих воздействий на элементы защищаемой системы.
* Маскировка – действия над защищаемой системой или информацией, приводящие к такому их преобразованию, которое делает их недоступными для злоумышленника (сюда можно, в частности, отнести криптографические методы защиты).
* Регламентация – разработка и реализация комплекса мероприятий, создающих такие условия обработки информации, которые существенно затрудняют реализацию атак злоумышленника или воздействия других дестабилизирующих факторов.
* Принуждение – метод заключается в создании условий, при которых пользователи и персонал вынуждены соблюдать условия обработки информации под угрозой ответственности (материальной, уголовной, административной)
* Побуждение – метод заключается в создании условий, при которых пользователи и персонал соблюдают условия обработки информации по морально-этическим и психологическим соображениям.

**Средства** защиты информации:

* Физические средства – механические, электрические, электромеханические, электронные, электронно-механические и т. п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.
* Аппаратные средства – различные электронные и электронно-механические и т.п. устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации.
* Программные средства – специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации.
* Организационные средства – организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации.
* Законодательные средства – нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности.
* Психологические (морально-этические средства) - сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

**1.2 Защита информации от утечки по акустическому каналу. Акустический (речевой) канал –** это канал распространения акустических волн через газовую, твердую и жидкую среду. Человеческая речь – наиболее распространенный способ обмена информацией между людьми, поэтому попытки перехвата речевой акустической информации (утечки по акустическому каналу) давно уже стали традиционными. Особая заинтересованность злоумышленников в получении речевой информации объясняется тем, что речь довольно часто содержит конфиденциальные и даже секретные сведения.

Для перехвата речевой информации по акустическим каналам в качестве средств акустической разведки используются электронные стетоскопы и закладные устройства с датчиками контактного типа. В качестве датчиков средств акустической разведки используются контактные микрофоны (вибропребразователи), чувствительность которых составляет от 50 до 100 мкВ/Па, что, дает возможность прослушивать разговоры и улавливать слабые звуковые колебания (шорохи, тиканье часов и т.д.) через бетонные и кирпичные стены толщиной более 100 см, а также двери, оконные рамы и инженерные коммуникации. Электронные стетоскопы и закладные устройства с датчиками контактного типа позволяют перехватывать речевую информацию без физического доступа людей в защищаемые помещения. Их датчики наиболее часто устанавливаются на наружных поверхностях зданий, на оконных проемах и рамах, в смежных (служебных и технических) помещениях за дверными проемами, ограждающими конструкциями, на перегородках, трубах систем отопления и водоснабжения, коробах воздуховодов вентиляционных и других систем.

Сила (интенсивность) звука– это количество звуковой энергии, проходящей за единицу времени через единицу площади, измеряется в ваттах на квадратный метр (Вт/м2). Звуковое давление и сила звука связаны между собой квадратичной зависимостью, то есть увеличение звукового давления в два раза приводит к увеличению силы звука в четыре раза. Уровень силы звука– это отношение силы данного звука  к нулевому (стандартному) уровню (за который принята сила звука = 10-12 Вт/м2) выраженное в децибелах (дБ)

|  |  |
| --- | --- |
|  | (1) |

Уровни звукового давления и силы звука, выраженные в дБ, совпадают по величине. Порог слышимости- наиболее тихий звук, который еще способен слышать человек на частоте 1000 Гц, что соответствует звуковому давлению 210-5 Н/м2. Громкость звука– это интенсивность звукового ощущения, вызванная данным звуком у человека с нормальным слухом. Громкость зависит от силы звука и его частоты, измеряется пропорционально логарифму силы звука и выражается количеством дБ, на которое данный звук превышает по интенсивности звук, принятый за порог слышимости. Единица измерения громкости – это фон. Динамический диапазон– это диапазон громкостей звука или разность уровней звукового давления самого громкого и самого тихого звуков, выраженная в дБ.

Возможности по перехвату информации будут во многом определяться затуханием информационного сигнала в ограждающих конструкциях и уровнем внешних шумов в месте установки контактного микрофона. Результаты экспериментальных исследований звукоизоляции Q стен и сплошных перегородок приведены в табл. 1, причём затухание

, (2)

где  – сила звука в защищаемом помещении,

 – сила звука в незащищённом коридоре.

Таблица 1 – Зависимость затухания Q от толщины конструкции стен и сплошных перегородок

|  |  |  |
| --- | --- | --- |
| Вид конструкции | Толщина конструкции | Среднее значение затухания Q, дБ, для среднегеометрической частоты, 1000 Гц |
| Кирпичная кладка, оштукатуренная с двух сторон | 0,5 кирпича  1 кирпич  1,5 кирпича  2 кирпича  2,5 кирпича | 48  58  61  65  67 |
|
| Железобетонная панель | 1 панель 100 мм  3 панели по 100 мм (всего 300 мм)  4 панели по 100мм (всего 400 мм) | 50  65  67 |
|

**1.3 Криптография. 1.3.1 Краткие сведения о криптографической защите информации. Криптография** – это наука о методах, алгоритмах, программных и аппаратных средствах преобразования информации в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования. Наряду с решением задач обеспечения конфиденциальности, целостности и доступности информации существует задача анализа стойкости используемых криптопреобразований. Эта задача решается наукой, называемой криптоанализ*.* Криптография и криптоанализ составляют науку – криптологию.

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, имеет вид (рис. 1). Отправитель генерирует открытый текст исходного сообщения , которое должно передаваться по открытому каналу. Отправитель шифрует текст с помощью обратимого преобразования  и ключа :  и получает шифротекст , который отправляет получателю. Получатель, приняв шифротекст , расшифровывает его с помощью обратного преобразования  и получает исходное сообщение в виде открытого текста :.

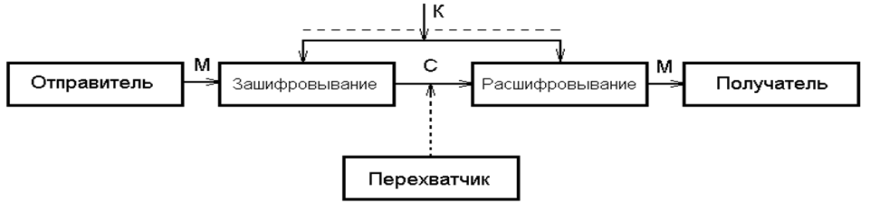


Рисунок 1 – Обобщенная схема симметричной криптографической системы с одним ключом

Преобразование  выбирается из семейства криптографических преобразований, называемых *криптоалгоритмами*. Параметр, с помощью которого выбирается конкретное преобразование, называется *криптографическим ключом* . Система, в которой осуществляется зашифровывание и расшифровывание сообщений, называется *криптосистемой.*

Преобразование зашифровывания может быть симметричным или асимметричным относительно преобразования расшифровывания. Поэтому различают два класса криптосистем: симметричные криптосистемы и асимметричные криптосистемы. Иногда их называют: одноключевые (с секретным ключом) и двухключевые (с открытым ключом). Схема симметричной криптосистемы с одним секретным ключом  была показана на рис. 1. Обобщенная схема асимметричной криптосистемы с двумя разными ключами  и  показана на рис. 2.

В этой криптосистеме один из ключей является открытым , а другой  – секретным. Для этой криптосистемы , а .

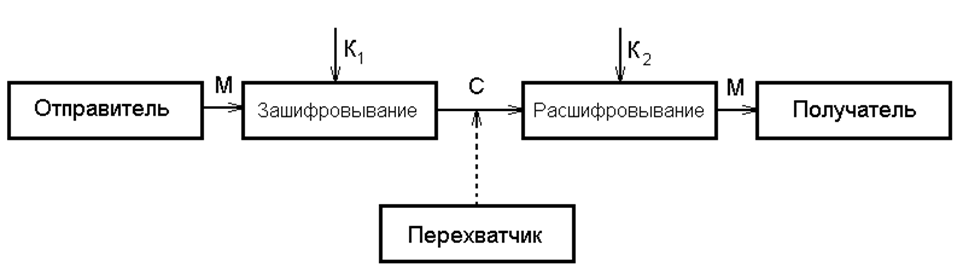


Рисунок 2 – Обобщенная схема симметричной криптографической системы с системы с двумя разными ключами

В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей, например, спецсвязью. В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют в месте его генерации.

Любая попытка со стороны злоумышленника расшифровать шифротекст  для получения открытого текста  или зашифровать свой собственный текст  для получения правдоподобного шифротекста , не имея подлинного ключа, называется *криптоатакой.* Свойство криптосистемы, противостоять криптоатаке называется *криптостойкостью*.

Фундаментальное правило криптоанализа, впервые сформулированное голландцем А.Керкхоффом еще в XIX веке, заключается в том, что стойкость шифра (криптосистемы) должна определяться только секретностью ключа. Иными словами, правило Керкхоффа состоит в том, что весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника. Другое почти общепринятое допущение в криптоанализе состоит в том, что криптоаналитик имеет в своем распоряжении шифротексты сообщений.

**1.3.2 Блочные и поточные шифры**. Применение шифрования ко всему сообщению в целом реализуется очень редко. Практически все применяемые криптографические методы связаны с разбиением сообщения на большое число фрагментов (или знаков) фиксированного размера, каждый из которых шифруется отдельно. Такой подход существенно упрощает задачу шифрования, так как сообщения обычно имеют различную длину. Можно выделить следующие характерные признаки методов шифрования данных:

* выполнение операций с отдельными битами или блоками;
* зависимость или независимость функции шифрования от результатов шифрования предыдущих частей сообщения;
* зависимость или независимость шифрования отдельных знаков от их положения в тексте.

В соответствии с этим различают три основных способа шифрования: поточные шифры; 2) блочные шифры; 3) блочные шифры с обратной связью.

***1.3.2.1 Поточное шифрование****.* Поточное шифрование состоит в том, что каждый бит открытого текста и соответствующий бит ключа преобразовываются по определенному алгоритму (например, складываются по модулю 2). К достоинствам поточных шифров относятся высокая скорость шифрования, относительная простота реализации и отсутствие размножения ошибок. Недостатком является необходимость использовать для каждого сообщения другой ключ. Это обусловлено тем, что если два различных сообщения шифруются на одном и том же ключе, то эти сообщения легко могут быть расшифрованы

***1.3.2.2*** *Блочное шифрование.* При блочном шифровании открытый текст сначала разбивается на равные по длине блоки, затем применяется зависящая от ключа функция шифрования для преобразования блока открытого текста длиной  бит в блок шифротекста такой же длины. Применение блочного шифра имеет недостатки. Первый из них заключается в том, что вследствие детерминированного характера шифрования при фиксированной длине блока 64 бита можно осуществить криптоанализ шифротекста "со словарем" в ограниченной форме. Это обусловлено тем, что идентичные блоки открытого текста длиной 64 бита в исходном сообщении представляются идентичными блоками шифротекста, что позволяет криптоаналитику сделать определенные выводы о содержании сообщения. Другой потенциальный недостаток этого шифра связан с размножением ошибок. Результатом изменения только одного бита в принятом блоке шифротекста будет неправильное расшифровывание всего блока. Это, в свою очередь, приведет к появлению искаженных битов (от 1 до 64) в восстановленном блоке исходного текста. Из-за отмеченных недостатков блочные шифры редко применяются в указанном режиме для шифрования длинных сообщений. Однако в финансовых учреждениях, где сообщения часто состоят из одного или двух блоков, блочные шифры широко используют в режиме прямого шифрования.

***1.3.2.3 Блочное шифрование с обратной связью****.* Как и при блочном шифровании, сообщения разбивают на ряд блоков, состоящих из  бит. Для преобразования этих блоков в блоки шифротекста, которые также состоят из  бит, используются специальные функции шифрования. Однако если в блочном шифре такая функция зависит только от ключа, то в блочных шифрах с обратной связью она зависит как от ключа, так и от одного или более предшествующих блоков шифротекста.

***1.3.3 Традиционные симметричные криптосистемы***. Традиционные (классические) методы шифрования, отличаются симметричной функцией шифрования. К ним относятся шифры перестановки, шифры простой и сложной замены, а также некоторые их модификации и комбинации. По мнению К. Шеннона, в практических шифрах необходимо использовать два общих принципа: рассеивание и перемешивание. **Рассеивание** представляет собой распространение влияния одного знака открытого текста на много знаков шифротекста, что позволяет скрыть статистические свойства открытого текста. **Перемешивание** предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов. Распространенным способом достижения эффектов рассеивания и перемешивания является использование составного шифра, т.е. такого шифра, который может быть реализован в виде некоторой последовательности простых шифров, каждые из которых вносит свой вклад в значительное суммарное рассеивание и перемешивание.

В составных шифрах в качестве простых шифров чаще всего используются простые перестановки и подстановки. При перестановке просто перемешивают символы открытого текста, причем конкретный вид перемешивания определяется секретным ключом. При подстановке каждый символ открытого текста заменяют другим символом из того же алфавита, а конкретный вид подстановки также определяется секретным ключом.

***1.3.4*** *Шифры перестановок.* Эти шифры являются наиболее простыми и, вероятно, наиболее древними. При шифровании перестановкой символы шифруемого текста переставляются по определённому правилу в пределах блока этого текста. Например, сообщение делится на блоки по 3 символа, 1-й символ становится 2-м, 3-й – 1-м, а 2-й – 3-м. Пример 1 шифротекста: МСОЙНОНЖЕЕАНДЛАКИТООЛ (СОМ НОЙ ЖЕН АНЕ ЛАД ИТК ОЛО ТИТ АНЕ ГЛА ДИТ). Правило перестановок символов является ключом и задается различными предметами: цилиндром (скитала, древние греки), размером таблицы, условным словом или фразой (шифрующие таблицы в эпоху Возрождения), магическим квадратом в средние века. Пример 2 шифрующей таблицы. Шифруем – НАШИ МАГИСТРАНТКИ САМЫЕ УМНЫЕ. Ключ – размер таблицы 13\*2, куда шифруемый текст записывается по столбцам, затем текст списывется по строкам:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Н | Ш | М | Г | С | Р | Н | К | С | М | Е | М | Ы |
| А | И | А | И | Т | А | Т | И | А | Ы | У | Н | Е |

Получим: НШМГСРНКСМЕМЫАИАИТАТИАЫУНЕ. Этот шифротекст для большей внешней запутанности можно разделить на группы по 2 символа, например: НШ МГ СР

Несколько большей стойкостью к расшифрованию обладает метод, называемый *одиночной перестановкой по ключу*. Возьмём в качестве шифруемого сообщения первых 15 символов сообщения из примера 1, запишем их в таблицу 5\*3 и используем ключевое слово БГУИР. Получим (справа БГУИР записано в алфавитном порядке):

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Б | Г | У | И | Р |  | Б | Г | И | Р | У |
| 1 | 2 | 4 | 3 | 5 | 1 | 2 | 3 | 4 | 5 |
| С | Н | Ж | А | Л | С | Н | А | Л | Ж |
| О | О | Е | Н | А | О | О | Н | А | Е |
| М | Й | Н | Е | Д | М | Й | Е | Д | Н |

Столбцы в квадрате справа переставляются так, как велит ключевое слово. Шифротекст – СНАЛЖ ООНАЕ-МЙЕДН.

1.3.4 сложный. Перестановки (более сложные) используются также в методе, основанном на применении *маршрутов Гамильтона.* Этот метод реализуется путем выполнения следующих шагов.

Шаг I. Исходная информация разбивается на блоки. Если длина шифруемой информации не кратна длине блока, то на свободные места последнего блока помещаются специальные служебные символы-заполнители (например, \*).

Шаг 2. Символами блока заполняется таблица, в которой для каждого порядкового номера символа в блоке отводится вполне определенное место (рис. 3).

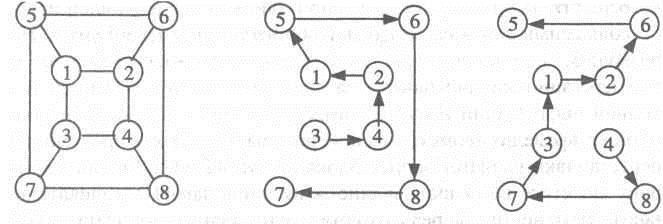


Таблица Маршрут .№ 1 Маршрут № 2

Рисунок 3 – Вариант 8-элементной таблицы и маршрутов Гамильтона

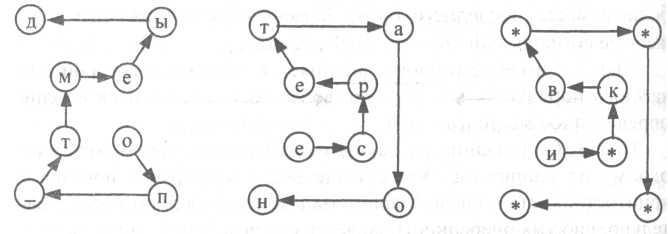
Шаг 3. Считывание символов из таблицы осуществляется по одному из маршрутов. Увеличение числа маршрутов повышает криптостойкость шифра. Маршруты выбираются либо последовательно, либо их очередность задается ключом К.

Шаг 4. Зашифрованная последовательность символов разбивается на блоки фиксированной длины L. Величина L может отличаться от длины блоков, на которые разбивается исходная информация на шаге 1. Расшифрование производится в обратном порядке. В соответствии с ключом выбирается маршрут и заполняется таблица согласно этому маршруту. Из таблицы символы считываются в порядке следования номеров элементов. Ниже приводится пример шифрования информации *с* использованием маршрутов Гамильтона.

Пример. Пусть требуется зашифровать исходный текст

То = <МЕТОДЫ\_\_ПЕРЕСТАНОВКИ>.

Ключ и длина зашифрованных блоков соответственно равны: К=<2,1,1>, L=4. Для шифрования используются таблица и два маршрута, представленные нарис. 3. Для заданных условий маршруты с заполненными матрицами имеют вид, показанный на рис. 4.



Маршрут № 2 Маршрут № 1 Маршрут № 1

Рисунок 4 – Пример шифрования с помощьюмаршрутов Гамильтона

Шаг 1. Исходный текст разбивается на три блока:  
Б1 =<МЕТОДЫ\_П>;

Б2 = <ЕРЕСТАНО>;

БЗ=<ВКИ\*\*\*\*\*>.

Шаг 2. Заполняются три матрицы с маршрутами 2, J,I (рис. 4).

Шаг 3. Получение шифртекста путем расстановки символов в соответствии с маршрутами.

Тl - <ОП\_ТМЕЫДЕСРЕТАОНИ\*КВ\*\*\*\*>.

Шаг 4. Разбиение на блоки шифртекста

Tj = <OП\_T МЕЫД ЕСРЕ ТАОН И\*КВ \*\*\*\*>.

***1.3.5*** *Шифры простой замены.* В них каждый символ открытого текста заменяется символом того же или другого алфавита по определенному правилу. Широко известны и исследованы шифры Цезаря. В шифре Цезаря алгоритм зашифрования Ek определяется ключом k как смещение вправо на k букв в алфавите, а алгоритм расшифрования Dk как соответствующее смещение влево. Примеры шифротекста для k=31 и алфавита – А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я – ЯМБПМЁВЮЙЕГЛЧЖЛХРМА. Такие шифры имеют слабость по отношению к атакам на основе подсчета частот появления букв в шифротексте. Более устойчивыми являются биграммные шифры (замена двух букв) и n-граммные шифры, позволяющие маскировать частоты появления букв. Модификации системы шифрования Цезаря (аффинная система подстановок Цезаря [9, с. 52-53], система Цезаря с ключевым словом [9, с. 53-54], шифрующие таблицы Трисемуса [9, с. 54-56], криптосистема Хилла [9, с. 56-60]) предлагаются на самостоятельное изучение.

Не глядя на простоту, шифры простой замены со своими усложнениями широко использовались и через полторы тысячи лет после Цезаря. Пример – шифр Ришелье (другое название – «посреди мусора»). Усложнение здесь – утверждение сэра Фрэнсиса Бэкона: «Криптотекст не должен вызывать подозрений, а должен выглядеть естественно». Ришелье использовал листы картона с прорезями. Значимыми являлись только буквы, видимые через прорези. Отправитель и получатель имели одинаковые листы картона с прорезями. Один такой лист изображён на рис. 5. Прорези в картоне на рис. 5 показаны крестиками.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1 |  |  |  |  |  |  |  | х |  |  |
| 2 |  |  |  |  |  |  |  |  | х |  |
| 3 |  |  |  |  |  | х |  |  |  |  |
| 4 |  |  |  |  | х | х |  |  |  |  |
| 5 | х |  |  |  |  | х | .х |  | х |  |
| 6 |  | х |  |  |  |  |  |  |  | х |
| 7 |  |  |  |  |  |  |  |  | х | х |

Рисунок 5 – Шифровальный листок Ришелье

Расположение прорезей: (1; 8); (2; 9); (3; 6); (4; 5); (4; 6); (5; 1); (5; 6); (5; 7); (5; 9); (6; 2); (6; 10); (7; 9); (7; 10). Сообщение записывается в прорезях, после чего незаполненные клетки заполняются «мусором» так, чтобы всё сообщение выглядело невинно. Например, из сообщения YOU KILL AT ONCE несложно получить любовный шифротекст

I – L O V E – Y O U

I – H A V E – Y O U

D E E P – U N D E R

M Y – S K I N – M Y

L O V E – L A S T S

F O R E V E R – I N

H Y P E R S P A C E

**1.3.6** **Шифрование RSA.** **1.3.6.1 Элементы теории чисел**. Число *а* называется **простым**, если оно не имеет других натуральных делителей, кроме 1 и *а*. Пример простых чисел: 17, 23. В интернете есть таблицы простых чисел (от 1 до 1000 и от 1 до 10000). Числа *а* и *b* называются взаимно простыми, если наибольший общий делитель этих чисел (*а,b*)=1. Пример: 8 и 9.

Целые числа называются **взаимно простыми**, если они не имеют никаких общих делителей, кроме ±1. Примеры:

14 и 25 взаимно просты – у них нет общих делителей.

15 и 25 не взаимно просты (у них имеется общий делитель 5).

6, 8, 9 взаимно просты – у них нет делителей, общих для всех трёх чисел.

**1.3.6.2. Модулярная арифметика***.* В модулярной арифметике все арифметические действия выполняются как в обычной арифметике с учетом того, что получаемые числа не могут превышать некоторой величины называемой модулем. Пример:

 другая форма записи того же: 

В общем случае . Читается  сравнимо с  по модулю . Это справедливо, если , где . Отсюда  называется вычетом числа  по модулю , . Использование модулярной арифметики позволяет оперировать с очень большими числами, например, при возведении в степень:

.

Пример: 72mod13 = 10 (49=3\*13+10), 74 mod13 = 9 (102=100= 7\*13+9),

78mod13=5 764 801mod13 = 3 ((49mod13)2mod13)2mod13=3, 2 401\*2 401mod13 = 3,

443 446\*13 +3=5 764 798 +3

**1.3.6.3. Алгоритм RSA**. Криптосистемы с открытыми ключами различаются видом односторонних функций. Среди них самыми известными являются системы RSA, Эль-Гамаля и Мак-Элиса. В настоящее время наиболее эффективным и распространенным алгоритмом шифрования с открытым ключом является алгоритм RSA, получивший свое название от первых букв фамилий его создателей: Rivest, Shamir и Adleman.

Алгоритм основан на использовании *операции* возведения в степень модулярной арифметики. Его можно представить в виде следующей последовательности шагов.

Шаг I. Выбираютсядва больших простых числа *р* и *q.*

Шаг 2. Получается открытая компонента ключа *n*:

*n=p\*q.*

Шаг 3. Вычисляется функция Эйлера по формуле:

*f(p,q) = (p-1)(q-1).*

Функция Эйлера показывает количество целых положительных чисел, начиная от 1, которые взаимно просты с *п.*

Шаг 4. Выбирается большое простое число *d*, которое является взаимно простым со значением *f(p,q).*

Шаг 5. Определяется число *е,* удовлетворяющее условию:

*e\*d =1{modf(p,q)}.*

Данное условие означает, что остаток от деления (вычет) произведения *e\*d* на функцию *f(p,q)* равен 1. Число *е* принимается в качестве второй компоненты открытого ключа. В качестве секретного ключа используются числа *d* и *п.*

Шаг 6. Исходная информация, независимо от ее физической природы, представляется в числовом двоичном виде. Последовательность бит разделяется на блоки длиной L бит, где L - наименьшее целое число, удовлетворяющее условию: L>=log2(n+1). Каждый блок рассматривается как целое положительное число *X(i),* принадлежащее интервалу [0,n-1]. Таким образом, исходная информация представляется последовательностью чисел

X(i),i = 1, I.

Значение I определяется длиной шифруемой последовательности.

Шаг 7. Зашифрованная информация получается в виде последовательности чисел Y(i), вычисляемых по формуле:

Y(i) = (X(1))e(mod n).

**Пример** применения метода RSA для криптографического закрытия информации. Примечание: для простоты вычислений использованы минимально возможные числа. Пусть требуется зашифровать сообщение на русском языке «ГАЗ». Для зашифрования сообщения необходимо выполнить следующие шаги:

Шаг 1. Выбирается р= 3 и *q=* 11.

Шаг 2. Вычисляется *п =* 3\*11=33.

Шаг 3. Определяется функция Эйлера

f(p,q) = (3-l)\*(11-l) = 20.

Шаг 4. В качестве взаимно простого числа выбирается число *d = 3.*

Шаг 5. Выбирается такое число *е,* которое удовлетворяло бы соотношению:

(еd = е3) (mod 20) = 1. Пусть е = 7.

Шаг 6. Исходное сообщение представляется как последовательность целых чисел. Пусть букве А соответствует число 1, букве Г – число 4. букве 3 – число 9. Для представления чисел в двоичном коде требуется 6 двоичных разрядов, так как в русском алфавите используются 33 буквы (случайное совпадение с числом *п*). Исходная информация в двоичном коде имеет вид:

000100 000001 001001.

Длина блока L определяется как минимальное число из целых чисел, удовлетворяющих условию: L>=log2(33+i), так как п=33. Отсюда L=6. Тогда исходный текст представляется в виде кортежа X(i)=<4, 1,9>.

Шаг 7. Кортеж X(i) зашифровывается с помощью открытого ключа {7, 33}:

Y(l) = (47) (mod 33) = 16384 (mod 33) = 16;  
Y(2) = (I7) (mod 33) = 1 (mod 33) = 1;  
Y(3) = (97) (mod 33) = 4782969 (mod 33) = 15.

Получено зашифрованное сообщение Y(i) = <16,1, 15>.

**2 ЗАДАНИЕ**

**Подзадание 2.1**. 2.1.1 Изучите пп. 1.1 теоретических сведений и, при необходимости, литературу [1] (с. 9-15), [2-4], [5] (с. 6-9), [6] (с. 2-7), [7], [8, с. 9-15] Активно используйте интернет при встрече с незнакомыми терминами и в других случаях.

2.1.2 Согласно выданному варианту (приложение «Варианты заданий»):

2.1.2.1 Укажите тип и место установки или эксплуатации объекта (ИО), заданного в Вашем варианте задания и кратко опишите его функциональные характеристики и порядок работы с ним. Проведите анализ угроз ИБ в Вашем объекте. Укажите, к какому виду относятся выявленные Вами угрозы.

2.1.2.2 Рассмотрите приоритеты угроз Вашего объекта и кратко объясните, почему Вы назначили именно такие приоритеты.

2.1.2.3 Предложите Ваши методы парирования перечисленных угроз при неограниченном источнике средств на их реализацию (способы защиты информации в анализируемом Вами ИО. Укажите, к какому виду относятся выявленные Вами методы.

**Пример** выполнения подзадания 2.1. Пусть ИО, заданный в Вашем варианте задания, это кассовый суммирующий аппарат (КСА). КСА используются для автоматизации учета, контроля и первичной обработки информации кассовых операций и регистрации ее на печатаемых документах. Основным объектом защиты информации в КСА являются фискальные данные (ФД) – информация о денежных расчетах с населением, проведенных на КСА, необходимая для правильного исчисления налогов и контроля со стороны налоговых органов, подлежащая ежесменной регистрации и долговременному хранению. ФД хранятся в фискальной памяти (ФП) КСА.

**Выполнение** задания:

**1.1 КСА** «Интеграл 301» установлен в малом магазине автозапчастей, в кассовом узле расчёта с покупателями. КСА работает в 2 смены, в каждую со своим кассиром-оператором. Операторы без опыта работы, сразу после курсов подготовки кассиров. Основные функциональные характеристики:

- возможность использования 4х видов оплат;

- количество запрограммированных товаров – 9500 товаров;

- поиск товара по коду, штриховому коду, цене, названию;

- возможность введения алфавитно-цифрового комментария в чек (22 символа);

- возможность обмена информацией с ПЭВМ, ввода информации со сканера штриховых кодов (типа Metrologic MS-6720, MS-951, CCD), электронных весов (типа ВН, ПВ, СП, CAS), считывателя платежной (идентификационной) карты (типа ТС-1) и др.

Для обеспечения работоспособности КСА при кратковременном отключении сетевого питания установлен свинцово-кислотный аккумулятор номинальным напряжением 6 В. Техническое обслуживание и ремонт КСА производит по договору с супермаркетом сторонняя фирма «Забела».

**1.2 Анализ угроз** ИБ КСА. В состав угроз ИБ КСА входят:

а) отказы аппаратно-программного обеспечения КСА (угроза доступности),

б) непреднамеренные ошибки штатных пользователей КСА (кассиров, например, ввод на реальную дату «26.02.2015» ошибочной даты «26.02.2035», что влечёт за собой обязательную замену ФП, (угроза целостности)

в) природные угрозы (стихийные бедствия, магнитные бури, радиоактивные излучения и осадки и др.) (угроза доступности),

г) атаки злоумышленников на ФП КСА (взлом ФП является для владельца КСА наиболее простым способом ухода от налогов) (угроза доступности),

д) кража КСА (угроза целостности) е) и др..

**1.3 Приоритеты угроз** (приоритет 1 – самая важная, приоритет 2 – самая маловажная):

угроза «а», приоритет 1, из-за частых поломок КСА материальный ущерб от них самый высокий,

угроза «б», приоритет 2, ошибки кассиров вследствие их неопытности встречаются часто, но реже, чем поломки КСА, и обходятся дешевле, чем поломки,

угроза «в», приоритет 5, стихийные бедствия, магнитные бури, радиоактивные излучения и осадки и др. в Беларуси – очень редкое явление,

угроза «г», приоритет 3 или 4, материальный ущерб от взлома ФП и ущерб от потери репутации владельца КСА в глазах налоговой инспекции велики, но на взлом ФП владельцы КСА идут крайне редко,

угроза «д», приоритет 3 или 4, материальный ущерб от кражи КСА (стоимость КСА) и ущерб от потери репутации владельца КСА в глазах налоговой инспекции велики, но кражи КСА в Беларуси – очень редкое явление.

**1.4 Способы защиты информации в КСА** (методы парирования угроз):

угроза «а», метод «регламентация»: повышение надёжности КСА у производителя, повышение качества ремонта и технического обслуживания КСА в фирме «Забела»,

угроза «б», метод «регламентация»: дополнительное обучение молодых кассиров, предоставление им во время работы кратковременных перерывов для отдыха,

угроза «в», метод «препятствие»: дополнительное обеспечение мер противопожарной безопасности, экранирование помещений от излучений,

угроза «г», метод «препятствие»: изменение законодательства в части увеличения ответственности за взлом ФП,

угроза «д», приоритет 3 или 4, метод «препятствие»: установка охранных систем («777», «Неман», «Орион», «Бирюза» и системы видеонаблюдения.

**Подзадание 2.2** Для защиты речевой информации ограниченного доступа при проведении переговоров компания, арендующая свои производственные площади, использует специальное помещение – защищённый служебный кабинет или зал (далее – защищённое служебное помещение (ЗСП). Двери и окна ЗСП надёжно защищены от прослушивания техническими средствами защиты информации. Однако дощатая оштукатуренная перегородка, отделяющая ЗСП от незащищённого коридора, не арендуемого компанией и допускающего возможность проникновения в него злоумышленников, даёт возможность слышать невооружённым ухом или с помощью средств технической разведки на коридоре всё, о чём говорят в ЗСП.

2.2.1 Согласно выданному варианту (файл «Варианты заданий») определите, используя данные табл. 1 и табл. 2, стоимость дополнительной кирпичной кладки или дополнительных железобетонных панелей (панели), усиливающих звукоизоляцию стены для обеспечения затухания Q информационного сигнала в стене на частоте 1000 Гц до уровня, не менее указанного в табл. 1:

Таблица 2 – Исходные данные для расчёта

|  |  |  |
| --- | --- | --- |
|  | Материал перегородки | |
|  | одинарный кирпич | Стеновая железобетонная панель ПЖС-65 |
| Размеры одного кирпича | 250\*120\*65 мм | 2985\*585\*100 мм |
| Информация из | СТБ 1160-99 «Кирпич и камни керамические. Технические условия» | Каталог продукции Светлогорского завода железобетонных изделий |
| Средняя цена одного кирпича (одной панели), без транспортных расходов | 0,6 у.е. | 10 у.е. |
| Стоимость укладки звукоизоляцион-онного материала, с учётом стои-мости вспомогательных материалов (раствор, и др.), на один кирпич (одну панель) | 0,03 у.е. | 60 у.е. |

**Пример** выполнения подзадания 2.2. Подвариант 2.1. Пусть для дополнительной звукоизоляции ЗСП, высота которого 3 м, а длина 12 м, используется кирпичная перегородка в полкирпича. Тогда для стены нам понадобится 12 000 : 250 = 48 кирпичей в длину, 3 000 : 65 = 46 кирпичей в высоту, а всего 48 \* 46 = 2208 кирпичей на стену. Следовательно, стоимость дополнительной кирпичной кладки, усиливающей звукоизоляцию стены для обеспечения затухания Q информационного сигнала в стене на частоте 1000 Гц до уровня 48 дБ, составит (при курсе валюты на день расчёта 15 000 рублей за 1 у.е.) и исходных данных из табл. 2

(0,6+0,03)\*2208\*15000 = 20,9 млн. рублей.

Подвариант 2.2. Пусть для дополнительной звукоизоляции ЗСП, высота которого 3 м, а длина 12 м, используются железобетонные панели ПЖС-65 по 3 панели толщиной 100 мм, стоящие друг за другом (всего общая толщина панелей 300 мм). Тогда для стены нам понадобится 12 000 : 585 = 20 панелей в длину, 1 панель в высоту и 3 панели в толщину, всего 20 \* 3 = 60 панелей на стену. Следовательно, стоимость дополнительных панелей, усиливающей звукоизоляцию стены для обеспечения затухания Q информационного сигнала в стене на частоте 1000 Гц до уровня 65 дБ, составит (при курсе валюты на день расчёта 15 000 рублей за 1 у.е.) и исходных данных из табл. 2

(10+60)\*60\*15000 = 63,0 млн. рублей.

**Подзадание 2.3.** 2.3.1 Зашифруйте с помощью шифра перестановок (см. выше п. 1.3.4, пример 1) Вашу фамилию, имя и отчество.

2.3.2 Зашифруйте с помощью шифрующей таблицы (см. выше п. 1.3.4, пример 2) Вашу фамилию, имя и отчество.

2.3.3 Зашифруйте с помощью одиночной перестановки по ключу (см. выше п. 1.3.4) Вашу фамилию, имя и отчество.

2.3.4 Зашифруйте с помощью шифра Цезаря (см. выше п. 1.3.5) Вашу фамилию, имя и отчество.

2.3.5 Зашифруйте с помощью шифровального листка Ришелье (см. выше п. 1.3.5, рис. 5) Вашу фамилию, имя и отчество.

2.3.6 Зашифруйте с помощью маршрутов Гамильтона (см. выше рис. 3, 4) Вашу фамилию, имя и отчество, используя при этом ключ и длину зашифрованных блоков такими же, как указано в примере рис. 3, 4, т. е. соответственно равными: К=<2,1,1, 4>, L=4.

2.3.7 Зашифруйте алгоритмом RSA (см. выше п. 1.3.6) Вашу фамилию, используя при этом числа *p* и *q*, а также открытый ключ *d* такими же, как указано в примере п. 1.3.6, т. е. соответственно равными:

*p* = 3, *q = 11*, *d = 7.*

**Пример** выполнения подзадания 2.3. Пусть фамилия, имя и отчество (ФИО) студента – ГАВРИЛОВ НИКИТА АЛЕКСАНДРОВИЧ.

1) Шифруем ФИО с помощью шифра перестановок. Для этого делим ФИО на блоки по 3 символа в каждом:

ГАВ РИЛ ОВН ИКИ ТАА ЛЕК САН ДРО ВИЧ

Переставляем буквы (символы) в каждом блоке так, что 1-й символ становится 2-м, 3-й – 1м, а 2-й – 3-м:

ВГА ЛРИ НОВ ИИК АТА КЛЕ САН ОДР ЧВИ

Объединяем блоки в готовый шифротекст (зашифрованный текст):

ВГАЛРИНОВИИКАТАКЛЕСАНОДРЧВИ

2) шифруем ФИО с помощью шифрующей таблицы. Для этого записываем ФИО в таблицу (табл. 3) размером 14\*2 (2 строки по 14 столбцов в каждой), сначала в 1-ую строку 1-го столбца, затем во 2-ую строку 1-го столбца, затем в 1-ую строку 2-го столбца, затем во 2-ую строку 2-го столбца и т. д.:

Таблица 3 – таблица для шифрования с помощью шифрующей таблицы

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Г | В | И | О | Н | К | Т | А | Е | С | Н | Р | В | Ч |
| А | Р | Л | В | И | И | А | Л | К | А | Д | О | И |  |

Переписываем (объединяем) в готовый шифротекст сначала в первую строку табл. 3, затем вторую:

ГВИОНКТАЕСНРВЧАРЛВИИАЛКАДОИ

Для большей внешней запутанности шифротекст можно разделить на блоки, например, по 2 символа в каждом:

ГВ ИО НК ТА ЕС НР ВЧ АР ЛВ ИИ АЛ КА ДО И

3) шифруем ФИО с помощью одиночной перестановки по ключу. Для этого записываем ФИО в левую часть таблицы (табл. 4) размером 5\*5 (5 строк по 5 столбцов в каждой), сначала в 1-ую строку 1-го столбца, затем во 2-ую строку 1-го столбца, затем в 3-ю строку 1-го столбца, затем в 4-ю строку 1-го столбца, затем в 5-ю строку 1-го столбца, затем в 1-ую строку 2-го столбца и т. д.:

Таблица 4 – таблица для шифрования с помощью одиночной перестановки по ключу

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Б | Г | У | И | Р |  | Б | Г | И | Р | У |
| 1 | 2 | 4 | 3 | 5 | 1 | 2 | 3 | 4 | 5 |
| Г | О | Т | С | В | Г | О | С | В | Т |
| А | В | А | А | И | А | В | А | И | А |
| В | Н | А | Н | Ч | В | Н | Н | Ч | А |
| Р | И | Л | Д | **\_** | Р | И | Д | **\_** | Л |
| И | К | Е | Р | **\_** | И | К | Р | **\_** | Е |
| Л | И | К | О | **\_** | Л | И | О | **\_** | К |

Вверху над таблицей записываем ключевое слово БГУИР. В правую часть таблицы переписываем левую часть таблицы, меняя в ней местами столбцы: на место 3-го столбца ставим 4-ый, на место 4-го – 5-ый, на место 5-го – 3-ий. Ключевое слово БГУИР при этом принимает вид БГИРУ.

Переписываем (объединяем) в готовый шифротекст сначала 1-ую строку правой части таблицы, затем 2-ую и т. д.:

ГОСВТАВАИАВННЧАРИД\_ЛИКР\_ЕЛИО\_К

Для большей внешней запутанности шифротекст можно разделить на блоки, например, по 5 символов в каждом:

ГОСВТ АВАИА ВННЧА РИД\_Л ИКР\_Е ЛИО\_К

4) Шифруем ФИО с помощью шифра Цезаря. Для этого выбираем ключ k как смещение вправо на k букв в алфавите, например, k=2.

Записываем алфавит в 1-ую строку табл. 5.

Записываем ФИО во 2-ую строку табл. 5.

Таблица 5 – таблица для шифрования с помощью шифра Цезаря

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

Заменяем 1-ую букву ФИО (букву «Г») буквой, смещённой в алфавите на 2 (k=2) позиции вправо (буквой «Е», см. алфавит). Записываем полученную букву «Е» в строку 3 табл. 5, столбец 1.

Повторяем то же для 2-й буквы ФИО (буквы «А»). Получаем букву «В» и записываем её в строку 3 табл. 5, столбец 2 и т. д.

Полученный в строке 3 табл. 5 шифротекст для большей внешней запутанности делим на блоки, например, по 5 символов в каждом:

ЕВДТК НРДПК МКФВВ НЖМУВ ПЁТРД КЩ.

5) Шифруем ФИО с помощью шифровального листка Ришелье. Для этого готовим лист картона с прорезями. Прорези в картоне показаны крестиками:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | Координаты прорезей по оси абсцисс | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Координаты прорезей по оси ординат | 1 | х |  | х | х |  |  |  | х | х |  |
| 2 |  |  | х | х | х | х | х | х | х |  |
| 3 | х | х |  |  |  |  | х |  | х | х |
| 4 | х | х |  |  |  | х | х | х | х |  |
| 5 |  |  |  | х | х |  |  |  |  |  |
| 6 |  |  | х | х |  |  |  |  |  |  |

Расположение прорезей (координаты крестиков, ключ шифрования): (1:1); (1:3); (1:4); (1:8); (1:9); (2:3); (2:4); (2:5); (2:6); (2:7); (2:8); (2:9); (3:1); (3:2); (3:7); (3:9); (3:10); (4:1); (4:2); (4:6); (4:7); (4:8); (4:9); (5:4); (5:5); (6:3); (6:4).

ФИО записывается в прорезях:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | Координаты прорезей по оси абсцисс | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Координаты прорезей по оси ординат | 1 | Г |  | А | В |  |  |  | Р | И |  |
| 2 |  |  | Л | О | В | Н | И | К | И |  |
| 3 | Т | А |  |  |  |  | А |  | Л | Е |
| 4 | К | С |  |  |  | А | Н | Д | Р |  |
| 5 |  |  |  | О | В |  |  |  |  |  |
| 6 |  |  | И | Ч |  |  |  |  |  |  |

Незаполненные клетки заполняются «мусором» так, чтобы всё сообщение выглядело невинно:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | Координаты прорезей по оси абсцисс | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Координаты прорезей по оси ординат | 1 | Г | Р | А | В | И | Й | - | Р | И | С |
| 2 | - | П | Л | О | В | Н | И | К | И | - |
| 3 | Т | А | Р | Е | Л | К | А | - | Л | Е |
| 4 | К | С | У | С | - | А | Н | Д | Р | Е |
| 5 | Й | - | В | О | В | А | - | М | О | С |
| 6 | К | В | И | Ч |  |  |  |  |  |  |

Объединяем) в готовый шифротекст сначала 1-ую строку таблицы, затем 2-ую и т. д. (слово ПЛОВНИКИ не существует, но пусть остаётся для загадочности:

ГРАВИЙ-РИС-ПЛОВНИКИ-ТАРЕЛКА-ЛЕКСУС-АНДРЕЙ-ВОВА-МОСКВИЧ

6) Шифруем ФИО с помощью маршрутов Гамильтона Ключ и длина зашифрованных блоков соответственно равны: К=<2,1,1,2> (маршруты 2, 1, 1, 2), L=4. Для этого делим ФИО на блоки по 8 символов в каждом:

ГАВРИЛОВ НИКИТААЛ ЕКСАНДРО ВИЧ\*\*\*\*\*

Для каждого блока заполняем таблицу рис. 3. Для первого блока ГАВРИЛОВ переставляем буквы по маршруту № 2 (см выше ключ К), получаем РВОВГАЛИ. Для второго блока НИКИТААЛ переставляем буквы по маршруту № 1, получаем КИИНТАЛА. Для третьего блока ЕКСАНДРО переставляем буквы по маршруту № 1, получаем САКЕНДОР. Для четвёртого блока ВИЧ\*\*\*\*\* переставляем буквы по маршруту № 2, получаем \*\*\*ВИЧ\*\*. Объединяем блоки с переставленными буквами в сообщение:

РВОВГАЛИ КИИНТАЛА САКЕНДОР \*\*\*ВИЧ\*\*.

Разбиваем полученное сообщение на блоки длины L=4. Готовый шифротекст выглядит как:

РВОВ ГАЛИ КИИН ТАЛА САКЕ НДОР \*\*\*В ИЧ\*\*.

7) Шифруем ФИО (для примера только первые 3 буквы фамилии, ГАВ) с помощью алгоритма RSA.

Y(l) = (47) (mod 33) = 16384 (mod 33) = 16;  
Y(2) = (17) (mod 33) = 1 (mod 33) = 1;  
Y(3) = (37) (mod 33) = 2187 (mod 33) = 9.

Получено зашифрованное сообщение Y(i) = <16,1, 9>.

**Подзадание 2.4.** Покажите свою осведомлённость в областях, упоминаемых выше в контрольной работе, для чего кратко опишите (1-2 абзаца), что такое или кто такой, и почему мы о них вспомнили в курсе ОЗИ (в контрольной или в конспекте, или вспоминаем в литературе по ОЗИ):

2.4.1 Клод Шеннон, п. 1.3.3,

2.4.2 скитала, п. 1.3.4,

2.4.3 древние греки, п. 1.3.4,

2.4.4 Гай Юлий Цезарь, п. 1.3.5,

2.4.5 Арман Жан дю Плесси Ришелье, п. 1.3.5,

2.4.6 Аббат Иоганнес Трисемус, п. 1.3.5,

2.4.7 Сандерс Лестер Хилл

2.4.8 криптосистема Хилла, п. 1.3.5,

2.4.9 аффинная система подстановок Цезаря, п. 1.3.5.

2.4.10 Блез Виженер

2.4.11 матрица Виженера

2.4.12 Гамильтон, п. 1.3.5,

2.4.13 Эвклид

2.4.14 алгоритм Эвклида

2.4.15 электронная цифровая подпись

2.4.16 Фрэнсис Бэкон

2.4.17 шифр Бэкона

2.4.18 Роберт Мак-Элис

2.4.19 криптосистема Мак-Элиса

2.4.20 гаммирование

2.4.21 Тахер Эль-Гамаль

2.4.22 имитовставка

2.4.23 Гилберт Вернам

2.4.24 Шифр Вернама

2.4.25 DES (Data Encryption Standard)

2.4.26 В. Диффи

2.4.27 М. Хеллман

2.4.28 алгоритм Diffie-Hellman

2.4.29 протокол Diffie-Hellman

2.4.30 Ро́нальд Линн Риве́ст

2.4.31 Ади Шамир

2.4.32 Леонард Макс Адлеман

2.4.33 Однонаправленная функция

2.4.34 Криптосистема Эль-Гамаля

2.4.35 Ламброс Деметриос Калимахос

2.4.36 Зендийская задача

ЛИТЕРАТУРА

1 Голиков, В. Ф., Лыньков, Л. М., Прудник, А. М., Борботько, Т. В. Правовые и организационно-технические методы защиты информации. – Мн.: БГУИР, 2004. – 81 с.

2 Современные технологии защиты информации – Интуит [Электронный ресурс]. – Режим доступа: www.intuit.ru/studies/courses/1162/285/lecture/7164. – Дата доступа 25.05.2015.

3 Основы информационной безопасности и защита ... – Sites [Электронный ресурс]. – Режим доступа: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1. – Дата доступа 25.05.2015.

4 Наиболее распространенные угрозы доступности – Интуит [Электронный ресурс]. – Режим доступа: [www.intuit.ru/studies/courses/10/10/lecture/300. – Дата доступа 25.05.2015](http://www.intuit.ru/studies/courses/10/10/lecture/300.%20–%20Дата%20доступа%2025.05.2015).

5 Борботько, Т. В. Лекции по курсу «Основы защиты информации». – Мн.: БГУИР, 2006. – 81 с.

6 Сечко, Г. В. Конспект лекций по курсу «Основы защиты информации». – Мн.: БГУИР, 2015. – 81 с.

7 Методы и средства защиты информации [Электронный ресурс]. – Режим доступа: abc.vvsu.ru/Books/inform\_tehnolog/page0025.asp. – Дата доступа 25.05.2015.

8 Криштопова, Е. А. Основы защиты информации: методическое пособие. – Мн.: 2012. – 176 с.

9 Романец, Ю.В., Тимофеев, П.А., Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – М.: Радио и связь, 1999. – 328 с.

ПРИЛОЖЕНИЕ: Варианты заданий:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вари-ант | Информационный объект (к заданию 2.1) | К заданию 2.2 | | К заданию 2.4,  позиции в п. 2.4 |
| размеры помещения, м | материал перегородки |
| 1 | Стационарный компьютер, установленный дома у владельца, без подключения к Интернету | высота 3 длина 6 | кирпич в 1 кирпич | 2.4.14, 2.4.1, 2.4.2, 2.4.3 |
| 2 | Стационарный компьютер, установленный дома у владельца, с подключением к Интернету | высота 3 длина 12 | железобетонная панель 4 панели по 100 мм (всего 400 мм) | 2.4.15, 2.4.4, 2.4.5, 2.4.6 |
| 3 | Стационарный компьютер, установленный на работе у владельца, без подключения к сети предприятия и Интернету | высота 3 длина 6 | кирпич в 1,5 кирпича | 2.4.17, 2.4.7, 2.4.10, 2.4.9 |
| 4 | Стационарный компьютер, установленный на работе у владельца, с подключением к сети предприятия и Интернету | высота 3 длина 12 | железобетонная панель 100 мм | 2.4.19, 2.4.12, 2.4.13, 2.4.16 |
| 5 | Компьютерный класс учреждения образования | высота 3 длина 6 | кирпич в 2 кирпича | 2.4.20, 2.4.18, 2.4.21, 2.4.23 |
| 6 | Стационарный компьютер, установленный дома у игромана (фаната компьютерных игр через Интернет) | высота 3 длина 12 | железобетонная панель 3 панели по 100 мм (всего 300 мм) | 2.4.22, 2.4.26, 2.4.27, 2.4.30 |
| 7 | Смартфон, айфон или планшет | высота 3 длина 6 | кирпич в 2,5 кирпича | 2.4.24, 2.4.31, 2.4.32, 2.4.35 |
| 8 | КСА у таксиста | высота 3 длина 6 | железобетонная панель 4 панели по 100 мм (всего 400 мм) | 2.4.25, 2.4.1, 2.4.2, 2.4.3 |
| 9 | Банкомат | высота 3 длина 12 | кирпич в 1 кирпич | 2.4.28, 2.4.4, 2.4.5, 2.4.6 |
| 10 | Электромобиль | высота 3 длина 6 | железобетонная панель 100 мм | 2.4.29, 2.4.7, 2.4.10, 2.4.9 |
| 11 | Флеш-карта | высота 3 длина 12 | кирпич в 1,5 кирпича | 2.4.33, 2.4.12, 2.4.13, 2.4.16 |
| 12 | Банковская кредитная карта | высота 3 длина 6 | железобетонная панель 3 панели по 100 мм (всего 300 мм) | 2.4.34, 2.4.18, 2.4.21, 2.4.23 |
| 13 | Телефонная карта | высота 3 длина 12 | кирпич в 2 кирпича | 2.4.36, 2.4.26, 2.4.27, 2.4.30 |
| 14 | Локальная вычислительная сеть | высота 3 длина 18 | железобетонная панель 4 панели по 100 мм (всего 400 мм) | 2.4.11, 2.4.31, 2.4.32, 2.4.35 |
| 15 | База данных на сервере | высота 3 длина 12 | кирпич в 2,5 кирпича | 2.4.8, 2.4.1, 2.4.2, 2.4.3 |
| 16 | CRM-система | высота 3 длина 18 | железобетонная панель 100 мм | 2.4.17, 2.4.4, 2.4.5, 2.4.6 |
| 17 | Облачные вычисления | высота 3 длина 18 | кирпич в 1 кирпич | 2.4.8, 2.4.7, 2.4.10, 2.4.9 |
| 18 | Микроконтроллер | высота 3 длина 18 | железобетонная панель 3 панели по 100 мм (всего 300 мм) | 2.4.11, 2.4.12, 2.4.13, 2.4.16 |
| 19 | АСУ ТП | высота 3 длина 18 | кирпич в 1,5 кирпича | 2.4.15, 2.4.18, 2.4.21, 2.4.23 |
| 20 | ЕRР-система | высота 3 длина 18 | кирпич в 2 кирпича | 2.4.17, 2.4.26, 2.4.27, 2.4.30 |

Примечания:

К варианту 11 – Ка́рта па́мяти или флеш-ка́рта — компактное электронное запоминающее устройство, используемое для хранения цифровой информации. Современные карты памяти изготавливаются на основе флеш-памяти, хотя принципиально могут использоваться и другие технологии.

К варианту 16 – СRM-система, сокращение от англ. Customer Relationship Management) — прикладное программное обеспечение для организаций, предназначенное для автоматизации стратегий взаимодействия с заказчиками (клиентами), в частности, для повышения уровня продаж, оптимизации маркетинга и улучшения обслуживания клиентов путём сохранения информации о клиентах и истории взаимоотношений с ними, установления и улучшения бизнес-процессов и последующего анализа результатов.

К варианту 17 – Облачные вычисления (англ. cloud computing) – технология рас-пределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис. Термин «Облако» используется как метафора, основанная на изображении Интернета на диаграмме компьютерной сети, или как образ сложной инфраструктуры, за которой скрываются все технические детали. Согласно документу IEEE, опубликованному в 2008 году, «Облачная обработка данных – это парадигма, в рамках которой информация постоянно хранится на серверах в интернете и временно кэшируется на клиентской стороне, например, на персональных компьютерах, игровых приставках, ноутбуках и т. д.»

К варианту 19 – АСУ ТП – автоматизированная система управления технологическим процессом. АСУ ТП сегодня – это сложнейший комплекс, состоящий из персональных и панельных компьютеров, микроконтроллеров, активного и пассивного сетевого оборудования. АСУ ТП являются неотъемлемой частью практически любого производственного процесса на современных предприятиях.

К варианту 20 – ЕRР-система (система класса ERP (Enterprise Resource Planning / управление ресурсами предприятия)) – корпоративная информационная система для автоматизации планирования, учета, контроля и анализа всех основных бизнес-процессов и решения бизнес задач в масштабе предприятия (организации).