Титулка

Зміст

[Список сокращений и условных обозначений 5](#_Toc511944384)

[Словарь терминов 6](#_Toc511944385)

[Введение 9](#_Toc511944386)

[1 Основные понятия безопасности 11](#_Toc511944387)

[Теоретические ведомости 11](#_Toc511944388)

[1 Основные понятия информационной безопасности 11](#_Toc511944389)

[2 Составляющие информационной безопасности 13](#_Toc511944390)

[3 Уровни защиты информации 14](#_Toc511944391)

[4 Виды информационных угроз 17](#_Toc511944392)

[Задания 18](#_Toc511944393)

[1 Тестирование 18](#_Toc511944394)

[2 Рассмотрение ситуации 18](#_Toc511944395)

[Пример выполнения работы 19](#_Toc511944396)

[Варианты задания 20](#_Toc511944397)

[2 Пакеты антивирусных программ 21](#_Toc511944398)

[Теоретические ведомости 21](#_Toc511944399)

[1 История 21](#_Toc511944400)

[2 Антивирусные склоки 23](#_Toc511944401)

[3 Классификация 24](#_Toc511944402)

[4 Виды антивирусной защиты 27](#_Toc511944403)

[Задания 29](#_Toc511944404)

[3 Мировые стандарты безопасности 30](#_Toc511944405)

[Требования к семинару 30](#_Toc511944406)

[1 Студент должен знать 30](#_Toc511944407)

[2 Студен должен уметь 30](#_Toc511944408)

[Термины для подготовки 30](#_Toc511944409)

[Темы для обсуждения 31](#_Toc511944410)

[Литература для ознакомления 31](#_Toc511944411)

[4 Методы сокрытия информации 32](#_Toc511944412)

[Теоретические ведомости 32](#_Toc511944413)

[Задания 32](#_Toc511944414)

[Ход работы 32](#_Toc511944415)

[Вопросы для самоконтроля 32](#_Toc511944416)

[5 Архивация данных 33](#_Toc511944417)

[Архивация данных 33](#_Toc511944418)

[1 Алгоритмы архивации данных 34](#_Toc511944419)

[Задания 42](#_Toc511944420)

[Вопросы для самоконтроля 42](#_Toc511944421)

[6 Cisco. Часть 1 43](#_Toc511944422)

[Теоретические ведомости 43](#_Toc511944423)

[Задания 43](#_Toc511944424)

[Ход работы 43](#_Toc511944425)

[Вопросы для самоконтроля 43](#_Toc511944426)

[7 Cisco. Часть 2 44](#_Toc511944427)

[Теоретические ведомости 44](#_Toc511944428)

[Задания 44](#_Toc511944429)

[Ход работы 44](#_Toc511944430)

[Вопросы для самоконтроля 44](#_Toc511944431)

[8 Анализ данных 45](#_Toc511944432)

[Теоретические ведомости 45](#_Toc511944433)

[Задания 45](#_Toc511944434)

[Ход работы 45](#_Toc511944435)

[Вопросы для самоконтроля 45](#_Toc511944436)

[Додаток А 46](#_Toc511944437)

[Додаток Б 47](#_Toc511944438)

1. Список сокращений и условных обозначений
2. Словарь терминов

**Открытый (исходный) текст** — данные (не обязательно текстовые), пере­даваемые без использования криптографии.

**Шифротекст, шифрованный (закрытый) текст** — данные, полученные после применения криптосистемы.

**Шифр, криптосистема** — совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.

**Символ** — это любой знак, в том числе буква, цифра или знак препинания. **Алфавит** — конечное множество используемых для кодирования информации символов. Стандартный алфавит может быть изменён или дополнен символами. **Ключ** — параметр шифра, определяющий выбор конкретного преобразования данного текста. В современных шифрах криптографическая стойкость шифра це­ликом определяется секретностью ключа (принцип Керкгоффса).

**Шифрование** — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате ко­торого возникает шифрованный текст.

**Расшифровывание** — процесс нормального применения криптографиче­ского преобразования шифрованного текста в открытый.

**Асимметричный шифр, двухключевой шифр, шифр с открытым ключом** — шифр, в котором используются два ключа, шифрующий и расшифро­вывающий. При этом, зная лишь ключ зашифровывания, нельзя расшифровать сообщение, и наоборот.

**Открытый ключ** — тот из двух ключей асимметричной системы, который свободно распространяется. Шифрующий для секретной переписки и расшифро­вывающий — для электронной подписи.

**Секретный ключ, закрытый ключ** — тот из двух ключей асимметричной системы, который хранится в секрете. Криптоанализ — наука, изучающая мате­матические методы нарушения конфиденциальности и целостности информации.

**Система шифрования (шифрсистема)** — это любая система, которую мо­жно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме адресата.

**Криптостойкостью** — это характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. способность противостоять криптоанализу).

**Криптоаналитик** — учёный, создающий и применяющий методы крипто­анализа. Криптография и криптоанализ составляют криптологию, как единую науку о создании и взломе шифров (такое деление привнесено с запада, до этого в СССР и России не применялось специального деления).

**Криптографическая атака** — попытка криптоаналитика вызвать откло­нения в атакуемой защищённой системе обмена информацией. Успешную криптографическую атаку называют взлом или вскрытие.

**Дешифрование (дешифровка)** — процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного. Тер­мин дешифрование обычно применяют по отношению к процессу криптоанализа шифротекста (криптоанализ сам по себе, вообще говоря, может заключаться и в анализе криптосистемы, а не только зашифрованного ею открытого сообщения).

**Криптографическая стойкость** — способность криптографического алго­ритма противостоять криптоанализу.

**Имитозащита** — защита от навязывания ложной информации. Другими словами, текст остаётся открытым, но появляется возможность проверить, что его не изменяли ни случайно, ни намеренно. Имитозащита достигается обычно за счет включения в пакет передаваемых данных имитовставки.

**Имитовставка** — блок информации, применяемый для имитозащиты, за­висящий от ключа и данных.

**Электронная цифровая подпись(электронная подпись)** — асимметри­чная имитовставка (ключ защиты отличается от ключа проверки). Другими словами, такая имитовставка, которую проверяющий не может подделать.

**Центр сертификации** — сторона, чья честность неоспорима, а открытый ключ широко известен. Электронная подпись центра сертификации подтверждает подлинность открытого ключа.

**Хеш-функция** — функция, которая преобразует сообщение произвольной длины в число («свёртку») фиксированной длины. Для криптографической хеш- функции (в отличие от хеш-функции общего назначения) сложно вычислить обратную и даже найти два сообщения с общей хеш-функцией.

1. Введение

Цель практических работ состоит в изучении основных концепций информационной безопасности, понимание уровней информационной безопасности и целей. Определение угроз на аппаратном и сетевом уровнях.

**Первая работа** изучить основные понятия и уровни информационной безопасности, составляющие и виды информационных угроз. После чего подготовиться к тестированию по заданным аспектам. На занятии разобрать ситуацию по варианту или предложенную руководителем.

**Вторая работа** данная работа предполагает настройку устройства, предположительно компьютера. В практическом занятии студент должен провести настройку компьютера, целью является защита от самых распространённых ошибок допускаемыми системными администраторами небольших фирм. После чего протестировать и оформить результаты в отчёт.

**Третья работа** проведение семинара предполагает ознакомить студента с основными стандартами информационной безопасности. Изучить сервисы и механизмы защиты. Так же предполагает разбор нескольких ситуаций из примеров или предложенные студентами.

**Четвёртая работа** ознакомиться с одним из методов криптографического преобразования информации, а именно стеганографией. Рассмотреть примеры сокрытия данных в файле, использование шумов и стохастической модуляции. Реализовать преобразование одним из методов.

**Пятая работа** разделена на две части. Первая, предполагает изучение методов сжатия данных. Изучение алгоритма Хаффмана и Лемпеля-Зива, реализация сжатия больших текстов и оценка актуальности.

**Шестая работа** является базовой по настройке и работе в сетях, рассматривается вариант «белой», безопасной сети, её подключение и общая настройка прав. Работы выполняются в среде Cisco. Можно использовать другое ПО, если оно предоставляет требуемый функционал.

**Седьмая работа** – это продолжение шестой работы, где студент должен будет реализовать безопасное подключение всей сети к мировой сети Интернет.

**Восьмая работа** настроена на исследование анализа больших потоков данных, прослушивание сети. Тут нужно будет дописать

# Основные понятия безопасности

**Тема:**История, основные понятия и уровни информационной безопасности.

**Цель:**Изучить основные понятия и уровни информационной безопасности, составляющие и виды информационных угроз.

## Теоретические ведомости

### 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:

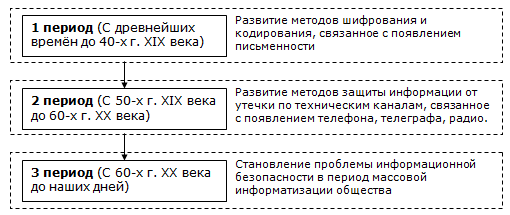


Рисунок . – Периоды развития

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.[3]

**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.

### Составляющие информационной безопасности

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

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

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

**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.[1, 5]

**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.

### Уровни защиты информации

#### 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.

#### 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.

#### 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.

#### 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.

### Виды информационных угроз

Информационные угрозы могут быть обусловлены:

* естественными факторами (пожар, наводнение, и др.);
* человеческими факторами.

Последние, в свою очередь, подразделяются на:

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

## Задания

### 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?

### Рассмотрение 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 выполнения работы

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:
   1. Немедленное блокирование пропуска сотрудницы, выдача нового.
   2. Усиленная проверка входящих в здание по пропускам в течении недели.
   3. Проверка персонала, находящегося в здании.
   4. Добавление/удаление пропусков происходят в следящем режиме.
   5. Сверка активности сотрудницы.
   6. Провести инструктаж на тему "Политика безопасности в организации".

## Варианты задания

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 защите 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.

# Пакети антивірусних програм

**Тема:**Пакети антивірусних програм.

**Мета:**Ознайомлення з основними функціями антивірусного ПЗ. Вивчити сучасні засоби захисту від вірусів.

## Теоретичні відомості

**Шкідлива програма -** будь-яке програмне забезпечення, призначене для отримання несанкціонованого доступу до обчислювальних ресурсів самої ЕОМ або до інформації, що зберігається на ЕОМ, з метою несанкціонованого використання ресурсів ЕОМ або заподіяння шкоди (нанесення збитку) власникові інформації, і/або власнику ЕОМ, і/або власнику мережі ЕОМ, шляхом копіювання, спотворення, видалення або підміни інформації.

### Історія

Сказати, де і коли з'явився перший вірус, неможливо, оскільки таких даних в природі не існує. Якщо на «комп'ютері» Чарльза Беббіджа, «батька» першої обчислювальної машини, вірусів ще не було, до середини семидесятих років минулого століття вони стали вельми поширеним і неприємним для більшості явищем. Проте, передумови до їх створення з'явилися практично відразу ж зі створенням перших ЕОМ.

Ще в 1940 році математик Джон фон Нейман написав книгу [2], в якій були описані математичні автомати, що самовідтворюються, тобто принципи, які лягли в основу всіх вірусів. У 1959 році американський науковий журнал «Scientific American» опублікував статтю Л. Пенроуза, розповідаючу про біологічні структури, що самостійно поширюються. Автор розглянув здатності подібних структур до мутацій, активації і розмноження. Інший вчений, Ф. Шталь, отримані з цієї статті знання реалізував на практиці. Працюючи оператором в науково-дослідній лабораторії, він мав доступ до найпотужнішої на той час ЕОМ - IBM 650. Експеримент дуже здивував Шталя, перевершивши всі його очікування. Одержаний в результаті «мутації» математичних алгоритмів електронний «звір» видалив всі сліди своїх «батьків», які були присутні в системі, після чого самознищився.

Звичайно, всі перераховані вище праці та досліди були спрямовані не для того, щоб нинішні «вірусописателі» щодня викидали в Інтернет мегабайти нової «зарази». Спочатку ці дослідження, що належали до області створення штучного інтелекту, представляли собою академічний інтерес. Однак будь-яке відкриття, зроблене в мирних цілях, може бути без особливих труднощів перетворено в наймогутнішу зброю руйнування.

У 1961 році серед комп'ютерників була дуже популярна гра *«Darwin»*. Її сюжет і сенс були прості: гравець керував «расою», яка повинна була знищити своїх конкурентів. Вигравав той, хто захопить всю віддану під ігровий процес оперативну пам'ять. Особливих дій в грі не було потрібно: необхідно було лише розмножити належачих до своєї раси на вільні комірки ОЗУ або ж захопити комірки противника. Подібний алгоритм дуже схожий на логіку роботи деструктивних програм.

Широке поширення комп'ютерних мереж стало каталізатором появи на світ перших деструктивних програм - *комп'ютерних вірусів*.

#### Конструктори шкідливих програм

У 1992 році хакер, відомий під ніком Dark Avenger, випустив у світ утиліту MtE (Mutation Engine). З її допомогою будь-який, навіть найпримітивніший вірус можна було зробити поліморфним. Цим же людиною був вперше створений вірус Peach, наділений здатністю обходити антивірусне ПЗ. Peach видаляв базу змін програми Central Point AntiVirus. Ця програма, не знаходячи свою базу даних, вважала, що запущена вперше, і створювала її знову. Таким чином, вірус обходив захист і продовжував заражати систему.

Група програмістів, відома в мережі, як Nowhere Man, випустила конструктор вірусів VCL (Virus Creation Laboratory). Відтепер будь-який школяр, навіть не володіючий мовами програмування, міг озброїтися конструктором і зібрати вірус будь-якого типу і руйнівної сили. З появою VCL і так чималий «потік» нових комп'ютерних шкідників став просто величезним.

### Антивірусні склоки

До 1997 року операційна система *Linux*, що раніше вважалася оплотом «чистоти і стабільності», більше не була платформою, вільною від вірусів. Linux.Bliss, що поширювався за допомогою конференцій UseNet, заражав виконувані файли цієї ОС.

У цьому ж році була відзначена поява двох нових типів черв'яків, що розповсюджувалися через IRC і FTP. Особливо великою їх кількістю міг «похвалитися» IRC, багато в чому через свою популярності, а також численних «дірок» mIRC - основного клієнта подібних мереж.

Під кінець ХХ століття в гонитві за лідерством стали нерідкі скандали серед виробників антивірусів. Так, представники компанії McAfee оголосили про те, що її програмісти виявили помилку в антивірусі фірми Dr.Solomon's. Суть заяви зводилася до того, що Dr.Solomon's міг знаходити нові і технічно досконалі віруси тільки в спеціальному «посиленому» режимі, в який переключався лише після знаходження звичайних, примітивних черв'яків. В результаті антивірус показував хороші швидкісні результати при скануванні незаражених дисків, і відмінні показники виявлення при роботі з зараженими файлами. У відповідь Dr.Solomon`s подала позов до суду на McAfee, причиною якого стала її «некоректно побудована рекламна компанія». У підсумку вся «заварушка» завершилася покупкою McAfee контрольного пакета акцій Dr.Solomon`s.

Через деякий час публічну заяву зробили тайванські розробники з фірми Trend Micro, які звинуватили McAfee і Symantec в нібито «порушення їхнього патенту на сканування даних». Світу були відразу представлені докази про «безгрішність» компаній, однак Trend Micro домоглася свого, отримавши відмінну безкоштовну рекламу в засобах масової інформації.

### Класифікація

У компаній-розробників антивірусного програмного забезпечення існують власні класифікації та номенклатури шкідливих програм. Наведена в цій статті класифікація заснована на номенклатурі «Лабораторії Касперського».

#### За шкідливим навантаженням

1. Перешкоди в роботі інфікованого комп’ютера: починаючи від відкриття-закриття піддону CD-ROM і закінчуючи знищенням даних і поломкою апаратного забезпечення. Поломками відомий, зокрема, Win32.CIH.
2. Блокування антивірусних сайтів, антивірусного ПЗ і адміністративних функцій ОС з метою ускладнити лікування.
3. Саботування промислових процесів, що управляються комп'ютером.
4. Інсталяція іншого шкідливого ПЗ.
5. Завантаження з мережі (downloader).
6. Розпаковка іншої шкідливої програми, що уже міститься всередині.
7. Крадіжка, шахрайство, вимагання і шпигунство за користувачем. Для крадіжки може застосовуватися сканування жорсткого диска, реєстрація натискань клавіш (Keylogger) і перенаправлення користувача на підроблені сайти, що в точності повторюють вихідні ресурси.
8. Викрадення даних, що представляють цінність або таємницю.
9. Крадіжка акаунтів різних служб (електронної пошти, месенджерів, ігрових серверів тощо). Акаунти застосовуються для розсилки спаму. Також через електронну пошту часто можна роздобути паролі від інших акаунтів, а віртуальне майно в MMOG - продати.
10. Крадіжка аккаунтів платіжних систем.
11. Блокування комп'ютера, шифрування файлів користувача з метою шантажу і вимагання грошових коштів (див. Ransomware). У більшості випадків після оплати комп'ютер або не розблокується, або незабаром блокується вдруге.
12. Використання телефонного модему для здійснення дорогих дзвінків, що тягне за собою значні суми в телефонних рахунках.
13. Платне ПЗ, що імітує, наприклад, антивірус, але нічого корисного не робить (fraudware або scareware).
14. Інша незаконна діяльність:
15. Отримання несанкціонованого (і/або безкоштовного) доступу до ресурсів самого комп'ютера або третіх ресурсів, доступних через нього, в тому числі пряме управління комп'ютером (так званий backdoor).
16. Організація на комп'ютері відкритих релеїв і загальнодоступних проксі-серверів.
17. Заражений комп'ютер (в складі ботнету) може бути використаний для проведення DDoS-атак.
18. Збір адрес електронної пошти і поширення спаму, в тому числі в складі ботнету.
19. Накрутка електронних голосувань, клацань по рекламних банерам.
20. Генерація монет платіжної системи Bitcoin.
21. Жартівливе ПЗ, що виконує будь-які, турбуючі користувача, речі.
22. Adware — програмне забезпечення, що показує рекламу.
23. Spyware — програмне забезпечення, що займається масовим зборо малоцінної інформації — наприклад, конфігурації комп’ютера, каталогів диску, активності користувача.
24. «Отруєні» документи, які дестабілізують ПЗ, що відкривають їх (наприклад, архів розміром менше мегабайта може містити гігабайти даних і надовго «завісити» архіватор).
25. Програми віддаленого адміністрування можуть застосовуватися як для того, щоб дистанційно вирішувати проблеми з комп'ютером, так і для недобрих цілей.
26. Руткіт потрібен, щоб приховувати інше шкідливе ПЗ від сторонніх очей. Це можливо завдяки тісній інтеграції руткіта з операційною системою.
27. Іноді шкідливе ПЗ для власного «життєзабезпечення» встановлює додаткові утиліти: IRC-клієнти, програмні маршрутизатори, відкриті бібліотеки перехоплення клавіатури ... Таке ПЗ шкідливим не є, але через те, що за ним часто стоїть істинно шкідлива програма, детектується антивірусами. Буває навіть, що шкідливим є тільки скрипт з одного рядка, а решта програми цілком легітимні.
28. Файли, що не є істинно шкідливими, але в більшості випадків небажані.

#### За методом розмноження

*Експлойт* - теоретично нешкідливий набір даних (наприклад, графічний файл або мережевий пакет), некоректно сприймається програмою, що працює з такими даними. Тут шкоди завдає не саме файл, а неадекватна поведінка ПЗ з помилкою. Також експлойтом називають програму для генерації подібних «отруєних» даних.

*Логічна бомба* в програмі спрацьовує при певній умові, і невіддільна від корисної програми-носія.

*Троянська програма*. За своєю дією є протилежністю вірусам і черв'якам. Його пропонують завантажити під виглядом законного додатку, проте замість заявленої функціональності він робить те, що потрібно зловмисникам. Трояни НЕ самовідтворюються і не поширюються самі по собі. Нинішні трояни еволюціонували до таких складних форм, як, наприклад, backdoor (троян, який намагається взяти на себе адміністрування комп'ютера) і троян-завантажувач (встановлює на комп'ютер жертви шкідливий код).

*Комп'ютерний вірус* розмножується в межах комп'ютера і через змінні диски. Розмноження через мережу можливо, якщо користувач сам викладе заражений файл в мережу. Віруси, в свою чергу, діляться за типом файлів, що заражаються (файлові, завантажувальні, макро, що автозапускаються); за способом прикріплення до файлів (паразитуючі, «супутники» і перезаписуючі) і т. д.

*Мережевий черв'як* здатний самостійно розмножуватися по мережі. Діляться на IRC-, поштові, що розмножуються за допомогою експлойтів і т. д.

*Завантажувач* - є невеликою частиною коду, що використовується для подальшого завантаження і установки повної версії. Після того як завантажувач потрапляє в систему шляхом збереження вкладення електронного листа або, наприклад, під час перегляду зараженої картинки, він з'єднується з віддаленим сервером і завантажує весь вірус.

### Види антивірусного захисту

**Сучасні антивіруси** – це комплексні програмні пакети, як правило, містять декілька взаємопов'язаних і взаємодоповнюючих модулів, націлені на боротьбу з усім спектром комп'ютерних загроз.

В сучасних антивірусах можуть бути задіяні такі види антивірусного захисту:

*Порівняння з вірусним зразком* – вірусною сигнатурою коду, шаблоном поведінки шкідливої ​​програми або цифровим відбитком в «чорному» списку відомих загроз. Цей різновид антивірусного захисту полягає в дослідженні підозрілої програми на наявність ознак, характерних для шкідливого ПЗ. Наприклад, реалізуючи даний вид захисту, антивірус шукає сигнатури - послідовності коду, унікальні для певного вірусу.

*Поведінковий моніторинг* – різновид антивірусного захисту, заснований на перевірці об'єктів під час здійснення читання, запису і інших операцій. Для проведення моніторингу антивірусна програма розташовується в оперативній пам'яті і діє як обробник системних подій. При старті будь-якої операції, яка може привести до зараження, антивірусний монітор запускає перевірку оброблюваного об'єкта (документа, програми і т.д.).

*Виявлення змін* – вид антивірусного захисту, який базується на контролі цілісності програмних компонентів комп'ютера. При зараженні віруси модифікують файли, системний реєстр або завантажувальні сектори диска. Антивірусна програма визначає, чи був змінений об'єкт за допомогою підрахунку кодів циклічного контролю (CRC-сум) та інших методів.

*Евристичний аналіз*. Даний вид антивірусного захисту заснований на тому, що виконувані вірусами дії і їх послідовність відрізняються від поведінки більшості програм. Тому аналіз послідовностей команд і системних викликів підозрілого програмного забезпечення допомагає виносити правильне рішення про його шкодочинність.

*Лікування* – різновид антивірусного захисту, що складається у видаленні шкідливих об'єктів і відновлення нормальних параметрів комп'ютерної системи.

*Репутаційний сервіс* – новітній вид антивірусного захисту, що набув поширення в останні роки і базується на перевірці репутації програм, веб-ресурсів та поштових систем. Така перевірка проводиться з використанням «хмарних» серверів репутації, підтримуваних провідними розробниками антивірусного ПЗ, і заснована на постійно оновлюваних списках «легітимних», шкідливих і підозрілих ресурсів. Перевагою репутаційних сервісів є дуже висока швидкість реакції на появу нових загроз.

Існують і застарілі, тепер уже рідко використовувані види антивірусного захисту, наприклад, імунізація, яка полягає в тому, що в пам'яті комп'ютера розміщується програма, що повідомляє вірусам, які уникають повторного зараження, про те, що система вже інфікована.

Реалізують антивірусний захист наступні модулі:

* Антивірусний сканер
* Антивірусний монітор, що використовує баготочисельні технології захисту
* Поведінковий блокувач
* Антивірусний ревізор або система контроля CRC
* Антивірусний фаг або лікар.

## Завдання

1. Підготувати коротку доповідь щодо вибору антивірусного ПЗ для повноцінного захисту. Дозволяється використовувати будь-які доступні джерела інформації.

**Рекомендація:** Зібраний матеріал буде найбільш актуальним, якщо включити в нього дані, отримані практичним шляхом. Для цього при можливості, встановіть демонстраційну версію заданого пакету ПЗ і протестуйте її протягом декількох днів.

1. Створіть таблицю «Оцінка антивірусного ПЗ» де, запишіть переваги і недоліки даного пакета. Дайте оцінку кожному з параметрів на основі підготовленого матеріалу.
2. Провести аналіз зібраної інформації і зробити висновки.

# Мировые стандарты безопасности

**Тема:**Стандарты информационной безопасности распределённых систем.

**Цель:**Изучить сервисы и механизмы защиты распределённых систем. Разбор планирования систем.

## Требования к семинару

### Студент должен знать

1. Основное содержание стандартов по информационной безопасности распределённых систем;
2. Основные сервисы безопасности в вычислительных сетях;
3. Наиболее эффективные механизмы безопасности;
4. Задачи администрирования средств безопасности.

### Студен должен уметь

1. Выбирать механизмы безопасности для защиты распределенных систем.

## Термины для подготовки

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 безопасностиc** – 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.

## Литература для ознакомления

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.

# Методы сокрытия информации

**Тема:**Сокрытие информации. Основы стеганографии.

**Цель:**Ознакомиться с методом стеганографии. Рассмотреть примеры сокрытия информации в файлах, реализовать один из методов.

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Архівація даних

**Тема:**Архівація та резервне копіювання даних.

**Мета:**Дослідження методів стиснення даних, алгоритма Хаффмана і Лемпеля-Зіва.

## Архівація даних

**Архівація (стиснення даних)** – процес подання інформації в іншому вигляді (перекодування) з потенційним зменшенням обсягу, необхідного для її зберігання. Існує безліч класів різних алгоритмів стиснення даних, кожен з яких орієнтований на свою область застосування [4].

Основоположником науки про стиснення інформації прийнято вважати *Клода Шеннона*. Його теорема про оптимальне кодування показує, до чого потрібно прагнути при кодуванні інформації і наскільки та чи інша інформація при цьому стиснеться. Крім того, ним були проведені досліди за емпіричною оцінкою, надмірності англійського тексту. Шеннон пропонував людям вгадувати наступну букву і оцінював вірогідність правильного вгадування. На основі ряду дослідів він прийшов до висновку, що кількість інформації в англійському тексті коливається в межах  біта на символ.

**Стиснення даних** – це процес, що забезпечує зменшення обсягу даних шляхом скорочення їх надмірності. Стиснення даних пов'язано з компактним розташуванням порцій даних стандартного розміру. Стиснення даних можна розділити на два основних типи:

*Стиснення без втрат* (повністю оборотне) – це метод стиснення даних, при якому раніше закодована порція даних відновлюється після їх розпакування повністю без внесення змін. Для кожного типу даних, як правило, існують свої оптимальні алгоритми стиснення без втрат.

*Стиснення з втратами* – це метод стиснення даних, при якому для забезпечення максимального ступеня стиснення вихідного масиву даних частина даних, що містяться в ньому, відкидається. Для текстових, числових і табличних даних використання програм, що реалізують подібні методи стиснення, є неприйнятними. В основному такі алгоритми застосовуються для стиснення аудіо і відео даних, статичних зображень.

### Алгоритми архівації даних

**Алгоритм стиснення даних** – це алгоритм, який усуває надмірність запису даних.

**Відношення стиснення** – одна з найбільш часто використовуваних величин для позначення ефективності методу стиснення.



Значення 0,6 означає, що дані займають 60% від початкового об'єму. Значення більше 1 означають, що вихідний потік більше вхідного.

**Коефіцієнт стиснення** – величина, зворотна відношенню стиснення.



Значення більше 1 позначають стиснення, а значення менше 1 – розширення.

**Середня довжина кодового слова** – це величина, яка обчислюється як зважена можливостями сума довжин всіх кодових слів.

   
де  – ймовірність кодових слів, – довжини кодових слів.

**Статистичні методи** – методи стиснення, які присвоюють коди змінної довжини символам вхідного потоку, причому більш короткі коди присвоюються символам або групам символів, які мають велику ймовірність появи у вхідному потоці. Кращі статистичні методи застосовують кодування Хаффмана.

**Словникове стиснення** – це методи стиснення, що зберігають фрагменти даних в "словнику" (деяка структура даних). Якщо рядок нових даних, що надходять на вхід, ідентичний будь-якому фрагменту, вже знаходиться в словнику, у вихідний потік поміщається покажчик на цей фрагмент. Кращі словникові методи застосовують метод Зіва-Лемпеля.

Розглянемо кілька відомих алгоритмів стиснення даних більш докладно.

#### Алгоритм Хаффмана

В основі алгоритму Хаффмана лежить ідея кодування бітовими групами. Спочатку проводиться частотний аналіз вхідної послідовності даних, тобто встановлюється частота входження кожного символу, що зустрічається в ній. Після цього, символи упорядковано відповідно до зменшення частоти входження.

Основна ідея полягає в наступному: чим частіше зустрічається символ, тим меншою кількістю біт він кодується. Результат кодування заноситься в словник, необхідний для декодування. Розглянемо простий приклад, який ілюструє роботу алгоритму Хаффмана.

Нехай заданий текст «beep boop beer!», Розглянемо таблицю з частотами всіх символів:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Символ** | ‘b’ | ‘e’ | ‘p’ | ‘ ’ | ‘o’ | ‘r’ | ‘!’ |
| **Частота** | 3 | 4 | 2 | 2 | 2 | 1 | 1 |
| За частотою використання | | | | | | | |
| **Символ** | ‘r’ | ‘!’ | ‘p’ | ‘o’ | ‘ ’ | ‘b’ | ‘e’ |

Після цього створимо елементи бінарного дерева для кожного символу і представимо їх як черга з пріоритетом, в якості якого будемо використовувати частоту.

Візьмемо перші два елементи з черги і створимо третій (рис. 5.1), який буде їх батьком. Цей новий елемент помістимо в чергу з пріоритетом, рівним сумі пріоритетів двох його нащадків. Інакше кажучи, що дорівнює сумі їх частот.

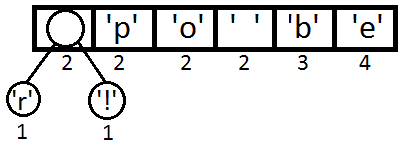
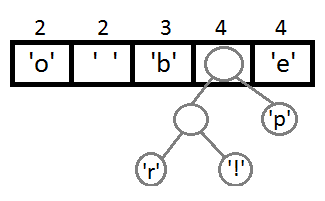
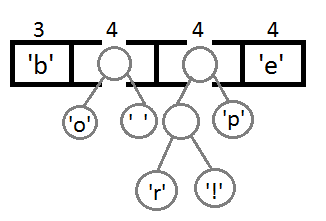
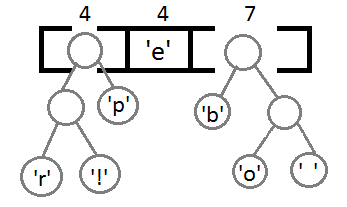


Рисунок .– Приклад об’єднання елементів

Далі будемо повторювати кроки, аналогічні попередньому:







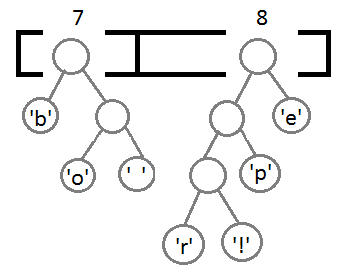


Рисунок . – Побудова дерева

Тепер, після об'єднання останніх двох елементів за допомогою їх нового батька, ми отримаємо підсумкове бінарне дерево:

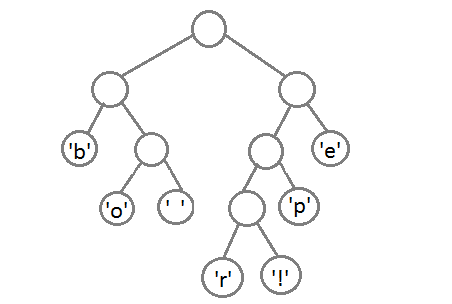


Рисунок . – Вид бінарного дерева

Залишилося присвоїти кожному символу його код (рис. Рисунок 1.1). Для цього запустимо обхід в глибину і кожен раз, розглядаючи праве піддерево, будемо записувати в код 1, а розглядаючи ліве піддерево - 0.

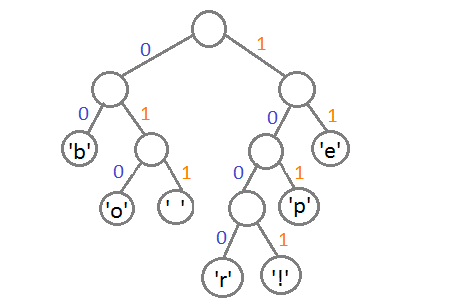


Рисунок . – Побудова кода

В результаті відповідність символів кодовим значенням вийде наступним:

Таблиця . – Кодові значення символів

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Символ** | ‘b’ | ‘e’ | ‘p’ | ‘ ’ | ‘o’ | ‘r’ | ‘!’ |
| **Кодове значення** | 00 | 11 | 101 | 011 | 010 | 1000 | 1001 |

Декодування бітів відбувається наступним чином: потрібно обходити дерево, відкидаючи ліве піддерево, якщо зустрілася одиниця і праве, якщо зустрівся 0. Продовжувати обхід потрібно до тих пір, поки не зустрінемо лист, тобто шукане значення закодованого символу.

Наприклад, закодованому рядку «101 11 101 11» і нашому дереву декодування відповідає рядок «pepe».

**Вхідний рядок:**

beep boop beer!

**Вхідний рядок в двійковому вигляді:**

0110 0010 0110 0101 0110 0101 0111 0000 0010 0000 0110 0010 0110 1111 0110 1111 0111 0000 0010 0000 0110 0010 0110 0101 0110 0101 0111 0010 0010 0001

**Закодований рядок:**

0011 1110 1011 0001 0010 1010 1100 1111 1000 1001

Різниця між ASCII-кодуванням рядка і її ж видом в коді Хаффмана очевидна.

Алгоритм Хаффмана універсальний, його можна застосовувати для стиснення даних будь-яких типів, але він малоефективний для файлів малих розмірів (за рахунок необхідності збереження словника). В даний час даний метод практично не застосовується в чистому вигляді, зазвичай використовується як один з етапів стиснення в більш складних схемах. Це єдиний алгоритм, який не збільшує розмір вихідних даних у гіршому випадку (якщо не брати до уваги необхідність зберігати таблицю перекодування разом з файлом).

#### Алгоритм Лемпеля-Зіва

Процес стиснення виглядає наступним чином. Послідовно зчитуються символи вхідного потоку і відбувається перевірка, чи існує в створеній таблиці рядків такий рядок. Якщо такий рядок існує, зчитується наступний символ, а якщо рядок не існує, в потік заноситься код для попереднього знайденого рядка, рядок заноситься в таблицю, а пошук починається знову. Наприклад, якщо стискають байтові дані (текст), то рядків в таблиці виявиться 256 (від «0» до «255»). Якщо використовується 10-бітний код, то під коди для рядків залишаються значення в діапазоні від 256 до 1023. Нові рядки формують таблицю послідовно, тобто можна вважати індекс рядка її кодом. Алгоритму декодування на вході потрібно тільки закодований текст, оскільки він може відтворити відповідну таблицю перетворення безпосередньо по закодованому тексту. Алгоритм генерує однозначно декодуємий код за рахунок того, що кожен раз, коли генерується новий код, новий рядок додається в таблицю рядків. LZW постійно перевіряє, чи є рядок вже відомим, і, якщо так, виводить існуючий код без генерації нового. Таким чином, кожен рядок буде зберігатися в єдиному екземплярі і мати свій унікальний номер. Отже, при дешифруванні при отриманні нового коду генерується новий рядок, а при отриманні вже відомого, рядок витягується зі словника. [6]

**Кодирование**

Нехай ми стискаємо послідовність (табл.

Таблиця 5.2).

abacabadabacabae

1. Спочатку ініціалізуємо таблицю, додавши в неї все рядки з одного символу.
2. Відповідно до алгоритму, ми додамо до спочатку порожнього рядка *«a»* і перевіримо, чи є рядок *«a»* в таблиці. Оскільки ми при ініціалізації занесли в таблицю всі рядки з одного символу, то рядок *«a»* є в таблиці.
3. Далі ми читаємо наступний символ *«b»* з вхідного потоку і перевіряємо, чи є рядок *«ab»* в таблиці. Такого рядка в таблиці поки немає.
4. Додаємо в таблицю <5> *«ab»*. В потік: <0>;
5. *«ba»* — немає. В таблицю: <6> *«ba»*. В потік: <1>;
6. *«ac»* — немає. В таблицю: <7> *«ac»*. В потік: <0>;
7. *«ca»* — немає. В таблицю: <8> *«са»*. В потік: <2>;
8. *«ab»* — є в таблиці; *«aba»* — немає.

В таблицю: <9> *«aba»*. В потік: <5>;

1. *«ad»* — немає. В таблицю: <10> *«ad»*. В потік: <0>;
2. *«da»* — немає. В таблицю: <11> *«da»*. В потік: <3>;
3. *«aba»* — є в таблиці; *«abac»* — немає.

В таблицю: <12> *«abac»*. В потік:<9>;

1. *«ca»* — є в таблиці; *«cab»* — немає.

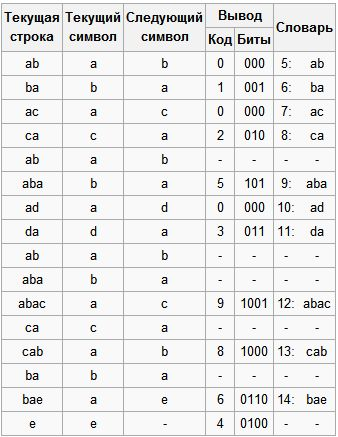
В таблицю: <13> *«cab»*. В потік:<8>;

1. *«ba»* — є в таблиці; *«bae»* — немає.

В таблицю: <14> *«bae»*. В потік:<6>;

Останній рядок *«e»,* за ним іде кінець повідомлення. Виводимо в потік <4>.

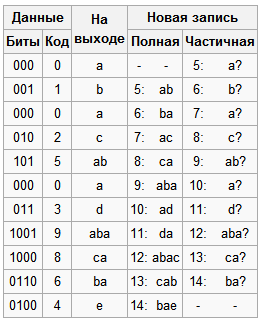
Таблиця 5.2 – Словник кодування LZW



**Декодування**

Особливість LZW полягає в тому, що для декомпресії нам не треба зберігати таблицю рядків в файл для розпакування. Алгоритм побудований таким чином, що ми в змозі відновити таблицю рядків, користуючись тільки потоком кодів. Тепер уявімо, що ми отримали закодоване повідомлення, наведене вище, і нам потрібно його декодувати. Перш за все, нам потрібно знати початковий словник, а наступні записи словника ми можемо реконструювати вже на ходу, оскільки вони є просто конкатенацією попередніх записів.

Таблиця 5.3 – Декодування LZW



**Переваги та недоліки**

* Не вимагає обчислення ймовірностей «зустрічаємості» символів/кодів.
* Даний тип компресії не вносить спотворень в вихідний графічний файл, і підходить для стиснення растрових даних будь-якого типу.
* Для декомпресії не треба зберігати таблицю рядків в файл для розпакування. Алгоритм побудований таким чином, що ми в змозі відновити таблицю рядків, користуючись тільки потоком кодів.
* Алгоритм не проводить аналіз вхідних даних, тому є неоптимальним.

## Завдання

1. Взяти дані відповідно до варіанту із файлу *«Prac5\_Var.txt».*
2. Видалити надлишкову інформацію методом *Хаффмана*.
3. Провести операцію методом *Лемпеля-Зіва*.
4. Порівняти результати проведених операцій.
5. Використовуючи архіватори, стиснути файл (> 4 Гбайт), повторивши кроки 2-4.
6. Описати актуальність архівації для різних об’ємів даних.
7. Зробити висновки щодо застосування методів стиснення в різних криптосистемах.

## Питання для самоконтролю

1. Що таке архівація даних?
2. Мета архівації?
3. Які Ви знаєте методи архівації?
4. Опишіть принцип дерева Хаффмана.
5. Опишіть алгоритм LZ77 або його аналог.
6. Області застосування заданих алгоритмів.
7. Як вибрати алгоритм, якщо дані завчасно відомі?

# Cisco. Часть 1

**Тема:**Тема.

**Цель:**Опишите цель.

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Cisco. Часть 2

**Тема:**Тема.

**Цель:**Опишите цель.

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Анализ данных

**Тема:**Тема.

**Цель:**Опишите цель.

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

1. Додаток А
2. Додаток Б