Название учреждения, в котором выполнялась данная диссертационная работа

На правах рукописи

Фамилия Имя Отчество

Название диссертационной работы

Специальность XX.XX.XX ”—
«Название специальности»

Диссертация на соискание учёной степени [0]
кандидата физико-математических наук

Научный руководитель:
уч. степень, уч. звание
Фамилия Имя Отчество

Город ”— 20XX

ЗМІСТ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

СЛОВАРЬ ТЕРМИНОВ

ВСТУП

Использовать можно в двух системах:

Первый вариант — это выполняются первые 8 работ и получают нужную оценку.

Второй вариант — каждое задание добавляет балы, общая сумма балов определяет итоговую оценку. (Данная система более правильна и гибка, но требует набирать балы за работу)

ПРАКТИЧНА РОБОТА 1

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мета роботи: Изучение способов и основных концепций ИБ.

Теоретические ведомости

1. Основные понятия информационной безопасности

Обеспечение защиты информации волновало человечество всегда. В процессе эволюции цивилизации менялись виды информации, для её защиты применялись различные методы и средства.

Процесс развития средств и методов защиты информации можно разделить на три относительно самостоятельных периода:

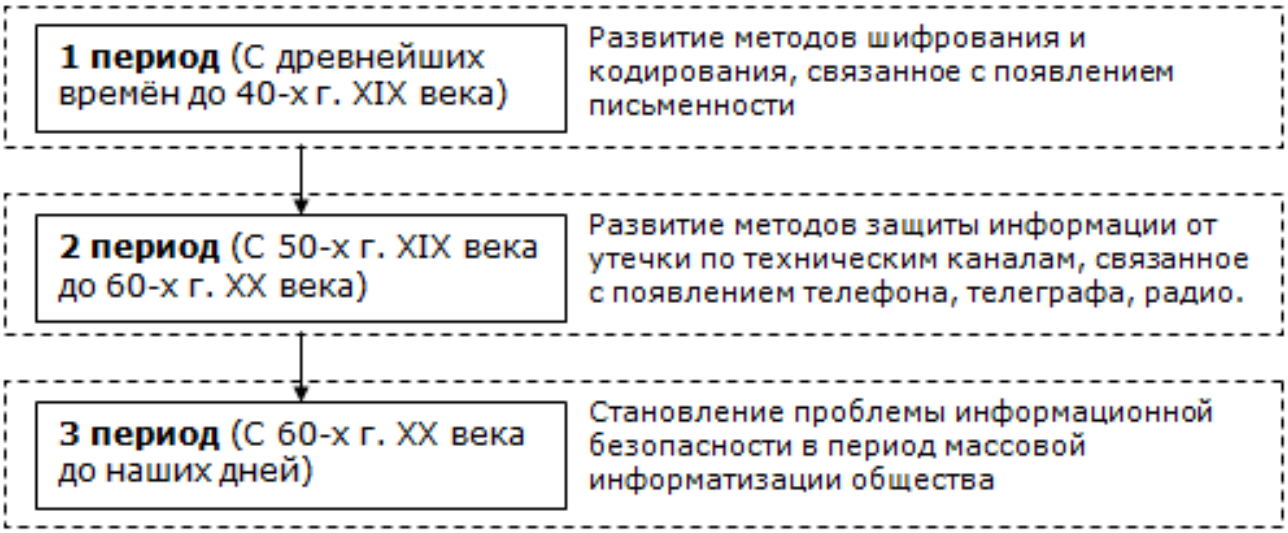

Рисунок 1.1 — Периоды развития

Наблюдаемые в последние годы тенденции в развитии информационных технологий могут уже в недалеком будущем привести к появлению качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне, которые могут принимать форму информационной войны, а сама информационная война станет одним из основных инструментов внешней политики, включая защиту государственных интересов и реализацию любых форм агрессии. Это является одной из причин, почему полезно ознакомиться с основными принципами обеспечения ИБ в ведущих зарубежных странах.

Прежде чем говорить об обеспечении безопасности персональных данных, необходимо определить, что же такое информационная безопасность. Термин «информационная безопасность» может иметь различный смысл и трактовку в зависимости от контекста. В данном пособии под информационной безопасностью мы будем понимать защищённость информации и поддерживающей инфраструктуры 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.[1]

Информационная безопасность — это защищённость информации и поддерживающей её инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

В ряде случаев понятие «информационная безопасность» подменяется термином «компьютерная безопасность». В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем. Несмотря на это, в рамках изучаемого курса основное внимание будет уделяться изучению вопросов, связанных с обеспечением режима информационной безопасности применительно к вычислительным системам, в которых информация хранится, обрабатывается и передаётся с помощью компьютеров. Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

2. Составляющие информационной безопасности

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трёх задач:

1. **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

2. **Целостность** – состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

3. **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. [2,3]

Атака — это попытка реализации угрозы. Кто предпринимает такую попытку, называется **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы**.

Угроза является следствием наличия уязвимых мест или уязвимости в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

- по свойствам информации (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход.

3. Уровни защиты информации

3.1. Законодательный уровень

Законодательный уровень является основой для построения системы защиты информации, так как даёт базовые понятия предметной области и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) отношение к людям, нарушающим информационную безопасность.

Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и

способы защиты, их правовой статус. Кроме того, к этому уровню относятся стандарты и спецификации в области информационной безопасности. Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений. К этому уровню можно отнести и морально-этические нормы поведения, которые сложились традиционно или складываются по мере распространения вычислительных средств в обществе. Морально-этические нормы могут быть регламентированными в законодательном порядке, т. е. в виде свода правил и предписаний. Наиболее характерным примером таких норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США. Тем не менее, эти нормы большей частью не являются обязательными, как законодательные меры.

3.2. Административный уровень

Это комплекс мер, предпринимаемых локально руководством организации. Включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации. Организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Разработка политики безопасности - дело тонкое, поскольку у каждой организации есть своя специфика. Здесь бессмысленно переносить практику режимных государственных организаций на коммерческие структуры, учебные заведения или персональные компьютерные системы. В этой области целесообразно предложить, во-первых, основные принципы разработки политики безопасности, а, во-вторых, - готовые шаблоны для наиболее важных разновидностей организаций.

3.3. Процедурный уровень

К процедурному уровню относятся меры безопасности, реализуемые людьми. В отечественных организациях накоплен богатый опыт составления и реализации процедурных (организационных) мер, однако проблема состоит в том,

что они пришли из докомпьютерного прошлого, поэтому нуждаются в существенном пересмотре.

Можно выделить следующие группы процедурных мер:

– управление персоналом;
– физическая защита;
– поддержание работоспособности;
– реагирование на нарушения режима безопасности;
– планирование восстановительных работ.

Для каждой группы в каждой организации должен существовать набор регламентов, определяющих действия персонала. В свою очередь, исполнение этих регламентов следует отработать на практике.

3.4. Программно-технический уровень

Согласно современным воззрениям, включает три подуровня: физический, технический (аппаратный) и программный.

Физический подуровень решает задачи с ограничением физического доступа к информации и информационным системам, соответственно к нему относятся технические средства, реализуемые в виде автономных устройств и систем, не связанных с обработкой, хранением и передачей информации: система охранной сигнализации, система наблюдения, средства физического воспрепятствования доступу (замки, ограждения, решётки и т. д.).

Средства защиты аппаратного и программного подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу.К аппаратным средствам относятся схемы контроля информации по четности, схемы доступа по ключу и т. д.

К программным средствам защиты, образующим программный подуровень, относятся специальное программное обеспечение, используемое для защиты информации, например антивирусный пакет и т. д. Программы защиты могут быть как отдельные, так и встроенные. Подчеркнём, что формирование режима информационной безопасности является сложной системной задачей, решение которой в разных странах отличается по содержанию и зависит от таких факторов, как научный потенциал страны, степень внедрения средств информатизации в жизнь общества и экономику, развитие производственной базы, общей культуры общества и, наконец, традиций и норм поведения.

4. Виды информационных угроз

Информационные угрозы могут быть обусловлены:

– естественными факторами (пожар, наводнение, и др.);

– человеческими факторами.

Последние, в свою очередь, подразделяются на:

1. Угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации;

2. Угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с несанкционированным доступом к ресурсам АИС.

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные. Угрозы также подразделяются на внутренние, возникающие внутри управляемой организации, и внешние.

Под внутренними угрозами понимаются — угрозы безопасности информации инсайдером (исполнителем) которых является внутренний по отношению к ресурсам организации субъект (инсайдер).

Под внешними угрозами понимаются — угрозы безопасности информации инициатором (исполнителем) которых является внешний по отношению к ресурсам организации субъект (удаленный хакер, злоумышленник).

Практические задания

1. Тестирование

1. В чем заключается проблема информационной безопасности?
2. Дайте определение понятию «информационная безопасность».
3. Что понимается под «компьютерной безопасностью»?
4. Перечислите составляющие информационной безопасности.
5. Приведите определение доступности информации.
6. Приведите определение целостности информации.
7. Приведите определение конфиденциальности информации.
8. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.

9. Перечислите задачи информационной безопасности общества.
10. Перечислите уровни формирования режима информационной безопасности.
11. Дайте краткую характеристику законодательно-правового уровня.
12. Какие подуровни включает программно-технический уровень?
13. Что включает административный уровень?
14. В чем особенность морально-этического подуровня?

2. Разбор ситуации

Оценив ситуацию соответствующую варианту нужно:

1. Определить источник угрозы.
2. Пострадавшее лицо.
3. Классифицировать вид угрозы.
4. Определить угрозу доступности, целостности, конфиденциальности.
5. Организовать меры по защите.

Так же организовать меры по защите информации в данных обстоятельствах и дальнейшее упреждение данной модели.

Пример решения

Сотрудница отделения коммерческого банка разместила фото с id своей карты в социальной сети;

В данной ситуации мы можем явно видеть, что сотрудник допустил халатность. В результате чего безопасность компании ставиться под вопрос.

1. Источником угрозы является сотрудница, а так же любые лица пытающиеся проникнуть в административную часть здания с поддельным пропуском на её имя.

2. Пострадавшим лицом является учреждение, в частности отдел по безопасности данного объекта. При бездействии круг пострадавших лиц может сильно увеличиться.

3. Классификация угрозы: - угроза обусловлена человеческим фактором; - носящим случайный, неумышленный характер; - угроза является внутренней.

4. Такие аспекты безопасности как доступность и целостность не нарушены. В данном контексте нарушена только конфиденциальность рабочих пропусков компании.

5. Меры по защите должны включать: - Немедленное блокирование пропуска сотрудницы, выдача нового. - Усиленная проверка входящих в здание по пропускам в течении недели. - Проверка персонала находящегося в здании. - Добавление/удачение пропусков происходят в следящем режиме. - Сверка активности сотрудницы. - Провести инструктаж на тему «Политика безопасности в организации».

Варианты задания

0. Сотрудница отделения коммерческого банка разместила фото с id своей карты в социальной сети;

1. В СМИ утекли результаты анализов одного из известных деятелей;

2. Ученик, взломав систему оценивания колледжа исправил себе бал по дисциплине;

3. Во время грозы были повреждены электролинии. В связи с этим более 200 клиентов охранной компании остались без наблюдения на 10 часов;

4. Используя брешь в интернет-сети страховой компании хакер заменил данные нескольких клиентов;

5. Интернет-магазин использует небезопасный канал. Клиент совершив покупку передал сумму третьему лицу;

6. Подкуплен сотрудник, после чего неизвестный проник в здание отделения полиции.

7. Сотрудник аудиторской компании использовал данные в своих целях;

8. После взлома сервера компании по информационной защиты ключи доступа пользователей появились на «чёрном рынке»;

9. Ночью из офиса была украдена печать адвоката, объект находится под охраной;

10. Сотрудник компании по разработке ПО скрыто вставлял мониторинг в продукт;

11. Сбой в работе компании по обеспечению vps серверов;

12. Обнаружен задержка интернет канала биржи. Предположительно злоумышленники подключившись к каналу получают данные первыми;

13. Сотрудник не соблюдал правила производства. В связи с чем завод потерял несколько партий продукта.

14. Зависание информационной системы на железной дороге привело к столкновению поездов.

15. Офис туристической компании был затоплен во время стихийного бедствия.

ПРАКТИЧНА РОБОТА 2

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Мета роботи: На практике использовать основные методы криптографической зашиты информации.

Теоретические ведомости

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость того, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Постепенно защита информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации; даже проводится ФЗ о защите информации, который рассматривает проблемы и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

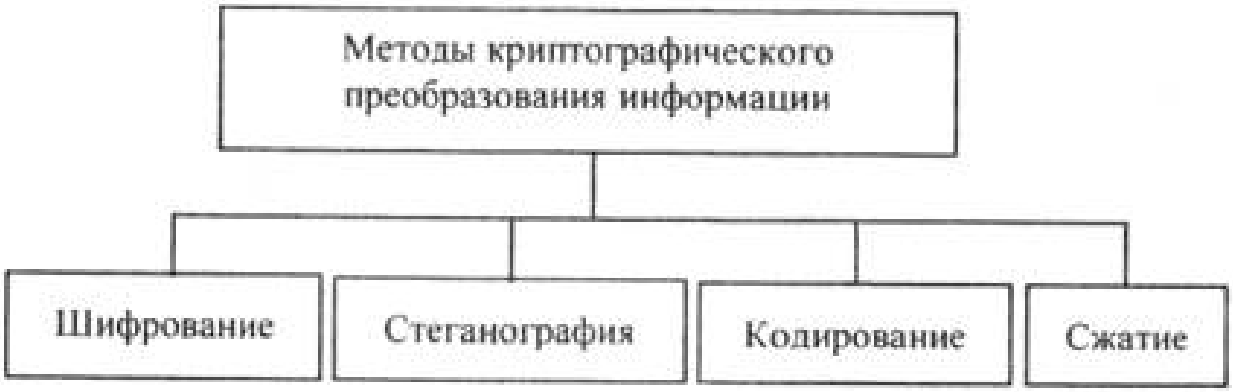

Рисунок 2.1 — Методы криптографического преобразования информации

1. Симметричные криптосистемы

1. Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение «Неясное становится ещё более непонятным» записывается в таблицу из 5 строк и 7 столбцов по столбцам.

Таблица 2.1

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Ё	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ–НЯЕЕО–ЯОЕТЯ–СВЕЛП–НСТИЩ–ЕОЫНА–ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает метод *одиночной перестановки* по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово - ЛУНАТИК, получим следующую таблицу:

Таблица 2.2 — Метод перестановки по ключу

Л	У	Н	А	Т	И	К
4	**7**	**5**	**1**	**6**	**2**	**3**
Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

До перестановки

А	И	К	Л	Н	Т	У
1	**2**	**3**	**4**	**5**	**6**	**7**
С	Н	Я	Н	Н	Б	О
Я	Е	Т	Е	О	О	Е
Е	П	Н	Я	В	Л	С
Щ	О	Ы	С	И	Е	Т
Е	Н	М	Н	Т	Е	А

После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв

ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН–БОЯЕТ–ЕООЕЕ–ПНЯВЛ–СЩОЫС–ИЕТЕН–МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины её строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются алгоритмы двойных перестановок. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в таблице 2.3.

Таблица 2.3 — Метод перестановки по ключу

	2	**4**	**1**	**3**
4	**П**	Р	И	Е
1	З	Ж	А	Ю
2	-	Ш	Е	С
3	Т	О	Г	**О**

	1	**2**	**3**	**4**
4	И	**П**	Е	Р
1	А	З	Ю	Ж
2	Е	-	С	Ш
3	Г	Т	**О**	О

	1	2	3	4
1	А	З	Ю	Ж
2	Е	-	С	Ш
3	Г	Т	**О**	О
4	И	**П**	Е	Р

Ключом к шифру служат номера столбцов **2413** и номера строк **4123** исходной таблицы. В результате перестановки получена шифровка:

АЗЮЖЕ_СШГТООИПЕР

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 33 их 36, для 44 их 576, а для $5 \cdot 5$ их 14400.

В средние века для шифрования применялись и магические квадраты. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведённой в квадрате нумерации и затем переписать содержимое таблицы по строкам. В ре-

Таблица 2.4 — Исходный текст с идентификаторами

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Таблиця 2.5 — Магический квадрат

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

О	И	Р	Т
З	Ш	Е	Ю
-	Ж	А	С
Е	Г	О	П

зультате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы $3 \times 3 \Rightarrow 1$ существует только один квадрат; для таблицы $4 \times 4 \Rightarrow 880$; а для таблицы $5 \times 5 \Rightarrow 250000$.

2. Шифры простой замены

2.1. Система шифрования Цезаря. частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на *K* букв. Известная фраза Юлия Цезаря `VENI VINI VICI` – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в `SBKF SFAF SFZF` (при смещении на 4 символа). Греческим писателем Полибием за 100 лет до н.э. был изобретён так называемый полибианский квадрат размером 5×5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже её в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

3. Шифры сложной замены

3.1. Шифр Гронсфельда. состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно так же, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

1. пусть в качестве ключа используется группа из трех цифр - 314;
2. тогда Сообщение СОВЕРШЕННО СЕКРЕТНО;
3. Ключ 3143143143143143;
4. Шифровка ФПЖИСЬИОССАХИЛФИУСС.

В шифрах *многоалфавитной замены* для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

В компьютере операция шифрования соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

4. Гаммирование

Процесс зашифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $T(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков Г(с)i аналогичной длины $(c)_i = G(c)_i \oplus T(0)_i$, где $\oplus$ - побитовое сложение, $i = 1 - m$).

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $T(0)_i = G(c)_i \oplus (c)_i$.

Исходное сообщение из букв русского алфавита преобразуется в числовое сообщение заменой каждой его буквы числом по следующей таблице:

Таблиця 2.6 — Числовая замена букв

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

$$\Omega_{i+1} = [(A_i + C_1 - 1) \cdot mod 30] + 1; \tag{2.1}$$

Исходное сообщение ОТДУШКА. Для шифрования числового сообщения используется шифрующий отрезок последовательности А1, А2, ... подходящей длины, начинающийся с A_{100}: $A_{101} \rightarrow 5$, $A_{102} \rightarrow 6$, $A_{103} \rightarrow 17$, $A_{104} \rightarrow 8$, $A_{105} \rightarrow 19$, $A_{106} \rightarrow 3$.

Исходное сообщение	О	Т	Д	У	Ш	К	А
Числовое исходное сообщение	13	17	4	18	23	9	0
Шифрующий отрезок	1	5	6	17	8	19	3
Числовое шифрованное сообщение	14	23	10	5	1	28	3
Шифрованное сообщение	П	Ш	Л	Е	Б	Ю	Г

Не забываем, что в выбранном алфавите 30 символов.

Задания

Использовать простые методы криптографической защиты для сокрытия фразы из табл. 2.7, в соответствии с вашим вариантом.

1. Шифры перестановки:
   - Метод перестановки по ключу;
   - алгоритм двойной перестановки;
   - магические квадраты.
2. Шифры замены:
   - Шифр Цезаря;
   - Аффиный шифр;
   - шифр Виженера;
   - шифра Плейфера.
3. Выполнить зашифровки методом гаммирования.
4. Записать сравнение различных видов шифров в отчёт.

Вопросы для контроля

1. Какие существуют методы криптографического преобразования информации?
2. Что такое шифрование?
3. Как происходит процесс шифровки/дешифровки сообщения?
4. Какие виды криптосистем вы знаете?
5. В чём принцип работы шифра Цезаря?
6. Безопасность использовать магических квадратов?
7. Как наложение гаммы влияет на исходный текст?

Таблиця 2.7 — Варианты к работе №2

1	6 x 6	небольшое сообщение для тестирования
2	3 x 13	В атмосфере происходит около 1800 гроз.
3	7 x 4	федеральное законодательство
4	4 x 6	Международные стандарты;
5	3 x 13	самая дорогая пицца в мире стоит $1000.
6	4 x 9	применение информационных технологий
7	3 x 12	административный уровень секретности
8	3 x 11	83% младших братьев выше старших
9	3 x 11	обеспечение доступа к информации
10	10 x 4	Индонезия расположена на 17508 островах.
11	4 x 7	у рыбы сарган зеленые кости.
12	8 x 4	язык хамелеона длиннее его тела
13	6 x 4	защищенность информации.
14	5 x 6	в озеро Байкал впадает 336 рек
15	3 x 10	гоночный болид едет по трассе.
16	8 x 3	опасность ”открывается”
17	4 x 8	процесс обеспечения целостности
18	4 x 9	рекомендация использования терминов
19	5 x 6	обеспечивающее ее формирование
20	5 x 5	общегосударственный орган
21	8 x 4	технических средств ее передачи
22	3 x 11	ворон и ворона — два разных вида.
23	5 x 6	наибольший ущерб субъектам ИБ
24	9 x 3	информационная безопасность
25	8 x 4	ущерб при сервисном обслуживании
26	5 x 7	свойство аутентичности пользователя
27	8 x 4	данные были действия выполнены?!
28	6 x 6	законодательный уровень безопасности
29	8 x 4	из множества потенциально угроз
30	4 x 9	Защита процессов, процедур, программ

ПРАКТИЧНА РОБОТА 3

МЕТОДЫ АТАКИ. ЧАСТОТНАЯ АТАКА

Мета роботи: Изучение способов атаки на разные уровни системы. Методы подбора и анализ частотной атаки.

Теоретические ведомости

Моноалфавитный подстановочный шифр – шифр, в котором каждой букве исходного алфавита поставлена в соответствие одна буква шифра.

Например, возьмем слово КУКУРУЗА. Пусть букве К текста соответствует буква А шифра, букве У текста соответствует буква Б шифра, букве Р текста соответствует буква В шифра, букве З текста соответствует буква Г шифра, букве А текста соответствует буква Д шифра. После подстановки букв шифра вместо букв исходного теста слово КУКУРУЗА в зашифрованном виде будет выглядеть как АБАБВБГД. Недостатком подобного шифрования является то, что, если какая-то буква встречается в исходном тексте чаще всего (например, буква О в русском алфавите), то и соответствующая ей буква шифра в зашифрованном тексте также встречается чаще всего. В ниже приведенной таблице приведены частоты встречаемости букв в английском тексте (в процентах):

диаграмма частот использования букв алфавита

Зная частоты наиболее встречающихся букв и подсчитав, какие буквы чаще всего встречаются в шифровке, криптоаналитик может подобрать расшифровку для некоторых букв текста. Затем, анализируя короткие слова, найти еще буквы, истинные значения которых можно с высокой степенью уверенности предугадать. Например, если уже расшифрована буква О и в тексте есть слово ОЫО (подчеркнуты уже расшифрованные буквы), то, скорее всего, шифру Ы соответствует буква Н в исходном тексте (ОНО). Чем дальше расшифровывается текст, тем легче идет процесс расшифровки.

Задания

1. Освоить теорию и принципы частотной атаки.
2. Проанализировать представленное ПО
3. Расшифровать текст и предоставить:

- шифрованное сообщение;
- перечень замен;
- расшифрованный текст;
- предоставить алгоритм дешифровки[1].

4. Выводы к работе

Пример выполнения работы

Варианты

Вопросы для контроля

[1] Задание для дополнительных баллов.

ПРАКТИЧНА РОБОТА 4

ПОСТРОЕНИЕ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Мета роботи: Знакомство с основными принципами построения концепции ИБ предприятия, с учётом особенностей его информационной инфраструктуры.

Теоретические ведомости

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов – Концепции и Политики информационной безопасности. Если Концепция ИБ в общих чертах определяет, ЧТО необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит КАК, какими средствами и способами они должны быть реализованы.

Концепция (от лат. conceptio) — генеральный замысел, определяющий стратегию действий.

Концепция защиты информации — это система взглядов на сущность, цели, принципы и организацию защиты информации.

Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;
- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- для формирования и реализации единой политики в области обеспечения информационной безопасности.

Концептуальная модель отвечает на общие вопросы и отражает схематично общую структуру модели информационной безопасности, на которой как на стержне строятся остальные модели и концепции информационной безопасности.

Для построения концептуальной модели информационной безопасности не зависимо от того насколько простая или сложная у Вас информационная система, необходимо как минимум ответить на три вопроса:

– Что защищать?
– От кого защищать?
– Как защищать?

Это обязательный минимум, которого может быть достаточно для небольших информационных систем. Однако принимая во внимание возможные последствия, то лучше выполнить построение полной концептуальной модель информационной безопасности, в которой необходимо определить:

1. Источники информации:
   – документы;
   – средства связи;
   – сотрудники;
   – электронные носители.
2. Степень важности информации.
3. Источники угроз:
   – внутренние;
   – внешние.
4. Цели угроз:
   – ознакомление;
   – дублирование;
   – модифицирование;
   – уничтожение.
5. Угрозы:
   – доступность;
   – целостность;
   – конфиденциальность.

1. Способы доступа:
   – разглашение;
   – утечка;
   – несанкционированный доступ.
2. Направления защиты:
   – правовое;
   – организационное;
   – инженерно-техническое.
3. Средства защиты:
   – физические;
   – аппаратные;
   – программные;
   – криптографические.
4. Методы защиты:
   – упреждение;
   – предотвращение;
   – пресечение;
   – противодействие.

Задания

Используя предложенные образцы, определить концептуальную модель безопасности компании.

1. Отделение коммерческого банка;
2. Поликлиника;
3. Колледж;
4. Офис страховой компании;
5. Рекрутинговое агентство;
6. Интернет-магазин;
7. Центр оказания гос. услуг;
8. Отделение полиции;
9. Аудиторская компания;
10. Дизайнерская фирма;
11. Офис интернет-провайдера;
12. Офис адвоката;
13. Компания по разработке ПО;
14. Агентство недвижимости;
15. Туристическое агентство;
16. Офис благотворительного фонда;
17. Издательство;
18. Консалтинговая фирма;
19. Рекламное агентство;
20. Отделение налоговой службы;
21. Офис нотариуса;
22. Бюро перевода (документов);
23. Научно проектное предприятие;
24. Брачное агентство;
25. Редакция газеты;
26. Гостиница;
27. Праздничное агентство;
28. Городской архив;
29. Диспетчерская служба такси;
30. Железнодорожная касса.

Пример выполнения работы

Вопросы для контроля

ПРАКТИЧНА РОБОТА 5

СЕМИНАР ПО ТЕМЕ СТАНДАРТОВ В ИБ

Мета: ознакомиться с основными положениями стандартов по обеспечению информационной безопасности в распределённых вычислительных сетях.

Требования к знаниям и умениям

Студент должен знать:

- основное содержание стандартов по информационной безопасности распределённых систем;
- основные сервисы безопасности в вычислительных сетях;
- наиболее эффективные механизмы безопасности;
- задачи администрирования средств безопасности.

Студент должен уметь:

- выбирать механизмы безопасности для защиты распределенных систем.

Термины

Распределённая информационная система — совокупность аппаратных и программных средств, используемых для накопления, хранения, обработки, передачи информации между территориально удалёнными пользователями.

Сервис *(Сервисная деятельность)* — это вид деятельности, направленный на удовлетворение потребностей социальных субъектов посредством оказания услуг.

Сервис безопасности — это деятельность государственных и частных организаций, а также отдельных специалистов, направленная на удовлетворение потребностей социальных субъектов в безопасности.

Цель сервиса безопасности − удовлетворение потребностей в безопасности индивидуальных и групповых социальных субъектов. **Сущность сервиса безопасности** состоит в оказании услуг, направленных на обеспечение безопасности. **Услуга безопасности** – это деятельность субъекта безопасности, направленная на удовлетворение потребности заказчика в безопасности, а также результат взаимодействия исполнителя и заказчика услуги безопасности, выраженный в виде полезного эффекта.

Темы для обсуждения

1. Механизмы безопасности.
2. Сервисы безопасности в вычислительных сетях.
3. Функций и механизмов безопасности.
4. Администрирование средств безопасности.
5. Международные стандарты.
6. Стандарты ГОСТ и ДСТУ.

Ссылки на литературу: 1. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издательство Молгачева С. В., 2001.2. Теория и практика обеспечения информационной безопасности / Под ред. П. Д. Зегжды. – М: Яхтсмен, 1996.3. Галатенко В. А. Основы информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2003.4. Галатенко В. А. Стандарты информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2004.5. www.iso.ch – Web-сервер Международной организации по стандартизации.

ПРАКТИЧНА РОБОТА 6

РАСПРЕДЕЛЕНИЕ ПРАВ В ОРГАНИЗАЦИЯХ

Мета роботи: Научиться определять потребности в системах по моделям IDEF0, предоставление полномочий для разных классов сотрудников.

Теоретические ведомости

1. **Права в информационной безопасности**
2. **Распределение прав**
3. **Использование модели IDEF0**

Задания

1. Выбрать предприятие, структуру из табл.
2. Построение модели IDEF0.
3. Распределить права между сотрудниками, их полномочия и средства защиты.
4. Определить технологии защиты от несанкционированного доступа.
5. Предоставить результаты в отчёте.

Пример выполнения работы

Варианты

Вопросы для контроля

ПРАКТИЧНА РОБОТА 7

ОБЗОР МЕТОДОВ СОКРЫТИЯ ИНФОРМАЦИИ

Мета роботи: Изучить методы, факторы и риски при сокрытии информации.

Теоретические ведомости

Стеганография — это наука о передачи секретной информации, причем сам факт передачи остаётся неизвестен внешнему наблюдателю. Развитие стеганографии мотивируется в основном потребностью защиты интеллектуальной собственности в компьютерных сетях, в основном в интернете.

Различают два вида стеганографии:

1. Сокрытие информации от пассивного наблюдателя. В этом случае основная цель – не допустить обнаружения скрытой информации.

2. Сокрытие информации от активного противника, т.е. наличие скрытой информации заведомо известно, но получение этой информации противником невозможно. Этот случай распространяется на схемы защиты авторских прав. Здесь используются digital *watermarking* (цифровые водяные знаки) и *fingerprinting* (отпечатки пальцев).

1. Методы сокрытия информации

В настоящее время методы компьютерной стеганографии развиваются по двум основным направлениям:

1. Методы, основанные на использовании специальных свойств компьютерных форматов;
2. Методы, основанные на избыточности аудио и визуальной информации.

1.1. Метод использовании свойств. Здесь применяется метод использования зарезервированных для расширения полей компьютерных форматов данных. Зарезервированные поля имеются во многих мультимедийных форматах, они заполняются нулевой информацией и не учитываются программой. Этот метод очень прост в использовании. Однако явным недостатком этого метода является низкая степень скрытности и передача небольших ограниченных объёмов информации.

Для передачи текстовых сообщений используются методы специального форматирования текстовых файлов:

- Методы, основанные на изменении положения строк и расстановки слов в предложении, что обеспечивается вставкой дополнительных пробелов между словами.
- Методы выбора определенных позиций букв (нулевой шифр). Акростих
- частный случай этого метода, когда например, начальные буквы каждой строки образуют сообщение или начальные буквы каждого слова.
- Методы, основанные на использовании специальных ”невидимых”, скрытых полей. Например, использование чёрного шрифта на чёрном фоне.
- Методы сокрытия в неиспользуемых местах гибких дисков. Информация может записываться, к примеру, на нулевую дорожку.
- Использования имитирующих функций (mimic-function). Метод основан на генерации текстов и является обобщением акростиха. Для тайного сообщения генерируется осмысленный текст, скрывающий само сообщение, расположение букв которого в сгенерированном тексте задаётся определённым образом.

Все эти методы просты в использовании, но малопроизводительны и обеспечивают низкую степень скрытости. Предназначены только для передачи небольших объемов информации.

Ярким примером применения компьютерной стеганографии является компьютерный вирус Win95.CIH. Этот вирус внедряется в исполняемый файл *.exe. Исполняемый файл может содержать не только код, но и многочисленные дополнительные данные: пиктограммы, различные служебные данные и информация об экспортируемых и импортируемых функциях. Каждый вид данных, содержащихся в файле, это отдельный объект, занимающий секцию фиксированного размера. Если объект не занимает всего объёма секции, то эта часть секции не используется. Поэтому в файле формата PE всегда достаточно свободного места для записи.

1.2. Метод избыточности информации. Младшие разряды представления аудио и видео формата малоинформативны и их изменение практически не сказывается на качестве передаваемого изображения или звука, что дает возможность использования их для кодирования конфиденциальной информации. Но при введении дополнительной информации искажаются статистические характеристики передаваемого файла, что может привести к обнаружению передаваемого

сообщения. Для повышения устойчивости к обнаружению применяют методы коррекции статистических характеристик. Основным достоинством данного метода является возможность скрытой передачи большого объёма информации, а также возможность защиты авторского права, скрытого изображения товарной марки, регистрационных номеров и т.п.

Наиболее распространенным является метод замены наименее значимых битов или LSB метод. Суть этого подхода заключается в том , что за счет погрешности дискретизации изменение младших разрядов в аудио видео изображении практически не сказывается на качестве передаваемого звука или картинки, особенно если изначально оно было закодировано с большой глубиной передачи цвета. Визуально определить было ли изображение подвергнуто трансформации или нет невозможно, но, используя специальные методы, основанные на статистическом анализе, можно сказать, было ли вкраплено в файл некоторое дополнительное количество информации и даже извлечь ее.

Другие популярные методы встраивания секретных сообщений основаны на использовании форматов файлов с потерей данных (например, JPEG). В отличие от LSB методов они более стойки к геометрическим преобразованиям и обнаружению канала передачи. Это достигается за счет возможности изменять качество сжатых данных в широком диапазоне, что приводит к невозможности определения происхождения изображения.

В современных системах формирования цифровых водяных знаков используется принцип встраивания метки, являющейся узкополосным сигналом, в то время как само маркируемое изображение является широкополосным. Указанный метод реализуется при помощи двух основных алгоритмов и их модификаций. В первом из них используется фазовая модуляция сигнала с псевдослучайной последовательностью чисел для сокрытия секретной информации. Во втором случае весь канал передачи информации делится на несколько каналов и передача осуществляется между ними. На плане исходного изображения встраиваемая метка представляет из себя дополнительный шум со своими статистическими характеристиками. За счет того, что некоторый шум в изображениях присутствует всегда, встраивание метки влияет лишь на уровень имеющегося шума, обычно незаметного для органов чувств. Кроме всего метка является устойчивой к выделению из основного сигнала за счет ее рассеивания по всему частотному диапазону изображения.

2. Примеры методов звуковых файлов

Low-bit coding. Является самым простым метод встроить метку в структуру данных. Наименее значимые биты в самплах заменяются на биты встраиваемой метки. Основным недостатком этого метода является его слабая устойчивость к манипуляциям над файлом. В процессе ресамплинга или в результате передачи скрытое сообщение может быть легко искажено или вообще потеряно.

Phase Coding заменяет фазу оригинального звукового сегмента на относительную фазу, которая и представляет собой секретное сообщение. Фаза последовательных сегментов добавляется таким образом, чтобы сохранить относительный фазовый сдвиг между сегментами. Phase coding – один из наиболее эффективных методов сокрытия информации в терминах отношения уровня сигнала к заметному искажению этого сигнала. Когда отношение фаз между частотами сильно меняется, происходит заметная фазовая дисперсия. Однако “неслышное” кодирование при этом все равно достигается, так как изменение фазы достаточно мало.

Spread spectrum. В обычном канале связи стремятся сконцентрировать информацию в как можно более узком диапазоне частот, чтобы сохранить доступную полосу пропускания и уменьшить энергию, необходимую для передачи. Основной метод расширения спектра спроектирован таким образом, чтобы закодировать поток информации, распространяя секретные данные в как можно большем спектре частот. Это позволяет извлечь скрытую в потоке информацию, даже если происходит интерференция на некоторых частотах.

Echo data hiding. При использовании этого метода данные заключаются в оригинальный звуковой сигнал посредством ввода эха. Данные скрываются при помощи изменения трех параметров эха: начальной амплитудой, степени затухания и задержки. Когда задержка между оригинальным сигналом и эхом уменьшается, сигналы смешиваются. В некоторой точке человеческое ухо уже не может различить эти два сигнала, эхо ощущается как добавочный резонанс. Эту точку достаточно сложно определить, она зависит о качества оригинальной записи, типа записи и слушателя. Обычно слияние сигналов осуществляется в районе 1/1000 секунды, что характерно для большинства типов звуков и слушателей. При кодировании используется две временные задержки, одна для обозначения логической единицы (*offset*), другая для логического нуля (offset + delta). Обе задержки должны быть меньше порога чувствительности человеческого уха, при котором

он может обнаружить эхо. Вдобавок к уменьшению временной задержки необходимо убедиться, что информацию нельзя раскрыть установлением начальной амплитуды и степени затухания ниже порога слышимости человеческого уха.

Для улучшения характеристик сигнала при использовании различных методов сокрытии информации в медиаданных, а также повышения устойчивости полученного сигнала к его анализу и обнаружению скрытой информации применяются некоторые полезные дополнения к обычным алгоритмам стеганографии. Вот некоторые из них.

Adaptive data attenuation. Оптимальный фактор подстройки изменяется при изменении уровня оригинального сигнала. Адаптируя подстройку к небольшим изменениям уровня сигнала или шума, можно удерживать уровень сигнала, представляющего закодированные данные, очень низким в течение интервалов тишины и увеличивать во время интервалов большего уровня звука.

Redundancy and error correction coding. Для того чтобы избежать ошибок при получении сигнала вследствие шума в канале или изменении оригинального звука, полезно применять кодирование с исправлением ошибок к скрываемым данным. Тем не менее, при использовании алгоритмов коррекции ошибок приходиться обходиться компромиссным вариантом, учитывающим надежность данных и объём данных, которые можно при этом скрыть.

Sound context analysis. Обнаруживаемость белого шума, встроенного в оригинальный сигнал, линейно зависит от уровня первоначального звука. Для максимизации объёма скрываемых данных, при условии, что они не будут обнаружены, полезно измерять уровень шума при кодировании. Уровень шума можно определить, измеряя изменение амплитуды сигнала в близлежащих самплах.

2.1. Стохастическая модуляция. Одним из последних методов стеганографии является прием стохастической модуляции. На примере графического файла он представляется следующим образом.

Сообщение, которое необходимо передать, обозначим m, состоящее из последовательных 1 и $-1(0)$. Сначала определяется вероятностная функция $P(x,s) \in -1,1$, равная 0 только при $s = 0$. Она также должна удовлетворять свойству антисимметричности для всех $x : P(x+s,s) = -P(x-s,s)$. Это свойство полезно в тех случаях, когда значения x+s или x-s выходят за допустимый диапазон значений. При наложении секретной информации пикселы проходятся в псевдослучайной последовательности, построенной с помощью генератора случайных чисел с распределением, совпадающим с распределением шума, который

будет наложен на картинку. Такая последовательность называется стегошумом. При генерации используется специальный стегоключ. Для каждой точки x генерируется случайной число s. Если s отлично от нуля, то если $P(x+s,s) = m$, то значение пикселя заменяется на $x+s$, если $P(x+s,s) = -m$, то значение заменяется на $x-s$. Формально процесс сокрытия есть

$$x'_i = xi + m_i \cdot P(x_i + s_i,s_i) \cdot s_i \tag{7.1}$$

Так как само изображение и стегошум s_i не зависят от секретного сообщения, то сигнал $v_i = m_i \cdot P(x_i + s_i,s_i)$ является псевдослучайной последовательностью 1 и -1. Таким образом, v_i имеет такие же статистические свойства, что и стегошум.

Для извлечения закодированного сообщения генерируется стегошум по тому же стегоключу, что и при кодировании. Применяя вероятностную функцию P к пикселам изображения, получаем секретное сообщение, формируемое из ненулевых значений $m_i = P(x_i,s_i)$.

В рассмотренном выше методе используется только один стегошум s_i, который добавляется или вычитается из значений пикселя в соответствии с вероятностной функцией. Возможно получить больший объём скрываемой информации с теми же шумовыми характеристиками.

Улучшенный метод стохастической модуляции использует сразу два стегошума, добавляя к значениям пикселей изображения всегда либо один стегошум, либо другой, основываясь опять на совпадении бит сообщения и вероятностной функции. Этот метод работает для стегошума с произвольным вероятностным распределением.

Метод стохастической модуляции можно также применять для изображений, полученных с помощью устройств, шум которых зависит от содержания изображения. Подробно этот способ рассмотрен в [2].

2.2. Использование шума. Есть два конечных абонента, которые хотят совершить разговор на расстоянии, с помощью какого-нибудь канала связи. Сам канал они не контролируют. Необходимо избежать утечки информации путем кодирования.

Для решения этой проблемы используется наложение защитного шума (накладывается шум перед отдачей в канал связи, и соответственно снимается перед

выводом на динамик). Шум должен быть случайным или, что то же самое, белым (большинство источников генерируют псевдо-случайный шум — такой шум достаточно легко может быть подавлен).

При использовании остальных способов шифрования остаются остаточные признаки речи, по которым, обладая достаточно мощным вычислительным комплексом, можно получить исходную речь в приемлемом качестве.

Даже если использовать белый шум возникают проблемы: его так же надо как-нибудь передать адресату, иначе (если не передавать), то злоумышленник может сделать то же самое, что и адресат (подавить шум).

2.3. Шум для шифрования изображений. Визуальная криптография впервые была введена Мони Наором и Ади Шамиром в 1994 году. Она используется для шифрования изображения или текста, представленного в виде изображения. Основная идея модели визуальной криптографии состоит в разбиении исходного изображения на несколько шифрованных («теневых» изображений, shadow images), каждое из которых не дает никакой информации об исходном изображении кроме, может быть, его размера (изображение – а-ля «белый шум»). При наложении шифрованных изображений друг на друга, можно получить исходное изображение. Таким образом, для декодирования не требуется специальных знаний, высокопроизводительных вычислений и даже компьютера (в случае, если распечатать теневые изображения на прозрачных пленках). В случае использования этого алгоритма в компьютерных системах, наложить все части изображения друг на друга можно используя логические операции AND, OR, XOR (или установив более высокую степень прозрачности в графическом редакторе). Данная технология обладает криптоустойчивостью за счёт того, что при разделении исходного изображения на множество шифроизображений происходит случайным образом.

3. Методы обнаружения информации

Обнаружения информации в файлах.

Rarjpeg — это особый вид файлов, представляющий собой склеенную вплотную jpeg-картинку и rar-архив. Он является прекрасным контейнером для сокрытия передачи информации. Создать rarjpeg можно с помощью следующих команд:

```
UNIX: cat image1.jpg archive.rar > image2.jpg
WINDOWS: copy /b image1.jpg+archive.rar image2.jpg
Или же при наличии hexредактора—.
```

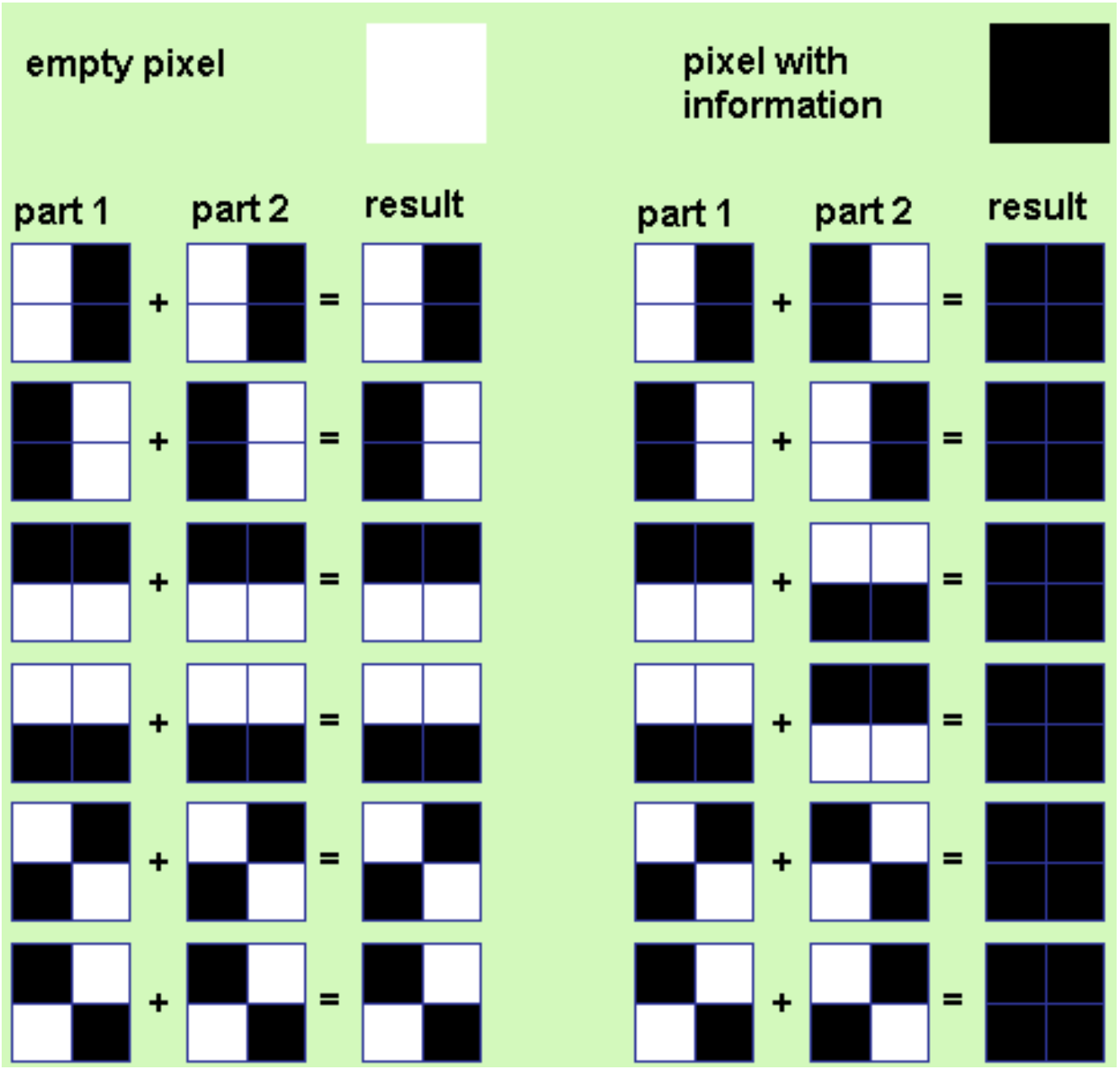

Рисунок 7.1 — Возможные состояния пикселя при визуальной схеме $2x2$

Разумеется, для скрытия факта передачи информации можно использовать не только формат JPEG, но и многие другие. Каждый формат имеет свои особенности, благодаря которым он может подходить или нет для роли контейнера.

4. Методы детектирования склеенных файлов

4.1. Метод проверки области после EOF-маркера. Множество популярных форматов файлов имеют так называемый маркер конца файла, который отвечает за отображение нужных данных. Например, программы для просмотра фотографий считывают все байты вплоть до этого маркера, однако, область после него остается игнорируемой. Этот метод идеально подходит для форматов: JPEG, PNG, GIF, ZIP, RAR, PDF.

4.2. Метод проверки размера файла. Структура некоторых форматов (аудио- и видеоконтейнеры) позволяет вычислить реальный размер файла и сравнить его с исходным размером. Форматы: AVI, WAV, MP4, MOV.

4.3. Метод проверки CFB-файлов. CFB или Compound File Binary Format — формат документов, разработанный в Microsoft, представляющий собой контейнер с собственной файловой системой. Этот метод основан на обнаружении аномалий в файле.

4.4. Продолжение файла. Ознакомившись с предыдущими тегами можно сделать вывод, что данные в файл могут быть записаны и после основного содержимого.

Далее предоставим несколько примеров:

JPEG

Для нахождения ответа на этот вопрос, необходимо углубиться в спецификации формата, который является «родоначальником» склеенных файлов и понять его структуру. Любой JPEG начинается с сигнатуры 0xFF 0xD8.

После этой сигнатуры находится служебная информация, опционально иконка изображения и, наконец, само сжатое изображение. В этом формате конец изображения отмечается двухбайтной сигнатурой 0xFF 0xD9.

PNG

Первые восемь байт PNG-файла занимает следующая сигнатура: 0x89, 0x50, 0x4E, 0x47, 0x0D, 0x0A, 0x1A, 0x0A. Сигнатура конца, которая заканчивает поток данных: 0x49, 0x45, 0x4E, 0x44, 0xAE, 0x42, 0x60, 0x82.

RAR

Общая сигнатура для всех rar-архивов: 0x52 0x61 0x72 0x21 (Rar!). После неё идет информация о версии архива и прочие сопутствующие данные. Опытным путём было установлено, что архив заканчивается сигнатурой 0x0A, 0x25, 0x25, 0x45, 0x4F, 0x46.

Таблиця 7.1 — Таблица форматов и сигнатур RAR

Формат	Начальная сигнатура	Конечная сигнатура
JPEG	0xFF 0xD8	0xFF 0xD9
PNG	0x89 0x50 0x4E 0x47 0x0D 0x0A 0x1A 0x0A	0x49 0x45 0x4E 0x44 0xAE 0x42 0x60 0x82
RAR	0x52 0x61 0x72 0x21	0x0A 0x25 0x25 0x45 0x4F 0x46

Алгоритм проверки на склейку в данных форматах предельно прост:

1. Найти начальную сигнатуру;
2. Найти конечную сигнатуру;
3. Если после конечной сигнатуры нет данных — ваш файл чист и не содержит вложений! В ином случае необходимо искать после конечной сигнатуры другие форматы.

GIF и **PDF**

Таблица 7.2

Формат	Начальная сигнатура	Конечная сигнатура
GIF	0x47 0x49 0x46 0x38	0x00 0x3B
PDF	0x25 0x50 0x44 0x46	0x0A 0x25 0x25 0x45 0x4F 0x46

PDF документ может иметь более одного EOF-маркера, например, из-за неправильной генерации документа. Количество конечных сигнатур в GIF-файле равно количеству кадров в нём. Исходя из особенностей этих форматов, можно улучшить алгоритм проверки наличия приклеенных файлов.

1. Пункт 1 повторяется из предыдущего алгоритма.
2. Пункт 2 повторяется из предыдущего алгоритма.
3. При нахождении конечной сигнатуры запомнить её расположение и искать дальше;
4. Если таким образом дошли до последнего EOF-маркера — файл чист.
5. Если файл не заканчивается конечной сигнатурой — goto место последней найденной конечной сигнатуры.

Большая разница между размером файла и позицией после последней конечной сигнатуры указывает на наличие приклеенного вложения. Разница может составлять больше десяти байт, хотя возможна установка иных значений.

ZIP

Особенность ZIP-архивов заключается в наличие трех различных сигнатур:

Таблица 7.3

Сигнатуры	Описание
0x50 0x4B 0x03 0x04	Сигнатура обычного архива
0x50 0x4B 0x05 0x06	Сигнатура пустого архива
0x50 0x4B 0x07 0x08	Сигнатура архива, разделенного на части

Больше всего интересна центральная директория, которая содержит метаданные о файлах в архиве. Центральная директория всегда начинается с сигнатуры 0x50 0x4b 0x01 0x02 и заканчивается сигнатурой 0x50 0x4b 0x05 0x06,

Таблиця 7.4

Local File Header 1
File Data 1
Data Descriptor 1
Local File Header 2
File Data 2
Data Descriptor 2
...
Local File Header n
File Data n
Data Descriptor n
Archive decryption header
Archive extra data record
Central directory

после которых следует 18 байт метаданных. Что интересно, пустые архивы состоят только из конечной сигнатуры и 18 нулевых байт. После 18 байт следует область комментария к архиву, которая является идеальным контейнером для скрытия файла.

Для проверки ZIP-архива необходимо найти конечную сигнатуру центральной директории, пропустить 18 байт и искать сигнатуры известных форматов в области комментария. Большой размер комментария также свидетельствует о факте склейки.

AVI

Структура AVI-файла следующая: каждый файл начинается с сигнатуры RIFF (0x52 0x49 0x46 0x46). На 8 байте идет уточняющая формат сигнатура AVI (0x41 0x56 0x49 0x20). Блок на смещении 4, состоящий из 4 байт, содержит начальный размер блока данных (порядок байт — little endian). Чтобы узнать номер блока, содержащего следующий размер, необходимо сложить размер заголовка (8 байт) и размер, полученный в блоке 4-8 байт. Таким образом вычисляется полный размер файла. Допускается, что вычисленный размер может быть меньше, чем реальный размер файла. После вычисленного размера файл будет содержать только нулевые байты (необходимо для выравнивания границы в 1 Кб).

WAV

Как и AVI, WAV-файл начинается с сигнатуры RIFF, однако, у этого файла сигнатура с 8 байта — WAVE (0x57 0x41 0x56 0x45). Размер файла вычисляется таким же образом, как и AVI. Реальный размер должен полностью совпадать с

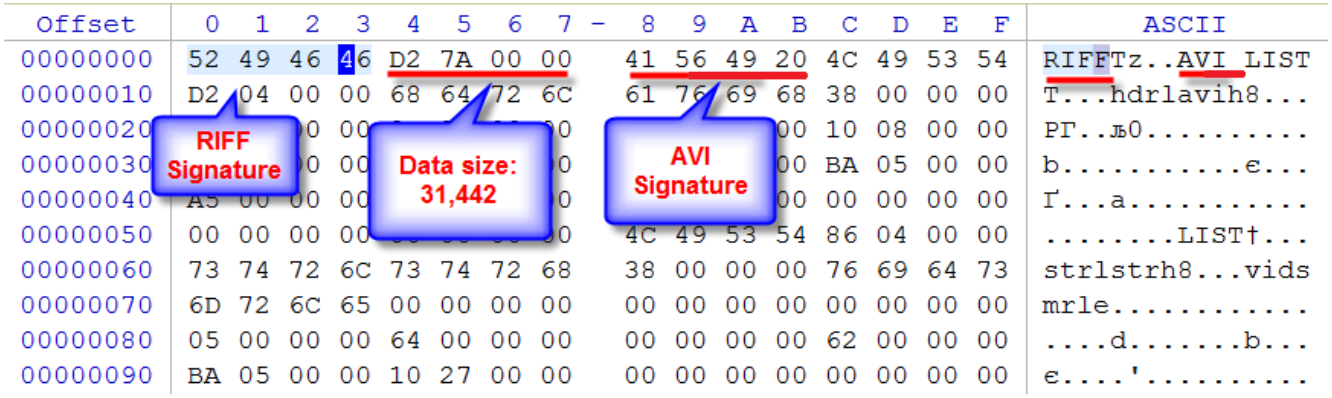

Рисунок 7.2 — Пример вычисления AVI

вычисленным.

MP4

MP4 или MPEG-4 – формат медиаконтейнера, используемый для хранения видео- и аудиопотоков, также предусматривает хранение субтитров и изображений.

На смещении 4 байта расположены сигнатуры: тип файла ftyp (66 74 79 70) (QuickTime Container File Type) и подтип файла mmp4 (6D 6D 70 34). Для распознания скрытых файлов, нас интересует возможность вычисления размера файла.

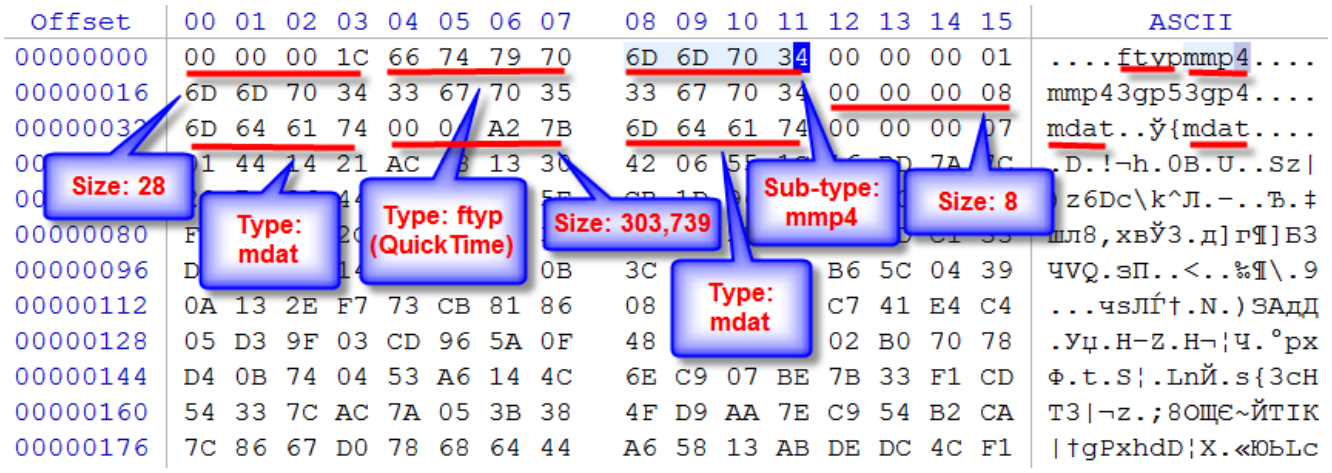

Рисунок 7.3 — Пример вычисления MP4

Рассмотрим пример. Размер первого блока находится на нулевом смещении, и он равен 28 (00 00 00 1C, порядок байт Big Endian); он же указывает на смещение, где находится размер второго блока данных. На 28 смещении находим следующий размер блока равный 8 (00 00 00 08). Чтобы найти следующий размер блока, необходимо складывать размеры найденных предыдущих блоков.

Таким образом, вычисляется размер файла:

MOV

Смещение	Значение	Следующее смещение
0	28	28+0=28
28	8	28+8=36
36	303739	36+303739=303775
303775	6202	303775+6202=309977

Этот широко используемый формат является также контейнером MPEG-4. MOV использует проприетарный алгоритм сжатия данных, имеет похожую на MP4 структуру и используется в тех же целях — для хранения аудио и видеоданных, а также сопутствующих материалов.

Как и MP4, любой mov-файл имеет на 4 смещении 4-х байтную сигнатуру ftyp, однако, следующая сигнатура имеет значение qtyp (71 74 20 20). Правило вычисления размера файла не изменилось: начиная с начала файла вычисляем размер следующего блока и складываем.

Метод проверки этой группы форматов на наличие «приклеенных» файлов заключается в вычислении размера по заданным выше правилам и сравнении его с размером проверяемого файла. Если текущий размер файла много меньше вычисленного, то это указывает на факт склейки. При проверке AVI-файлов допускается, что вычисленный размер может быть меньше размера файла из-за наличия добавленных нулей для выравнивания границы. В таком случае, необходимо проверять нули после вычисленного размера файла.

Задания

Цель практической части работы состоит в получении максимально коэф. сокрытия информации.

1. Изучить теорию, быть готовым к опросу.
2. Сокрыть информацию с помощью предоставленного ПО:
    а) в тесте;
    б) в изображении;
    в) в музыке.
3. Сравнение методов и выводы к работе.

Инструкция к работе с ПО

(ф-ции программы, методы и т.д.)

Вопросы для контроля

1. Какие есть способы сокрытия информации?
2. В каких файлах лучше скрывать информацию?
3. Что такое шум?
4. Риски потери и дешифровка информации.

ПРАКТИЧНА РОБОТА 8

АНАЛИЗ РИСКОВ

Мета роботи: Изучение анализа рисков. Формирование навыка определения угроз и защита.

Теоретические ведомости

1. **Риски в информационной безопасности**
2. **Анализ стойкости системы**
3. **Правила определения угроз и защиты информации**

Риск ИБ — потенциальная возможность использования определенной угрозой уязвимостей актива или группы активов для причинения вреда организации.

Уязвимость — слабость в системе защиты, делающая возможной реализацию угрозы.

Угроза ИБ — совокупность условий и факторов, которые могут стать причиной нарушений целостности, доступности, конфиденциальности информации.

Информационный актив — это материальный или нематериальный объект, который:

- является информацией или содержит информацию,
- служит для обработки, хранения или передачи информации,
- имеет ценность для организации.

Задания

1. Защита объекта по варианту из табл..
2. Оценка качества защиты.

Пример выполнения работы

Варианты

РЕКОМЕНДАЦІЇ