Титулка

Зміст

[Список сокращений и условных обозначений 5](#_Toc511700509)

[Словарь терминов 6](#_Toc511700510)

[Введение 9](#_Toc511700511)

[1 Основные понятия безопасности 11](#_Toc511700512)

[Теоретические ведомости 11](#_Toc511700513)

[1 Основные понятия информационной безопасности 11](#_Toc511700514)

[2 Составляющие информационной безопасности 13](#_Toc511700515)

[3 Уровни защиты информации 14](#_Toc511700516)

[4 Виды информационных угроз 17](#_Toc511700517)

[Задания 17](#_Toc511700518)

[5 Тестирование 17](#_Toc511700519)

[6 Рассмотрение ситуации 18](#_Toc511700520)

[Пример выполнения работы 18](#_Toc511700521)

[Варианты задания 19](#_Toc511700522)

[2 Локальная защита устройств 21](#_Toc511700523)

[Теоретические ведомости 21](#_Toc511700524)

[Задания 21](#_Toc511700525)

[Ход работы 21](#_Toc511700526)

[Вопросы для самоконтроля 21](#_Toc511700527)

[3 Мировые стандарты безопасности 22](#_Toc511700528)

[Требования к семинару 22](#_Toc511700529)

[1 Студент должен знать 22](#_Toc511700530)

[2 Студен должен уметь 22](#_Toc511700531)

[Термины для подготовки 22](#_Toc511700532)

[Темы для обсуждения 23](#_Toc511700533)

[Литература для ознакомления 23](#_Toc511700534)

[4 Методы сокрытия информации 24](#_Toc511700535)

[Теоретические ведомости 24](#_Toc511700536)

[Задания 24](#_Toc511700537)

[Ход работы 24](#_Toc511700538)

[Вопросы для самоконтроля 24](#_Toc511700539)

[5 Архивация и резервное копирование данных 25](#_Toc511700540)

[Архивация данных 25](#_Toc511700541)

[1 Алгоритмы архивации данных 26](#_Toc511700542)

[Задания 33](#_Toc511700543)

[Часть первая 33](#_Toc511700544)

[Часть вторая 34](#_Toc511700545)

[Ход работы 34](#_Toc511700546)

[Вопросы для самоконтроля 34](#_Toc511700547)

[6 Cisco. Часть 1 35](#_Toc511700548)

[Теоретические ведомости 35](#_Toc511700549)

[Задания 35](#_Toc511700550)

[Ход работы 35](#_Toc511700551)

[Вопросы для самоконтроля 35](#_Toc511700552)

[7 Cisco. Часть 2 36](#_Toc511700553)

[Теоретические ведомости 36](#_Toc511700554)

[Задания 36](#_Toc511700555)

[Ход работы 36](#_Toc511700556)

[Вопросы для самоконтроля 36](#_Toc511700557)

[8 Анализ данных 37](#_Toc511700558)

[Теоретические ведомости 37](#_Toc511700559)

[Задания 37](#_Toc511700560)

[Ход работы 37](#_Toc511700561)

[Вопросы для самоконтроля 37](#_Toc511700562)

[Додаток А 38](#_Toc511700563)

[Додаток Б 39](#_Toc511700564)

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. Вторая, рассматривает резервное сохранение данных, как объект защиты целостности. Ознакомление с возможностями резервного сохранения и различиями реализаций.

**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

# Основні поняття безпеки

**Тема:**Історія, основні поняття і рівні інформаційної безпеки.

**Мета:**Вивчити основні поняття і рівні інформаційної безпеки, складові та види інформаційних загроз.

## Теоретичні відомості

### Основні поняття інформаційної безпеки

Забезпечення захисту інформації хвилювало людство завжди. В процесі еволюції цивілізації змінювалися види інформації, для її захисту застосовувалися різні методи і засоби.

Процес розвитку засобів і методів захисту інформації можна розділити на три відносно самостійних періоди:

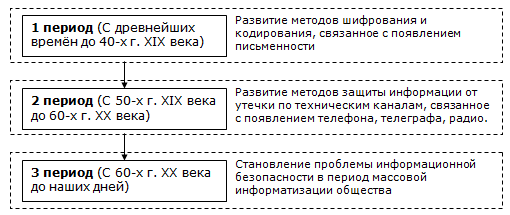


Рисунок 1.1 – Періоди розвитку

Тенденції в розвитку інформаційних технологій, що спостерігаються в останні роки, можуть вже в недалекому майбутньому привести до появи якісно нових (інформаційних) форм боротьби, в тому числі і на міждержавному рівні, які можуть приймати форму інформаційної війни, а сама інформаційна війна стане одним з основних інструментів зовнішньої політики, включаючи захист державних інтересів і реалізацію будь-яких форм агресії. Це є однією з причин, чому корисно ознайомитися з основними принципами забезпечення ІБ в провідних зарубіжних країнах.

Перш ніж говорити про забезпечення безпеки персональних даних, необхідно визначити, що ж таке інформаційна безпека. Термін "інформаційна безпека" може мати різний зміст і трактування в залежності від контексту. В даному посібнику під інформаційною безпекою ми будемо розуміти захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, в тому числі власникам і користувачам інформації і підтримуючої інфраструктури. [2]

**Інформаційна безпека** – це захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати шкоди власникам або користувачам інформації.

У ряді випадків поняття "інформаційна безпека" підміняється терміном "комп'ютерна безпека". У цьому випадку інформаційна безпека розглядається дуже вузько, оскільки комп'ютери тільки одна зі складових інформаційних систем. Незважаючи на це, в рамках курсу, що вивчається основна увага буде приділятися вивченню питань, пов'язаних із забезпеченням режиму інформаційної безпеки стосовно до обчислювальних систем, в яких інформація зберігається, обробляється і передається за допомогою комп'ютерів. Згідно з визначенням, комп'ютерна безпека залежить не тільки від комп'ютерів, але і від підтримуючої інфраструктури, до якої можна віднести системи електропостачання, життєзабезпечення, вентиляції, засоби комунікацій, а також обслуговуючий персонал.

### Складові інформаційної безпеки

Забезпечення інформаційної безпеки в більшості випадків пов'язано з комплексним рішенням трьох завдань:

**Конфіденційність** – стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на нього право.

**Цілісність** – стан інформації, при якому відсутня будь-яка її зміна або зміна здійснюється тільки навмисно суб'єктами, що мають на неї право.

**Доступність** – стан інформації, при якому суб'єкти, які мають право доступу, можуть реалізовувати його безперешкодно.

**Загрози інформаційної безпеки** – сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення безпеки інформації. [1, 4]

**Атака** – це спроба реалізації загрози. Хто робить таку спробу, називається *зловмисником*. Потенційні зловмисники називаються *джерелами загрози*.

Загроза є наслідком наявності вразливих місць або уразливості в інформаційній системі. Уразливості можуть виникати з різних причин, наприклад, в результаті ненавмисних помилок програмістів при написанні програм.

Загрози можна класифікувати за декількома критеріями:

* за властивостями інформації (доступність, цілісність, конфіденційність), проти яких загрози спрямовані в першу чергу;
* за компонентами інформаційних систем, на які загрози націлені (дані, програми, апаратура, інфраструктура);
* за способом здійснення (випадкові/навмисні, дії природного/техногенного характеру);
* за розташуванням джерела загроз (всередині/зовні інформаційної системи, що розглядається).

Забезпечення інформаційної безпеки є складним завданням, для вирішення якого потрібен комплексний підхід.

### Рівні захисту інформації

#### Законодавчий рівень

Законодавчий рівень є основою для побудови системи захисту інформації, так як дає базові поняття предметної області і визначає міру покарання для потенційних зловмисників. Цей рівень відіграє координуючу і спрямовуючу роль і допомагає підтримувати в суспільстві негативне (і каральне) ставлення до людей, які порушують інформаційну безпеку.

Законодавчо-правовий рівень включає комплекс законодавчих та інших правових актів, що встановлюють правовий статус суб'єктів інформаційних відносин, суб'єктів і об'єктів захисту, методи, форми і способи захисту, їх правовий статус. Крім того, до цього рівня відносяться стандарти і специфікації в області інформаційної безпеки. Система законодавчих актів і розроблених на їх базі нормативних і організаційно-розпорядчих документів повинна забезпечувати організацію ефективного нагляду за їх виконанням з боку правоохоронних органів та реалізацію заходів судового захисту та відповідальності суб'єктів інформаційних відносин. До цього рівня можна віднести і морально-етичні норми поведінки, які склалися традиційно або складаються в міру поширення обчислювальних засобів в суспільстві. Морально-етичні норми можуть бути регламентованими в законодавчому порядку, тобто у вигляді зводу правил і приписів. Найбільш характерним прикладом таких норм є Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США. Проте, ці норми здебільшого не є обов'язковими, на відміну від законодавчих заходів.

#### Адміністративний рівень

Це комплекс заходів, що вживаються локально керівництвом організації. Включає комплекс заходів, що взаємно координуються, і технічних заходів, що реалізують практичні механізми захисту в процесі створення і експлуатації систем захисту інформації. Організаційний рівень повинен охоплювати всі структурні елементи систем обробки даних на всіх етапах їх життєвого циклу: будівництво приміщень, проектування системи, монтаж і налагодження обладнання, випробування і перевірки, експлуатація.

Розробка політики безпеки - справа тонка, оскільки у кожної організації є своя специфіка. Тут немає сенсу переносити практику режимних державних організацій на комерційні структури, навчальні заклади або персональні комп'ютерні системи. У цій галузі доцільно запропонувати, по-перше, основні принципи розробки політики безпеки, а, по-друге, - готові шаблони для найбільш важливих різновидів організацій.

#### Процедурний рівень

До процедурного рівня відносяться заходи безпеки, що реалізуються людьми. У вітчизняних організаціях накопичено багатий досвід складання та реалізації процедурних (організаційних) заходів, однак проблема полягає в тому, що вони прийшли з докомп’ютерного минулого, тому потребують суттєвого перегляду.

Можна відзначити наступні групи процедурних мір:

* Управління персоналом;
* фізичний захист;
* підтримка працездатності;
* реагування на порушення режиму безпеки;
* планування відновлювальних робіт.

Для кожної групи в кожній організації має існувати набір регламентів, що визначають дії персоналу. У свою чергу, виконання цих регламентів слід відпрацювати на практиці.

#### Програмно-технічний рівень

Відповідно до сучасних поглядів, даний рівень включає три підрівні: фізичний, технічний (апаратний) і програмний.

Фізичний підрівень вирішує завдання з обмеженням фізичного доступу до інформації та інформаційних систем, відповідно до нього ставляться технічні засоби, що реалізуються у вигляді автономних пристроїв і систем, не пов'язаних з обробкою, зберіганням і передачею інформації: система охоронної сигналізації, система спостереження, засоби фізичного перешкоджання доступу (замки, огорожі, решітки та т. д.).

Засоби захисту апаратного і програмного підрівнів безпосередньо пов'язані з системою обробки інформації. Ці засоби або вбудовані в апаратні засоби обробки, або пов'язані з ними за допомогою стандартного інтерфейсу.

До апаратних засобів відносяться схеми контролю інформації по парності, схеми доступу по ключу і т. д.

До програмних засобів захисту, що утворюють програмний підрівень, відносяться спеціальне програмне забезпечення, що використовується для захисту інформації, наприклад, антивірусний пакет і т. д. Програми захисту можуть бути як окремі, так і вбудовані. Підкреслимо, що формування режиму інформаційної безпеки є складним системним завданням, рішення якого в різних країнах відрізняється за змістом і залежить від таких факторів, як науковий потенціал країни, ступінь впровадження засобів інформатизації в життя суспільства і економіку, розвиток виробничої бази, загальної культури суспільства і, нарешті, традицій і норм поведінки.

### Види інформаційних загроз

Інформаційні загрози можуть бути обумовлені:

* природними факторами (пожежа, повінь тощо);
* людськими факторами.

Останні, в свою чергу, поділяються на:

* Загрози, що носять випадковий, ненавмисний характер. Це загрози, пов'язані з помилками процесу підготовки, обробки і передачі інформації;
* Загрози, обумовлені навмисними діями людей. Це загрози, пов'язані з несанкціонованим доступом до ресурсів АІС.

Умисні загрози мають мету нанесення шкоди користувачам АІС і, в свою чергу, поділяються на активні і пасивні. Загрози також підрозділяються на внутрішні, що виникають всередині керованої організації, і зовнішні.

**Під внутрішніми загрозами** – розуміються загрози безпеки інформації, інсайдером (виконавцем) яких є внутрішній по відношенню до ресурсів організації суб'єкт (інсайдер).

**Під зовнішніми загрозами** – розуміються загрози безпеки інформації, ініціатором (виконавцем) яких є зовнішній по відношенню до ресурсів організації суб'єкт (віддалений хакер, зловмисник).

## Завдання

### Тестування

1. В чому полягає проблема інформаційної безпеки?
2. Дайте визначення поняттю «інформаційна безпека».
3. Що розуміється під «комп’ютерною безпекою»?
4. Перерахуйте складові інформаційної безпеки.
5. Дайте визначення доступності інформації.
6. Дайте визначення цілісності інформації.
7. Дайте визначення конфіденційності інформації.
8. Як пов’язані між собою складові інформаційної безпеки? Наведіть власні приклади.
9. Перерахуйте завдання інформаційної безпеки суспільства.
10. Перерахуйте рівні формування режиму інформаційної безпеки.
11. Дайте коротку характеристику законодавчо-правового рівня.
12. Які підрівні включає програмно-технічний рівень?
13. Що включає адміністративний рівень?
14. У чому особливість морально-етичного підрівня?

### Розгляд ситуації

Оцінивши ситуації згідно варіанту необхідно:

1. Визначити джерело загрози.
2. Визначити постраждалу особу.
3. Класифікувати вид загрози.
4. Визначити загрозу доступності, цілісності, конфіденційності.
5. Організувати заходи по захисту.

Також організувати заходи щодо захисту інформації в даних обставинах і подальше попередження даної моделі.

## Приклад виконання роботи

Співробітниця відділу комерційного банку розмістила фото з id своєї карти в соціальній мережі.

У даній ситуації ми можемо явно бачити, що співробітник допустив халатність. В результаті чого безпека компанії ставиться під сумнів.

1. Джерелом загрози є співробітниця, а так само будь-які особи намагаються проникнути в адміністративну частину будівлі з підробленим пропуском на її ім'я.
2. Постраждалим особою є установа, зокрема відділ з безпеки даного об'єкту. При бездіяльності коло потерпілих осіб може сильно збільшитися.
3. Класифікація загрози:
   * + загроза обумовлена людським фактором;
     + несе випадковий, ненавмисний характер;
     + загроза є внутрішньою.
4. Такі аспекти безпеки як доступність і цілісність не порушені. В даному контексті порушена тільки конфіденційність робочих пропусків компанії
5. Заходи по захисту повинні включати:
   1. Негайне блокування пропуску співробітниці, видача нового.
   2. Посилена перевірка людей, що входять у будинок, за перепустками протягом тижня.
   3. Перевірка персоналу, що знаходиться в будівлі.
   4. Додавання/видалення пропусків відбувається в стежачому режимі.
   5. Звірка активності співробітниці.
   6. Провести інструктаж на тему "Політика безпеки в організації".

## Варіанти завдань

1. Співробітниця відділення комерційного банку розмістила фото з id своєї карти в соціальній мережі.
2. У ЗМІ спливли результати аналізів одного з відомих діячів.
3. Учень, зламавши систему оцінювання коледжу, виправив собі бал з дисципліни.
4. Під час грози були пошкоджені електролінії. У зв'язку з цим більше 200 клієнтів охоронної компанії залишилися без нагляду на 10 годин.
5. Використовуючи прогалину в інтернет-мережі страхової компанії, хакер замінив дані декількох клієнтів.
6. Інтернет-магазин використовує небезпечний канал. Клієнт, зробивши покупку, передав суму третій особі.
7. Підкуплений співробітник, після чого невідомий проник в будівлю відділення поліції.
8. Співробітник аудиторської компанії використовував дані в своїх цілях.
9. Після злому сервера компанії по інформаційному захисту ключі доступу користувачів з'явилися на «чорному ринку».
10. Вночі із офісу було викрадено печатку адвоката, об'єкт знаходиться під охороною.
11. Співробітник компанії з розробки ПЗ приховано вставляв моніторинг в продукт.
12. Збій в роботі компанії по забезпеченню vps серверів.
13. Виявлено затримку інтернет каналу біржі. Імовірно зловмисники, підключившись до каналу отримують дані першими.
14. Співробітник не дотримувався правил виробництва. У зв'язку з чим завод втратив кілька партій товару.
15. Зависання інформаційної системи на залізниці призвело до зіткнення поїздів.
16. Офіс туристичної компанії був затоплений під час стихійного лиха.

# Локальная защита устройств

**Тема:**Настройка системы от внутренних и внешних угроз.

**Цель:**Определить цели и методы для настройки устройств, на практике реализовать защиту локального устройства.

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# 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

# Архивация и резервное копирование данных

**Тема:**Архивация и резервное копирование данных.

**Цель:**Изучение методов сжатия данных, алгоритма Хаффмана и Лемпеля-Зива. Рассмотреть резервное копирование данных.

## Архивация данных

**Архивация (сжатие данных)** – есть процесс представления информации в ином виде (перекодирования) с потенциальным уменьшением объёма, требуемого для её хранения. Существует множество классов различных алгоритмов сжатия данных, каждый из которых ориентирован на свою область применения[3].

Основоположником науки о сжатии информации принято считать *Клода Шеннона*. Его теорема об оптимальном кодировании показывает, к чему нужно стремиться при кодировании информации и насколько та или иная информация при этом сожмется. Кроме того, им были проведены опыты по эмпирической оценке, избыточности английского текста. Шеннон предлагал людям угадывать следующую букву и оценивал вероятность правильного угадывания. На основе ряда опытов он пришел к выводу, что количество информации в английском тексте колеблется в пределах  бита на символ. Несмотря на то, что результаты исследований Шеннона были по-настоящему востребованы лишь десятилетия спустя, трудно переоценить их значение.

**Сжатие данных** – это процесс, обеспечивающий уменьшение объёма данных путём сокращения их избыточности. Сжатие данных связано с компактным расположением порций данных стандартного размера. Сжатие данных можно разделить на два основных типа:

**Сжатие без потерь** (полностью обратимое) – это метод сжатия данных, при котором ранее закодированная порция данных восстанавливается после их распаковки полностью без внесения изменений. Для каждого типа данных, как правило, существуют свои оптимальные алгоритмы сжатия без потерь.

**Сжатие с потерями** – это метод сжатия данных, при котором для обеспечения максимальной степени сжатия исходного массива данных часть содержащихся в нём данных отбрасывается. Для текстовых, числовых и табличных данных использование программ, реализующих подобные методы сжатия, является неприемлемыми. В основном такие алгоритмы применяются для сжатия аудио и видеоданных, статических изображений.

### Алгоритмы архивации данных

**Алгоритм сжатия данных** – это алгоритм, который устраняет избыточность записи данных.

**Отношение сжатия** – одна из наиболее часто используемых величин для обозначения эффективности метода сжатия.



Значение 0,6 означает, что данные занимают 60% от первоначального объема. Значения больше 1 означают, что выходной поток больше входного (отрицательное сжатие, или расширение).

**Коэффициент сжатия** – величина, обратная отношению сжатия.



Значения больше 1 обозначают сжатие, а значения меньше 1 расширение.

**Средняя длина кодового слова** – это величина, которая вычисляется как взвешенная вероятностями сумма длин всех кодовых слов.

   
где  – вероятности кодовых слов, – длины кодовых слов.

**Статистические методы** – методы сжатия, присваивающие коды переменной длины символам входного потока, причем более короткие коды присваиваются символам или группам символам, имеющим большую вероятность появления во входном потоке. Лучшие статистические методы применяют кодирование Хаффмана.

**Словарное сжатие** – это методы сжатия, хранящие фрагменты данных в "словаре" (некоторая структура данных). Если строка новых данных, поступающих на вход, идентична какому-либо фрагменту, уже находящемуся в словаре, в выходной поток помещается указатель на этот фрагмент. Лучшие словарные методы применяют метод Зива-Лемпела.

Рассмотрим несколько известных алгоритмов сжатия данных более подробно.

#### Алгоритм Хаффмана

В основе алгоритма Хаффмана лежит идея кодирования битовыми группами. Сначала проводится частотный анализ входной последовательности данных, то есть устанавливается частота вхождения каждого символа, встречащегося в ней. После этого, символы сортируются по уменьшению частоты вхождения.

Основная идея состоит в следующем: чем чаще встречается символ, тем меньшим количеством бит он кодируется. Результат кодирования заносится в словарь, необходимый для декодирования. Рассмотрим простой пример, иллюстрирующий работу алгоритма Хаффмана.

Пусть задан текст «beep boop beer!», рассмотрим таблицу с частотами всех символов:



После этого создадим элементы бинарного дерева для каждого символа и представим их как очередь с приоритетом, в качестве которого будем использовать частоту.

Возьмём первые два элемента из очереди и создадим третий(рис. Рисунок 5.1), который будет их родителем. Этот новый элемент поместим в очередь с приоритетом, равным сумме приоритетов двух его потомков. Иначе говоря, равным сумме их частот.

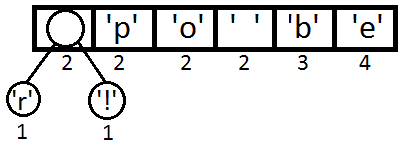
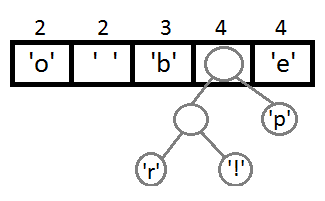
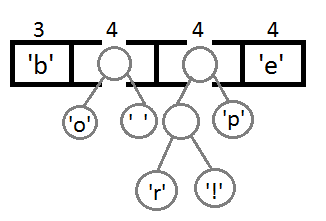
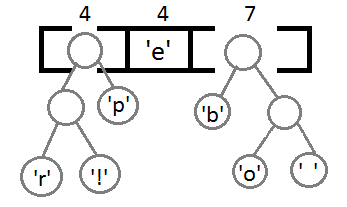


Рисунок .– Пример объединения элементов

Далее будем повторять шаги, аналогичные предыдущему:







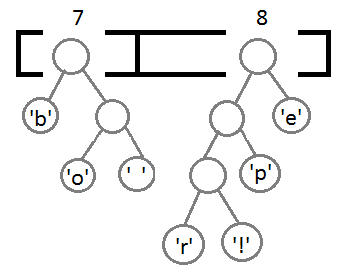


Рисунок . – Построение дерева

Теперь, после объединения последних двух элементов с помощью их нового родителя, мы получим итоговое бинарное дерево:

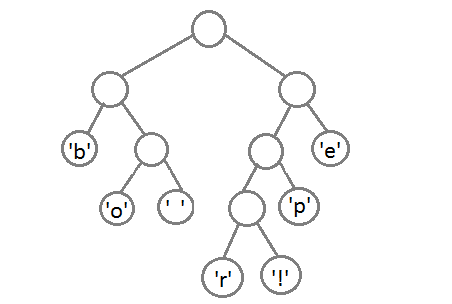


Рисунок . – Вид бинарного дерева

Осталось присвоить каждому символу его код(рис. Рисунок 1.1). Для этого запустим обход в глубину и каждый раз, рассматривая правое поддерево, будем записывать в код 1, а рассматривая левое поддерево – 0.

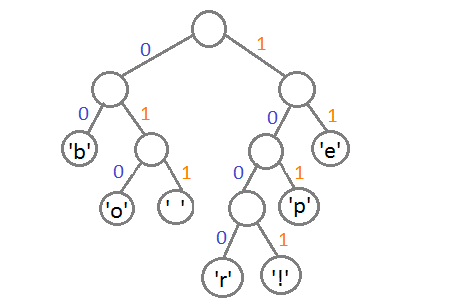


Рисунок . – Построение кода

В результате соответствие символов кодовым значениям получится следующим:



Декодирование битов происходит следующим образом: нужно обходить дерево, отбрасывая левое поддерево, если встретилась единица и правое, если встретился 0. Продолжать обход нужно до тех пор, пока не встретим лист, т.е. искомое значение закодированного символа.

Например, закодированной строке «101 11 101 11» и нашему дереву декодирования соответствует строка «pepe».

**Входная строка:**

beep boop beer!

**Входная строка в двоичном виде:**

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

**Закодированная строка:**

0011 1110 1011 0001 0010 1010 1100 1111 1000 1001

Разница между ASCII-кодировкой строки и её же видом в коде Хаффмана очевидна.

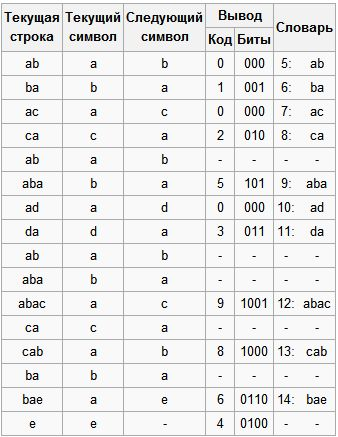
Алгоритм Хаффмана универсальный, его можно применять для сжатия данных любых типов, но он малоэффективен для файлов маленьких размеров (за счет необходимости сохранения словаря). В настоящее время данный метод практически не применяется в чистом виде, обычно используется как один из этапов сжатия в более сложных схемах. Это единственный алгоритм, который не увеличивает размер исходных данных в худшем случае (если не считать необходимости хранить таблицу перекодировки вместе с файлом).

#### Алгоритм Лемпеля-Зива

Процесс сжатия выглядит следующим образом. Последовательно считываются символы входного потока и происходит проверка, существует ли в созданной таблице строк такая строка. Если такая строка существует, считывается следующий символ, а если строка не существует, в поток заносится код для предыдущей найденной строки, строка заносится в таблицу, а поиск начинается снова. Например, если сжимают байтовые данные (текст), то строк в таблице окажется 256 (от «0» до «255»). Если используется 10-битный код, то под коды для строк остаются значения в диапазоне от 256 до 1023. Новые строки формируют таблицу последовательно, т. е. можно считать индекс строки ее кодом. Алгоритму декодирования на входе требуется только закодированный текст, поскольку он может воссоздать соответствующую таблицу преобразования непосредственно по закодированному тексту. Алгоритм генерирует однозначно декодируемый код за счет того, что каждый раз, когда генерируется новый код, новая строка добавляется в таблицу строк. LZW постоянно проверяет, является ли строка уже известной, и, если так, выводит существующий код без генерации нового. Таким образом, каждая строка будет храниться в единственном экземпляре и иметь свой уникальный номер. Следовательно, при дешифровании при получении нового кода генерируется новая строка, а при получении уже известного, строка извлекается из словаря.[5]

**Кодирование**

Пусть мы сжимаем последовательность <<abacabadabacabae>>.



Мы получаем закодированное сообщение:

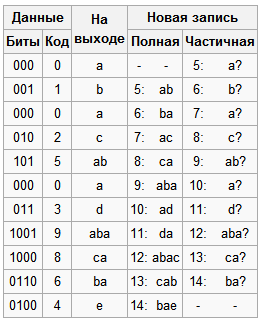
0 1 0 2 5 0 3 9 8 6 4

что на 11- бит короче.

000 001 000 010 101 000 011 1001 1000 0110 0100

**Декодирование**

Особенность LZW заключается в том, что для декомпрессии нам не надо сохранять таблицу строк в файл для распаковки. Алгоритм построен таким образом, что мы в состоянии восстановить таблицу строк, пользуясь только потоком кодов. Теперь представим, что мы получили закодированное сообщение, приведённое выше, и нам нужно его декодировать. Прежде всего, нам нужно знать начальный словарь, а последующие записи словаря мы можем реконструировать уже на ходу, поскольку они являются просто конкатенацией предыдущих записей.



**Достоинства и недостатки**

* Не требует вычисления вероятностей встречаемости символов или кодов.
* Для декомпрессии не надо сохранять таблицу строк в файл для распаковки. Алгоритм построен таким образом, что мы в состоянии восстановить таблицу строк, пользуясь только потоком кодов.
* Данный тип компрессии не вносит искажений в исходный графический файл, и подходит для сжатия растровых данных любого типа.
* Алгоритм не проводит анализ входных данных поэтому не оптимален.

## Задания

### Часть первая

1. Взять данные соответственно варианту из таблицы
2. Удалить лишнюю информацию методом Хаффмана.
3. Провести операцию методом Лемпеля-Зива.
4. Сравнить результаты проведённых операций.
5. Описать актуальность архивации для различных объёмов данных.
6. Сделать выводы по применению методов сжатия в различных криптосистемах.

### Часть вторая

## Ход работы

## Вопросы для самоконтроля

# 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