**КОНТРОЛЬНАЯ РАБОТА (ред 2017 г)**

по Основам Защиты Информации (ОЗИ)

Часть 1 Угрозы ИБ, защита помещения

**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, 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].

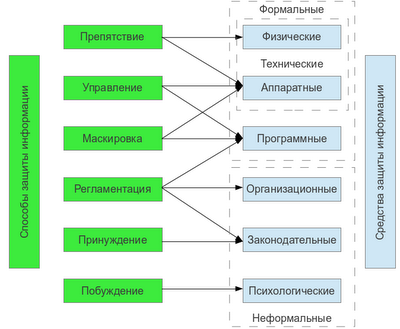
Под **угрозой** ИБ ИО будем понимать возможные воздействия на него, приводящие к ущербу. Некоторое свойство объекта, делающее возможным возникновение и реализацию угрозы, будем называть **уязвимостью**. Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку, – **злоумышленником**. 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. **Классификация угроз и методов их парирования** подробно описана в подразделе 1.3 конспекта [2, с. 4].

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. |  |

**1.1.2 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 (более подробно см. конспект, с. 72.

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 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.

**1.3.3 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 Сложные перестановки.** 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. 8).

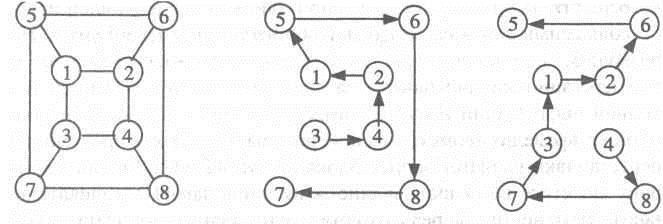


Таблица Маршрут .№ 1 Маршрут № 2

Рисунок 8 – Вариант 8-элементной таблицы и маршрутов Гамильтона

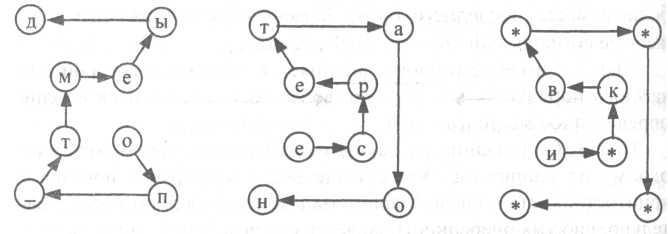
Шаг 3. Считывание символов из таблицы осуществляется по одному из маршрутов. Увеличение числа маршрутов повышает криптостойкость шифра. Маршруты выбираются либо последовательно, либо их очередность задается ключом К.

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. 9.



Маршрут № 2 Маршрут № 1 Маршрут № 1

Рисунок 9 – 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. 9).

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. 10. Прорези в картоне на рис. 10 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 10 – 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.* Простыми называются числа, которые делятся только на самих себя и на 1. Величина этих чисел должна быть больше 200 (в примере, см ниже, числа выбраны меньше 200 для облегчения расчётов).

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.* Взаимно простыми являются такие числа, которые не имеют ни одного общего делителя, кроме 1.

Шаг 4. Выбирается большое простое число *d*, которое является взаимно простым со значением функции Эйлера *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:

(*е*d = *е*3) (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 [26 = (33+*i*)]. 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) = (17) (mod 33) = 1 (mod 33) = 1;  
Y(3) = (97) (mod 33) = 4782969 (mod 33) = 15.

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

**1.4** Объекты промышленной собственности (далее – ОПС) – это изобретения (далее – Из), полезные модели (далее – ПМ), промышленные образцы (далее – ПО), топологии интегральных микросхем, сорта растений (СР), а также такие средства индивидуализации участников гражданского оборота, товаров, работ и услуг, такие, как товарные знаки и знаки обслуживания, географические указания, в том числе наименования мест происхождения товаров и другие результаты интеллектуальной деятельности (ИД) [12].

Одной из наиболее распространенных коммерчески значимых форм правовой таких ОПС, как Из, ПМ, ПО, СР, является патент, который обеспечивает патентообладателю исключительное (монопольное) право на использование ОПС и запрещает всем третьим лицам их использование в любых целях без разрешения патентообладателя. В контрольной работе мы будем рассматривать только патенты на Из.

Чтобы результат ИД охранялся как ОПС, необходимо оформить и подать заявочные материалы (заявку) в уполномоченный орган (Национальный центр интеллектуальной собственности, НЦИС) и пройти процедуру экспертизы и регистрации.

**1.4.1 Составление и оформление заявок на изобретение**. Алгоритм патентования:

– отбор изобретений для патентования; подготовка заявок на выдачу патентов;

– подача заявок в НЦИС и ведение переписки с НЦИС в процессе проведения экспертизы по заявкам на патенты;

– ведение переписки по патентным спорам с административными и судебными органами (при необходимости);

– получение патентов;

– оплата пошлин за юридически значимые действия;

– поддержание в силе заявок на патенты и собственно патентов.

Рассмотрим подробно некоторые из перечисленных этапов, хотя их содержание не всегда можно четко разграничить.

**1.4.2 Подача заявки на изобретение**. Заявка на выдачу патента на Из подается автором Из, нанимателем, если Из служебное, физическим или юридическим лицом, которым автор или наниматель передает на до-говорной основе свое право на подачу заявки или к которому они перешли в соответствии с законодательством Республики Беларусь в наследовании. Она может быть передана через патентного поверенного, зарегистрированного в НЦИС. Заявки, поступившие в НЦИС, назад не возвращаются.

**1.4.2.1 Состав заявки**. Заявка должна содержать:

• заявление о выдаче патента;

• описание изобретения, раскрывающее его с полнотой достаточной для осуществления изобретения (3 экз.);

• формулу изобретения, выражающую его сущность и полностью основанную на описании (3 экз.);

• чертежи и иные материалы, если они необходимы для понимания сущности изобретения (3 экз.);

• реферат (3 экз.);

• доверенность в случае подачи заявки патентным поверенным (1 экз.),

• документ, подтверждающий уплату пошлины (1 экз.) и другие документы (см. «бланк заявления о выдаче изобретения»).

**1.4.2.2 Формула изобретения** – это логическое определение Из совокупностью всех его существенных признаков, служащее для определения объема правовой охраны, предоставляемой патентом [12]. Формула Из печатается на отдельном листе и подписывается заявителем или патентным поверенным. Передачу таких полномочий подтверждает доверенность.

Структура формулы изобретения может быть однозвенной и многозвенной. Однозвенная формула применяется для характеристики одного Из совокупностью признаков, не имеющей развития или уточнения применительно к частным случаям его выполнения или использования [12] и имеет один независимый пункт. **Пример 1:**

**Способ проведения игры с использованием кредитной карточки**, *заключающийся в том, что**проверяют достоверность карточки, определяют возможность проведения игры, проводят игру с помощью электронного игрового устройства и записывают результат игры*, ОТЛИЧАЮЩИЙСЯ ТЕМ, ЧТО упомянутое проведение игры осуществляют автономно и результат игры записывают непосредственно на кредитную карточку с помощью электронного игрового устройства.

В этой формуле объектом Из является «способ проведения игры с использованием кредитной карточки». Существуют следующие виды объектов Из: устройство, способ, вещество, биотехнологический продукт и применение по новому назначению известного ранее устройства, способа, вещества, биотехнологического продукта. В контрольной работе мы будем рассматривать только 2 первых вида как наиболее употребительные для тематики изобретений в области информатики и радиоэлектроники.

При этом под устройством понимается устройство (объекта) конструкции, изделия, их части, а под способом – процесс выполнения действий (операций, приемов) над материальным объектом с помощью материальных объектов, приводящих к созданию новых или изменению известных материальных объектов, или процессы исследования материальных объектов [12]. В США видом Из может быть также программный продукт, в нашей же стране, чтобы запатентовать программный продукт, необходимо патентовать устройство, в котором содержится патентуемая программа.

Из примера 1 следует структура независимого пункта формулы:

• Название изобретения (родовое понятие, отражающее назна-чение Из, аналог объекта Из) [1]. В примере 1 и далее название Из выделено жирным шрифтом.

• Ограничительная часть (включает признаки заявленного объ-екта, совпадающие с признаками наиболее близкого аналога). В примере 1 и далее название эта часть выделена курсивом.

• Переходная фраза (разделительное словосочетание) ОТЛИЧАЮЩИЙСЯ (-АЯСЯ, -ЕЕСЯ) ТЕМ, ЧТО.

• Отличительная часть (отличительный признак) (включает при-знаки, которые отличают изобретение от наиболее близкого аналога). В примере 1 это фраза «упомянутое проведение игры осуществляют авто-номно и результат игры записывают непосредственно на кредитную кар-точку с помощью электронного игрового устройства».

В различных странах формулы Из принято составлять по-разному. Эти формулы могут быть составлены в соответствии с германской (логической) и американской системами описания Из. Обе системы имеют существенные различия, В основу конструкции германской формулы положены два принципа Гартига [14]:

1) формула составляется в виде одного предложения, поскольку Из представляет собой решение только одной технической задачи;

2) формула делится на две части – ограничительную, содержащую признаки общие для прототипа и Из, и отличительную, имеющую новые признаки, характеризующие существо Из и составляющие вместе с ограничительными признаками предмет изобретения. Ограничительная и отличительная части разделяются словами «ОТЛИЧАЮЩИЙСЯ (-АЯСЯ, -ЕЕСЯ) ТЕМ, ЧТО».

Как следует из примера 1, представленная в нем формула Из составлена в точном соответствии с германской (логической) системой описания Из. Она имеет один отличительный признак, поэтому и называется **однозвенной**.

Американская формула включает в себя все возможные варианты осуществления Из. Каждый вариант Из представлен своим пунктом, однако фактически второй, третий и последующие пункты представляют собой точную копию первого пункта и отличаются от него включением характерного отличительного признака варианта Из. Такой прием позволяет защитить Из в том случае, если патентным ведомством аннулируется первый пункт формулы Из. Ограничительные и отличительные признаки в американской формуле Из не разбиваются, а приводятся вперемежку или подряд. Поэтому американская формула Из называется инвентарной.

Случаев аннулирования белорусским патентным ведомством (НЦИС) первого пункта формулы Из практически не бывает. Кроме того, германская система описания Из легко поддается стандартизации, что является особо ценным при подготовке специалиста в техническом вузе. Поэтому студентам НЕОБХОДИМО ИСПОЛЬЗОВАТЬ только германскую систему.

**Многозвенная формула** применяется для характеристики одного Из с развитием и/или уточнением совокупности его признаков применительно к частным случаям выполнения или использования изобретения. Существует ряд вариантов такой формулы.

**Вариант 1. Многозвенная с одним независимым пунктом** (применяется для характеристики одного изобретения с развитием и/или уточнением совокупности его признаков применительно к частным случаям выполнения или использования изобретения). Схематично формула Из имеет следующий вид:

• независимый пункт формулы:

• зависимые пункты формулы. **Пример 2** (рассматриваемой формулы, для устройства, обратите внимание – в пунктах 2, 3 вместо полного приведен сокращенный вариант наименования Из (устройство)):

1. Устройство охлаждения компьютера, содержащее первичный контур переноса тепла, вторичный контур переноса тепла, конденсатор, выполненный с возможностью охлаждения первичным контуром переноса тепла, и испаритель для охлаждения компьютерного оборудования, ОТЛИЧАЮЩЕЕСЯ ТЕМ, ЧТО флюид для переноса тепла является летучим флюидом, в качестве которого использован диоксид углерода так, что температура летучего флюида, принимаемого в испарителе, находится в пределах от 12 до 16°С.

2. Устройство по п. 1, ОТЛИЧАЮЩЕЕСЯ ТЕМ, ЧТО устройство выполнено с возможностью размещения относительно компьютерного оборудования так, что испаритель прилегает к компьютерному оборудованию, подлежащему охлаждению.

3. Устройство по п. 1, ОТЛИЧАЮЩЕЕСЯ ТЕМ, ЧТО дополнительно содержит компьютерный шкаф для размещения компьютерного оборудования

**Вариант 2. Многозвенная с несколькими независимыми пунктами** (применяется для характеристики группы изобретений, например, способ и устройство, объединенных общим изобретательским замыслом). Схематично формула Из имеет следующий вид:

- независимый пункт формулы;

- независимый пункт формулы. Пример такой формулы приведен в [12, с. 28].

**Вариант 3. Многозвенная с несколькими независимыми пунктами** (применяется для характеристики группы изобретений, объединенных об-щим изобретательским замыслом) и зависимыми от соответствующих независимых пунктов. Схематично формула Из имеет следующий вид:

- первый независимый пункт формулы:

- зависимые пункты от первого независимого пункта формулы:

- независимый пункт формулы:

зависимые пункты от второго независимого пункта формулы. Пример такой формулы приведен в [12, с. 29].

**1.4.2.3. Реферат** представляет собой сокращенное изложение содержания раздела «Описания изобретения» патента, включающее название, характеристику области техники, к которой относится изобретение и область применения, если это не ясно из названия, характеристику сущности с указанием достигаемого результата. Сущность изобретения описывают путем такого свободного изложения формулы, при котором сохраняются все существенные признаки независимого пункта формулы изобретения.

Он должен быть четким и сжатым, насколько это позволяет техническое описание. Не следует использовать фразы, которые являются очевидными, такие например как: данное описание касается…, изобретение, определяемое в данном описании… . Реферат не должен содержать ссылок на предполагаемые достоинства или ценности изобретения, а также на теоретическую возможность его применения. Реферат может содержать при необходимости чертеж. В реферате следует применять стандартизованные термины, а при их отсутствии – наиболее употребляемые, принятые в научной и технической литературе, соблюдая в тексте единство терминологии.

**Пример составления реферата (устройство):**

ПОЧТОВАЯ СЕКЦИЯ

Изобретение относится к почтовому оборудованию и может быть использовано, в частности, для установки в подъездах жилых многоквартирных домов.

Патентуется почтовая секция, которая содержит корпус с размешенными в нем наклонными полками (ячейками) с индивидуальными запирающимися дверцами. Корпус шарнирно закреплен на вертикальной опорной пластине. Каждая ячейка выполнена так, что наклонная полка со стороны дверцы направлена вверх. Изобретение позволяет исключить возможность непредусмотренного доступа к корреспонденции и повысить удобство пользования.

**Пример составления реферата (способ)**

СПОСОБ РАЗМЕЩЕНИЯ РЕКЛАМЫ ТОВАРОВ И УСЛУГ

Изобретение относится к области рекламы на различных предметах или в них, в частности на бумажных изделиях, а именно на конвертах.

Патентуется способ размещения рекламы товаров и услуг, который заключается в том, что в верхней части передней наружной поверхности конверта закрепляют несколько карманов, в которых размещают рекламные вкладыши с плоским изображением и/или объемные рекламные вкладыши. На наружной поверхности клапана, на задней наружной и передней наружной поверхности конверта, на передней и задней наружной и внутренней поверхности каждого из карманов, а также на обеих поверхностях реклам-ных вкладышей с плоским изображением и объемных рекламных вкладышей наносят текст и/или графическое изображение, и на любой из указанных наружных поверхностей размещают легко стираемое покрытие. Следовательно, имеет место повышение эффективности размещения рекламы.

*Обратите внимание на то, что название реферата представляет собой полное наименование Из из независимого пункта формулы, выделенное в примерах 1 и 2 жирным шрифтом и не включает ограничительную часть того же пункта,*

**1.4.2.4 Заявление о выдаче патента.** Заявление представляется по установленной НЦИС форме (см. сайт НЦИС). Образец заполнения заявления при заполнении его автором приведен в [12, с. 218].

**1.4.3** **Патентная информация и патентные исследования. 1.4.3.1 Патент** на изобретение **удостоверяет** авторство, приоритет изобретения и исключительное право на его использование. Объем правовой охраны, предоставляемой патентом на изобретение, определяется формулой изобретения. Перед подачей заявки на изобретение в патентный орган заявитель должен провести ***патентные исследования*** с целью оценки новизны и уровня техники. Для создания эффективного поискового инструмента и классификации изобретений используются индексы **МПК – международной патентной классификации**. Патентный документ имеет унифицированную структуру и содержит два типа информации: библиографическую информацию и техническую информацию.

***Библиографическая информация*** включает: 1. Дату, наименование и адрес публикующего ведомства. 2. Лица или компании, имеющие отношение к патенту (изобретатель, обладатель патентного права, представитель или патентный поверенный). 3. Классификационные символы МПК и в некоторых случаях также символы национальной патентной классификации. 4. Название изобретения, реферат описания изобретения и основной чертеж или химическую формулу. Каждый элемент из библиографических данных, находящихся на первой странице патентного документа, идентифицируется двузначным цифровым кодом ИНИД (Международные коды для идентификации данных).

***Техническая информация*** включает: 1. Краткое состояние уровня техники, насколько это известно автору. 2. Детальное описание изобретения, изложенное таким образом, чтобы специалист в данной области был в состоянии осуществить это изобретение. 3. Один или несколько чертежей (или химическую формулу), наглядно иллюстрирующих функционирование изобретения. 4. Формулу, которая определяет объем изобретения.

**Описание изобретения** наряду с формулой изобретения и графическими материалами (если они необходимы) является основным документом на выдачу патента. Оно представляет собой технико-правовой документ и должно полностью раскрывать техническую сущность изобретения, а также содержать достаточную информацию для дальнейшей разработки объекта изобретения. Кроме того, описание изобретения должно давать точное и ясное представление о новизне, изобретательском уровне и промышленной применимости изобретения.

Описание *начинается* с названия изобретения и указания индекса или индексов рубрики действующей редакции МПК, к которой относится заявляемое изобретение и содержит следующие разделы: 1 Область техники, к которой относится изобретение. 2. Уровень техники. 3. Сущность изобретения. 4. Перечень фигур чертежей, если они прилагаются, с кратким указанием на то, что изображено на каждой из них. Если представлены иные материалы, поясняющие сущность изобретения, то перечисляют их. 5. Сведения, подтверждающие возможность осуществления изобретения. При *этом оценка новизны и изобретательского уровня осуществляется в сравнении с уровнем техники*, для определения которого проводится информационный поиск.

В разделе **Уровень техники** приводятся сведения об аналогах и прототипах. *Аналог* изобретения – это известное до даты приоритета средство того же назначения, совокупность признаков которого сходна с совокупностью существующих признаков изобретения. Приоритет изобретения устанавливается по дате поступления в патентный орган надлежащим образом оформленной заявки. Если в процесс экспертизы установлено, что идентичное изобретение имеет одну и туже дату приоритета, то патент может быть выдан по заявке, по которой доказана более ранняя дата ее отправки в патентный орган.

За *прототип* изобретения принимается аналог наиболее близкий по совокупности признаков. К приводимым сведениям о каждом из аналогов, в то числе о прототипе относятся библиографические данные источника информации, в котором он раскрыт, *признаки аналога с указанием тех из них, которые совпадают с существенными признаками заявляемого изобретения*, а также указание причин препятствующих получению требуемого технического результата. Если аналогов несколько, то последним описывается прототип. Возможность получения указанного в разделе **Сущность изобретения** технического результата показывается путем описания непосредственно в материалах заявки средства для его достижения или методов его получения, либо указанием на известность такого средства или метода.

**1.4.3.2 Патентные исследования (патентный поиск)** – это исследования технического уровня и тенденций развития объектов техники для обеспечения высокого технического уровня и конкурентоспособности объекта техники, использования современных научно-технических достижений и исключения неоправданного дублирования исследований разработок на ос-нове патентной и другой информации. Патентные исследования проводятся при: 1. Разработке научно-технических прогнозов для перспективного планирования. 2. Разработке планов развития науки и техники. 3. Составлении заявок на разработку и освоение продукции. 4. Создании объектов техники (научные исследования и разработка). 5. Освоении и производстве продукции.

При проведении патентных исследований используются все доступные источники патентной и другой научно-технической информации. Порядок проведения патентных исследований: 1. Разработка программы (ре-гламента) исследований; 2. Поиск и отбор патентной и научно-технической информации; 3. Анализ результатов исследований.

Этапы разработки регламента поиска: 1. Определение предмета исследований (объект в целом, его составные части, или элементы). 2. Определение стран (фирм) поиска. 3. Определение видов информационных источников; 4. Определение глубины поиска. 5. Определение примерного классификационного индекса МПК с помощью алфавитно-предметного указателя (АПУ) к МПК (МКИ), включающего перечень ключевых понятия соответствующих индексов системы классификации МПК; 6. Уточнение классификационного индекса с помощью соответствующего индекса раздела МПК.

**1.4.3.3 Порядок поиска патентных документов** в базе данных Патентного ведомства США. **1.4.3.3.1 Вход** на главную страницу сайта Патентного ведомства США по адресу: http://www.uspto.gov/. В открывшемся окне нужно найти Search for Patent, затем в появившемся меню Searching Full Text Patents (Since 1976) выбрать Patent Number Search. Более сложный поиск может быть выполнен с помощью имеющихся на сайте Патентного ведомства США подсказок (хелпов)

**1.4.3.3.2 Альтернативный** вариант: набрать номер патента в любом поисковике в виде: 7,181,346 (например).

**2 ЗАДАНИЕ**

**Подзадание 2.1**. 2.1.1 Изучите пп. 1.1 теоретических сведений и, при необходимости, литературу [1] (с. 9-15), [2], [3-5], [6] (с. 6-9),, [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 электромобиль. Электромобиль – автомобиль, приводимый в движение одним или несколькими электродвигателями с питанием от автономного источника электроэнергии (аккумуляторов, топливных элементов и т. п.), а не двигателем внутреннего сгорания (ДВС). Отсутствие вредных выбросов от ДВС делает электромобиль самым экологичным транспортным средством.

**Выполнение** задания: **В.2.1.1** Электромобиль City EV (внутригородской электромобиль) используется его владельцем для поездок по городу или хранится в его гараже. Основные функциональные характеристики:

- максимальная скорость 500 км/час;

- максимальный пробег без заправки аккумуляторов 600 км;

- управление с помощью бортовой ПЭВМ (рис. 1);

Рисунок 1 – Бортовой компьютер электрического Рисунок 2 – Блокировка троянцем возможности

седана Model S компании Tesla Motors выбора водителем каких-либо альтернативных

каналов автомобильной аудиосистемы

- доступ в интернет через бортовую ПЭВМ;

- советы водителю от бортовой ПЭВМ по навигации с учётом пробок и объездных путей;

- присвоение имени; владелец электромобиля Model S может присвоить своему любимцу официальное имя, которое будет отображаться в мобильном приложении на смартфоне и на экране автомобильного компьютера, в разделе «About Your Tesla»;

- ночной режим энергосбережения и возможность удалённого подключения со смартфона так, что электромобиль не выходит из спящего режима;

- ежедневник: запланированные мероприятия из ежедневника на смартфоне выводятся на автомобильный экран; если на смартфоне указать место мероприятия, то не нужно повторно вводить координаты в навигационную систему;

- регулировка пневматической подвески по памяти о прошлых действиях водителя на том или ином участке дороги (по координатам); функция актуальна для тех электромобилей, которые оборудованы, собственно, этим механизмом; например, если водитель каждый раз при подъезде к дому увеличивал клиренс машины, чтобы преодолеть препятствие, то Model S теперь будет делать это автоматически;

- запуск электромобиля со смартфона; если водитель забыл автомобильный брелок («ключ зажигания»), то теперь может включить машину, введя пароль в мобильном приложении.

**В.2.1.2 Анализ угроз** ИБ электромобиля. В состав угроз ИБ электромобиля входят:

а) отказы аппаратно-программного обеспечения бортовой ПЭВМ (угроза доступности);

б) проникновение вредоносного программного обеспечения (ВПО) в бортовую ПЭВМ через интернет (угроза целостности, рис. 2);

в) атаки злоумышленников на бортовую ПЭВМ с целью перехвата управления электромобилем во время его движения (угроза доступности);

г) угон электромобиля со стоянки с помощью кодграббера (угроза целостности и конфиденциальности одновременно);

д) электромагнитное излучение (ЭМИ) от мощного инвертора напряжения (МИН, рис. 3), которое создаёт сильные помехи работе бортовой ПЭВМ [9]; ЭМИ возникает от заземлителя (поз. 61, рис. 4) на кейсе (поз. 22) инвертора и от основной платы (поз. 62) МИН; на практике относительно широкий интервал между первым и вторым креплениями приводит к возникновению паразитной индуктивности между площадкой заземлителя 61 цепи управления и кейсом инвертора; при высоких частотах переключения, используемых инверторами напряжения, эти паразитные индуктивности приводят к образованию ЭМИ (угроза целостности);

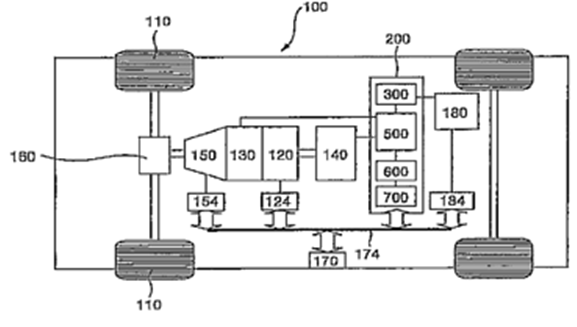
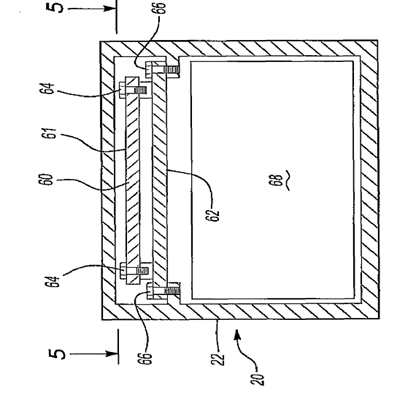
 

Рисунок 3 – Расположение МИН (поз. 200) на Рисунок 4 – Кейс (поз. 22) инвертора мощности электромобиле (вид снизу) МИН в разрезе

е) и менее значимые другие.

**В.2.1.3 Приоритеты угроз** (приоритет 1 – самая важная, приоритет 5 – самая маловажная):

угроза «д», приоритет 1, электромагнитное излучение действует на бортовой компьютер постоянно, информация постоянно теряется;

угроза «а», приоритет 2, из-за частых поломок аппаратно-программного обеспечения бортовой ПЭВМ материальный ущерб от них самый высокий,

угроза «г», приоритет 3, угоны случаются реже, чем поломки аппаратно-программного обеспечения, но обходятся дороже, чем поломки, кроме того, материальный ущерб от угона электромобиля высокий, случаи угона не редкость в условиях всеобщей технической грамотности молодёжи в Беларуси, широко использующей подсказки интернета для изготовления кодграббера,

угроза «б», приоритет 4, проникновение ВПО в ПЭВМ легко блокируется качественными антивирусными программами,

угроза «в», приоритет 5, хакерские атаки на бортовую ПЭВМ с целью перехвата управления электромобилем во время его движения наблюдались только за рубежом, в Беларуси таких случаев пока не было.

**В.2.1.4 Способы защиты информации в электромомобиде** (методы парирования угроз):

угроза «а», метод «регламентация»: повышение надёжности бортовой ПЭВМ у производителя, повышение качества ремонта и технического обслуживания ПЭВМ при обслуживании на СТО (станции технического обслуживания),

угроза «б», метод «препятствие»: установка антивирусного программного обеспечения,

угроза «в», метод «препятствие»: установка системы обнаружения вторжений,

угроза «г», метод «препятствие»: применение устройств блокировки работы кодграббера [10],

угроза «д», метод «препятствие»: объединение креплений (поз. 64 на рис. 4) и вторых креплений (поз. 66 на рис. 4) в единое крепление (поз. 76 на рис. 6), что позволяет уменьшить паразитную индуктивность между заземлителем (поз. 61 на рис. 4) платы (поз. 60 на рис. 4, платы цепи управления) и кейсом (поз. 22 на рис. 4) [9].

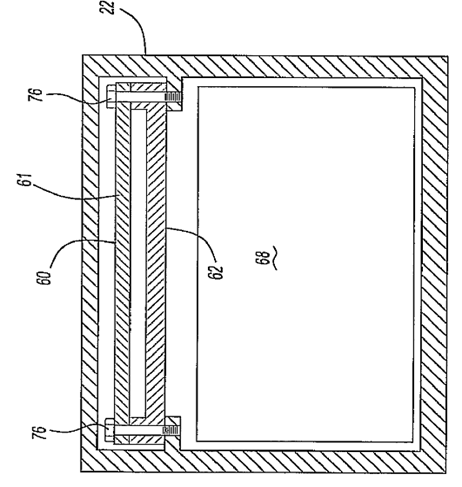
 

Рисунок 5–Действующий макет устройства для Рисунок 6– К поячнению минимизации ЭМИ путём

нейтрализации кодграббера [10] объединения двух креплений в единое [9]

**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 Вашему варианту и исходным данным табл. 2 определите 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 некого уровня, заданного в «Плане организационно-административных мероприятий по защите информации в КОМПАНИИ». Перед расчётом стоимости кирпичной кладки внимательно изучите рис. 7.

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 1,95 рубля за 1 у.е.) и исходных данных из табл. 2

(0,6+0,03)\*2208\*1,95 = 2 713 рублей.

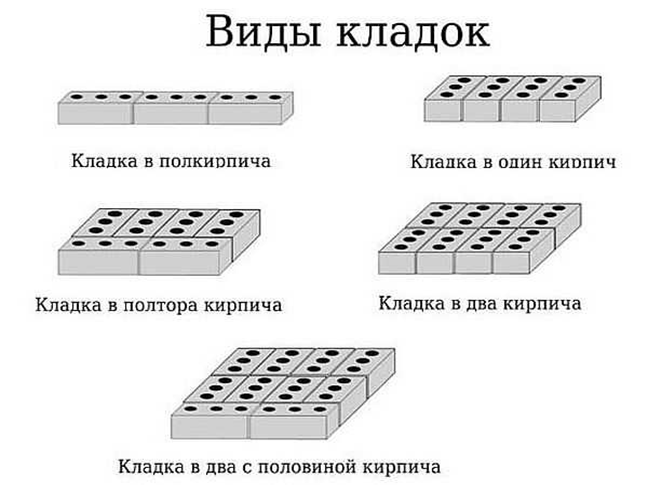
 

Рисунок 7–Варианты кирпичной кладки

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 1,95 рубля за 1 у.е.) и исходных данных из табл. 2

(10+60)\*60\*1,95 = 8 190 рублей.

**Подзадание 2.3.** 2.3.1 Изучите пп. 1.3 теоретических сведений и, при необходимости, литературу (список в ПЗ № 1) [2, подраздел 5.3, с. 72–77), [11, с. 131–138]. 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.** 2.4.1 Изучите пп. 1. теоретических сведений и, при необходимости, литературу (список в ПЗ № 1) [2, подраздел 6.2, с. 93–99, 6.3, с. 99–105), [14, нужные страницы выдаются в виде файла «Малёнова Е сокр»]. Согласно форме бланка «Регламент поиска» (выдаётся) составить регламент поиска патента США номера, заданного в Вашем варианте, на тему «Объекты промышленной собственности» (инженер по патентной и изобретательской работе – Вы, руководитель подразделения-исполнителя работы и научный руководитель темы – произвольные лица, одинаковые или разные). Указания к заданию 2.4.1:

а) Предмет поиска (в столбце 1 таблицы) совпадает с темой.

б) Шифр темы – любой.

в) Классификационные рубрики (МПК) в столбце 4 таблицы заполняются после проведения поиска и берутся из найденного патента.

**Подзадание 2.4.2** Проведите патентный поиск в Интернете согласно подготовленному регламенту.

**Подзадание 2.4.3** Составьте по форме бланка «Регламент поиска» (п. 2.4.1). Указания к подзаданию 2.4.3:

а) Наименование темы в регламенте и титульном листе отчета, а также в столбцах 1 форм 1 и 2 отчета должны совпадать.

б) Найденный патент должен быть записан в столбце 2 бланка «Регламент поиска» (п. 2.4.1) по образцу: *США 7,481,946, C04B 35/26; H01F 1/34,* а в столбце 3 формы 1 по образцу: *TDK Corporation (Tokyo, JP). — № 10/529,333; Заявл. 26.12.2003; Опубл. 29.07.2004.*

в) Название изобретения должно быть записано в столбце 4 бланка «Регламент поиска» (п. 2.4.1) по-английски и по-русски, например: Emissions blocking apparatus – устройство блокирования излучений.

г) В бланке «Регламент поиска» (п. 2.4.1) записываются сведения о публикациях по теме найденного патента, в т. ч. в столбце 2 – название опубликованной статьи, например: *Relationship between magnetic properties and microwave-absorbing characteristics of NiZnCo ferrite composites,* в столбце 3 – автор (ы), например: *S.B. Cho, D.H. Kang, J.H. Oh*, ив столбце 4 – название, год, том, номер и страницы источника, где опубликована статья, например: *Journal of materials science — 1996. —Vol.31 — P.4719-4722.* Сведения о публикациях по теме найденного патента содержатся в патенте в разделе **References Cited** [**[Referenced By]**](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2Fsearch-adv.htm&r=0&f=S&l=50&d=CR02&Query=ref/6,359,581)**,** подразделе **Other References,** например,

Other References: «Seminar on Recent Trends and Examples of Developments in Electromagnetic Wave Absorbers and Shield Materials», Kogyo Gijutsukai ed., Dec. 17, 1998 (Partial Translation)

Если такого подраздела в патенте нет, то столбцы 2-4 бланка «Регламент поиска» (п. 2.4.1) не заполняются. Если какие-либо сведения из перечисленных выше сведений о публикациях в патенте отсутствуют, то они отсутствуют и в бланке «Регламент поиска» (п. 2.4.1). Например, вышеприведенная фраза «Seminar on Recent Trends and Examples of Developments in Electromagnetic Wave Absorbers and Shield Materials, Kogyo Gijutsukai ed., Dec. 17, 1998 (Partial Translation)» полностью помещается в столбец 4 бланка «Регламент поиска» (п. 2.4.1), а столбцы 2 и 3 того же бланка применительно к данной публикации остаются пустыми

**Подзадание 2.4.4**  Найденный патент и чертежи к нему в электронном виде приложить к выполненной работе. Отметить в копии найденного документа (выделением и подписью – что это?) в найденном документе следующие части (если таковые имеются):

а) Библиографическую часть, в т. ч.: а1) дату установления приоритета; а2) автора (ов); а3) патентообладателя; а4) индекс МПК; а5) название; а6) реферат.

б) Техническую информацию, в т. ч.: б1) отсылки к родственным заявкам; б2) уровень техники, в т. ч. б.2.1) область техники, к которой относится изобретение; б2.2) описание (обзор) известного уровня техники;б2.3) аналоги и прототипы изобретения; б2.4)критика прототипа; б2.5) сущность (резюме) изобретения; б2.6) краткое описание чертежей; б2.7) подробное описание изобретения; б2.8) формулу и определить, однозвенная или многозвенная формула. Примечания:

образец выделения может быть любым, но понятным, например,

United States Patent 7,181,346

Kleist , et al. February 20, 2007

System and method for assessing the people and property impact of weather

При выполнении задания использовать материал «Перевод американских патентов на русский язык» выданного (п. 2.4.1) файла «Малёнова Е сокр».

**Подзадание 2.4.5** Выделить в формуле ограничительную и отличительную части, независимые и зависимые пункты.

**Подзадание 2.4.6**  Перевести на русский название и части **Abstract** и **Claims**найденного патента, описать по-русски сущность запатентованного ОПС. **2.4.6.1 Вариант** качественного перевода: использовать словарь или автопереводчик из интернета. Для перевода сложных грамматических конструкций используйте выданный (п. 2.4.1) файл «Малёнова Е сокр»

**2.4.6.2 Вариант** некачественного автоперевода (нуждающегося в правке), зато быстрого: выполнить п. **1.4.3.3.2.** В полученном после выполнения пункта окне (см пример ниже) нажать выделенную ниже жёлтым фразу «Перевести эту страницу», дождаться автоперевода и скопировать его.

Patent US7181346 - System and method for assessing the people and ...

<https://www.google.ch/patents/US7181346> Перевести эту страницу

Veröffentlichungsnummer, US7181346 B1. Publikationstyp, Erteilung. Anmeldenummer, US 11/095,345. Veröffentlichungsdatum, 20. Febr. 2007. Eingetragen ...

**3 ВАРИАНТЫ ДЛЯ ВЫПОЛНЕНИЯ ЗАДАНИЙ**

К заданиям 2.1, 2.2

|  |  |  |  |
| --- | --- | --- | --- |
| Вари-ант | Информационный объект (к заданию 2.1) | К заданию 2.2 | |
| 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 | Стационарный компьютер, установленный дома у владельца, с подключением к Интернету | высота 3 длина 12 | железобетонная панель 4 панели по 100 мм (всего 400 мм) |
| 3 | Стационарный компьютер, установленный на работе у владельца, без подключения к сети предприятия и Интернету | высота 3 длина 6 | кирпич в 1,5 кирпича |
| 4 | Стационарный компьютер, установленный на работе у владельца, с подключением к сети предприятия и Интернету | высота 3 длина 12 | железобетонная панель 100 мм |
| 5 | Компьютерный класс учреждения образования | высота 3 длина 6 | кирпич в 2 кирпича |
| 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) |
| 7 | Смартфон или айфон с мобильной операционной системой (указать систему) | высота 3 длина 6 | кирпич в 2,5 кирпича |
| 8 | Кассовый суммирующий аппарат | высота 3 длина 6 | железобетонная панель 4 панели по 100 мм (всего 400 мм) |
| 9 | Банкомат | высота 3 длина 12 | кирпич в 1 кирпич |
| 10 | Сайт или веб-страница | высота 3 длина 6 | железобетонная панель 100 мм |
| 11 | Флеш-карта | высота 3 длина 12 | кирпич в 1,5 кирпича |
| 12 | Банковская кредитная карта | высота 3 длина 6 | железобетонная панель 3 панели по 100 мм (всего 300 мм) |
| 13 | Телефонная карта (карта для таксофона) | высота 3 длина 12 | кирпич в 2 кирпича |
| 14 | Локальная вычислительная сеть | высота 3 длина 18 | железобетонная панель 4 панели по 100 мм (всего 400 мм) |
| 15 | База данных на сервере | высота 3 длина 12 | кирпич в 2,5 кирпича |
| 16 | CRM-система | высота 3 длина 18 | железобетонная панель 100 мм |
| 17 | Облачные вычисления | высота 3 длина 18 | кирпич в 1 кирпич |
| 18 | Микроконтроллер | высота 3 длина 18 | железобетонная панель 3 панели по 100 мм (всего 300 мм) |
| 19 | АСУ ТП | высота 3 длина 18 | кирпич в 1,5 кирпича |
| 20 | ЕRР-система | высота 3 длина 18 | кирпич в 2 кирпича |
| 21 | Станок с ЧПУ | высота 3 длина 18 | кирпич в 2,5 кирпича |
| 22 | Электронная почта | высота 3 длина 24 | железобетонная панель 100 мм |
| 23 | Проект «Электронная школа» | высота 3 длина 24 | кирпич в 1 кирпич |
| 24 | Аэропорт | высота 3 длина 24 | железобетонная панель 3 панели по 100 мм (всего 300 мм) |
| 25 | Учреждение здравоохранения (поликлиника или частный медицинский центр или станция скорой помощи или больница или роддом) | высота 3 длина 24 | кирпич в 1,5 кирпича |
| 26 | Проект «Электронное правительство» (направления взаимодействия G2C/С2G) | высота 3 длина 24 | кирпич в 2 кирпича |

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.

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).

К варианту 26 – Электронное правительство представляет собой сложный комплекс средств, позволяющих осуществлять взаимодействие между органами государственного и местного управления, а также самоуправления, гражданами и субъектами коммерческой деятельности и предполагает три направления взаимодействия:

G2B/B2G (government to business, государство – бизнес/бизнес – государство),

G2G (government to government, государство – государство) и

G2C/С2G (government to citizens, государство – граждане/граждане – государство).

К подзаданию 2.4 варианты патентов выдаются индивидуально каждой группе

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 Насонова, Н. В. Конспект по курсу «Основы защиты информации». – Минск: БГУИР, 2017. –176 с.

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

4 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.

5 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).

6 Борботько, Т. В. Лекции по курсу «Основы защиты информации». – Минск: БГУИР, 2006. – 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. – Минск: ИИТ БГУИР, 2012. – 176 с.

9 US патент № 7,911,806, кл. Н05K 9/00, патентообладатель Hitachi,Ltd, заявка № 11/864,341 от 28.09.2007, приор. 02.04.2009, публ. 22.03.2011, Funato et al, Method and apparatus for reducing EMI emissions from a power invertor.

10 Дубина, С.С., Козлов, К.С., Сечко, Г.В., Чернецкий, А.М. Обеспечение целостности информации в автосигнализации мобильных объектов // Международная науч.-техн. конф., приуроченная к 50-летию МРТИ–БГУИР (Минск, 18–19 марта 2014 года): материалы конф. в 2 ч. – Ч. 1 / редкол.: А. Н. Осипов [и др.]. – Минск: БГУИР, 2014. – 451 с. – С. 384–385.

11 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.

12 Герасимова, Л. К. Основы управления интеллектуальной собственностью: учеб. пособие. – Минск: Изд-во Гревцова, 2011. – 256 с.

13

14 Малёнова, Е. Д., Матвеева, Л. А. Перевод патентов США и Великобритании. От теории к практике. – Омск: Изд-во Омского гос ун-та, 2008. – 144 с.