МАМАРАЖАБОВ МИРСАЛИМ,
ЮСУПОВА ГУЛЬЧЕХРА

Учебное пособие по дисциплине ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИНТЕРНЕТ

УДК: 681.142.37
ББК: 73.6
М 22

Данное учебное пособие предназначено для обучения студентов высших педагогических образовательных учреждений направления специальности 601120000 – «допризывная военная подготовка» по учебной дисциплине «Информационная безопасность и интернет».

Учебное пособие рекомендовано студентам педагогических университетов и институтов, а также учителям школ, академических лицеев, слушателям институтов и факультетов повышения квалификации.

This textbook is intended for training students in higher pedagogical educational institutions specializing in the field of "601120000 – Pre-Conscription Military Training" for the course "Information Security and the Internet." The textbook is recommended for students of pedagogical universities and institutes, as well as for school teachers, academic lyceum educators, and attendees of institutes and faculties for professional development.

ISBN: 978-9910-639-20-3

Рецензенты: Доцент кафедры «Математика и ИТО» ТГПУ имени Низами — Д.ф.п.н.(PhD) Умарова З.А.

Заведующая кафедры «Общеобразовательные предметы» Университета «Янги аср» доцент — д.ф.п.н.(PhD) Бекчонова Ш.Б.

7513

Muharrir: Sh.Muhammedov
Texnik muharrir: G. Ne'matova
Dizayner: S.Jiyanov
Sahifalovchi: SH. Muhiddinov

Nashr. lits. № 220812 08.02.2024.
Bosmaxonaga berildi: 27.12.2024. Bosishga ruxsat etildi: 26.02.2025.
Bichimi 60x84 1/16 Offset qog'ozi. Times New Roman garniturasi.
Shartli bosma tabog'i 11,25. Nashr hisob tabog'i 6,1.
Adadi 50 nusxada. Buyurtma № 05-03.
"ZUXRO BARAKA BIZNES" nashriyoti.
Toshkent shahar, Yakkasaroy tumani
Yusuf Xos Xojib ko'chasi 103 uy.

Bosmaxona. lits. № 220812 08.02.2024.
«ZUXRO BARAKA BIZNES» bosmaxonasida chop etildi. Toshkent shahri Bunyodkor shoh ko'chasi 27 A–uy.

МИНИСТЕРСТВО ДОШКОЛЬНОГО И ШКОЛЬНОГО ОБРАЗОВА РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ НИЗАМИ

Кафедра "Информационные технологии"

МАМАРАЖАБОВ МИРСАЛИМ ЭЛЬМИРЗАЕВИЧ
ЮСУПОВА ГУЛЬЧЕХРА ЮЛДАШОВНА

Учебное пособие по дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИНТЕРНЕТ

Ташкент-2025

УДК: 681.142.37
ББК: 73.6
М 22

Данное учебное пособие предназначено для обучения студентов высших педагогических образовательных учреждений направления специальности 601120000 – «допризывная военная подготовка» по учебной дисциплине «Информационная безопасность и интернет».

Учебное пособие рекомендовано студентам педагогических университетов и институтов, а также учителям школ, академических лицеев, слушателям институтов и факультетов повышения квалификации.

This textbook is intended for training students in higher pedagogical educational institutions specializing in the field of "601120000 – Pre-Conscription Military Training" for the course "Information Security and the Internet." The textbook is recommended for students of pedagogical universities and institutes, as well as for school teachers, academic lyceum educators, and attendees of institutes and faculties for professional development.

ISBN: 978-9910-639-20-3

Рецензенты: Доцент кафедры «Математика и ИТО» ТГПУ имени Низами — Д.ф.п.н.(PhD) Умарова З.А.

Заведующая кафедры «Общеобразовательные предметы» Университета «Янги аср» доцент — д.ф.п.н.(PhD) Бекчонова Ш.Б.

Оглавление

ПРЕДИСЛОВИЕ 4

I-ГЛАВА. Понятие информации. Информационные системы и безопасность. 5

§1.1. Понятие информации. Понятие информационной системы. 5

§1.2. Защита информации и ее виды. 22

§1.3. Основные понятия информационной безопасности. 37

2-ГЛАВА. Методы защиты информации 53

§2.4. Основы защиты информации. 53

§2.5. Основы криптосистемы. 69

§2.6. Безопасность в информационных системах. 91

3-ГЛАВА. Методы защиты и защиты информации в сети, Интернет-системе и электронной почте 105

§3.7. Организация защиты сети Интернет 105

§3.8. Сетевая безопасность..... 131

§3.9. Правовая законодательная база для определения информационного преступления 146

§3.10. Критическое использование СМИ...... 161

ГЛОССАРИЙ 173

Список использованной литературы.....176

ПРЕДИСЛОВИЕ

Цель преподавания дисциплины – развитие представлений будущего преподавателя об информационной безопасности и ее угрожающих причинах, которые необходимо усвоить в его профессиональной сфере, об информационной безопасности, интернет-безопасности и криптографии, понимание информационных систем и защищенных информационных систем, стандарты, обеспечивающие информационную безопасность, модели, обеспечивающие информационную безопасность, методы защиты информации, программные и технические средства, обеспечивающие безопасность информационных систем инструменты, средства защиты операционной системы, заключается в формировании навыков формирования теоретической и практической значимости информации о безопасности в электронной почте и интернете.

Задача дисциплины-дать студентам-предметникам теоретические знания, практические умения и навыки. развивать свое видение информационной безопасности и причин, ее угрожающих, развивать понимание информационных систем и защищенных информационных систем, знание стандартов и моделей, обеспечивающих информационную безопасность, знания о том, как использовать методы защиты и защиты информации.

I-ГЛАВА. Понятие информации. Информационные системы и безопасность.

§1.1. Понятие информации. Понятие информационной системы.

Понятие информации и ее виды, объяснение способов получения, хранения и обработки информации. Классификация и виды каналов распространения информации. Технические и организационные меры противодействия утечке информации по возможным каналам утечки.

Понятие информации

Что такое информация? В самом общем смысле,

> Информация - это данные, организованные таким образом, чтобы они были полезными и понятными для получателя.

Это может быть любая форма данных, которые имеют смысл для

> Информация - это то, что дает нам знания, понимание или просто помогает нам узнавать о мире вокруг нас.

нас и помогают нам принимать решения или действовать.

Виды информации

Рассмотрим это поподробнее.

Пример 1. Возьмем книгу. Каждая страница этой книги содержит буквы, слова, предложения. Это данные. Когда вы читаете эти данные и понимаете смысл, который автор хочет донести, это уже информация для вас.

Пример 3. Вы слушаете радио. Звук, который вы слышите, - это данные. Но когда это музыка, новости или интересное интервью, это уже информация, которую вы воспринимаете.

Таким образом, информация - это не просто поток данных, но что-то, что имеет смысл и ценность для того, кто ее получает.

Информация - это данные, которые предоставляют нам знания или понимание о мире вокруг нас. Она может быть представлена в различных формах, таких как текст, изображения, звуки и многое другое.

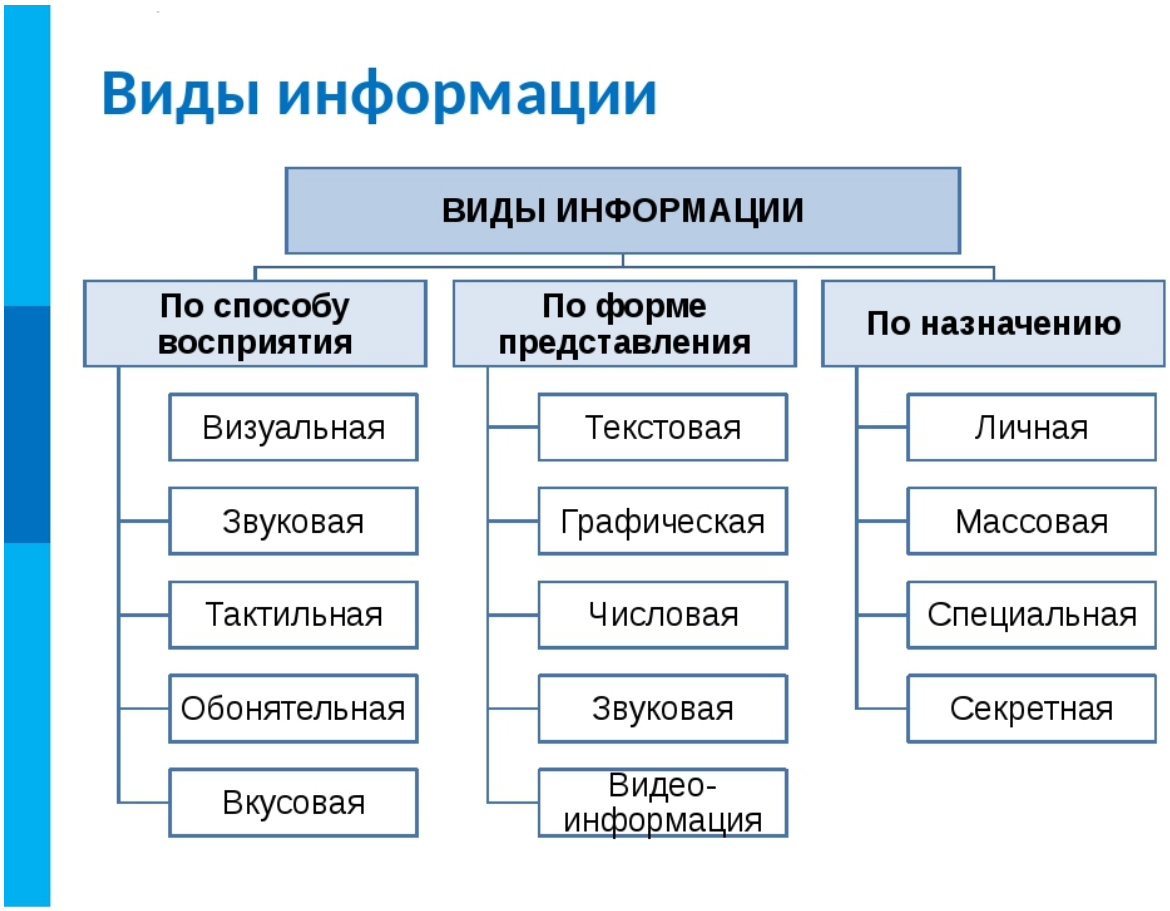

Рисунок 1.1 Виды информации

Информация помогает нам принимать решения, понимать ситуации и взаимодействовать с окружающим миром.

Рисунок 1.2. Передача информации

На рисунке 1.2. один из примеров, который иллюстрирует передачу информации.

На этом рисунке изображены два человека, обменивающихся информацией. Один человек говорит (предоставляет информацию), а другой слушает (принимает информацию).

Это иллюстрирует процесс коммуникации, в котором одна сторона передает сообщение (информацию), а другая сторона его воспринимает. Как видно, рисунок является визуальным представлением процесса передачи информации между людьми.

Восприятие информации происходит через различные органы чувств, которые передают сигналы в мозг для обработки. Вот основные органы чувств и их роли в восприятии информации.

1. Зрение (глаза). Глаза играют ключевую роль в восприятии визуальной информации. Они преобразуют свет в нервные импульсы, которые передаются в зрительные центры мозга для обработки. Зрительная информация помогает нам видеть и понимать окружающий мир.

2. Слух (уши). Уши позволяют нам воспринимать звуковую информацию. Звуки преобразуются в нервные сигналы в ушной раковине, затем передаются в мозг для интерпретации. Аудиальная информация помогает нам слышать речь, звуки окружающей среды и музыку.

3. Обоняние (нос). Нос позволяет нам воспринимать запахи. Обонятельные рецепторы в носу обнаруживают химические вещества в воздухе и передают сигналы в мозг для анализа. Запаховая информация помогает нам определять ароматы еды, цветов и других предметов.

4. Осязание (кожа). Кожа является основным органом осязания. Она содержит рецепторы, которые чувствуют прикосновения, давление, температуру и боль. Осязательная информация помогает нам ощущать текстуры, формы и тепло окружающих предметов.

5. Вкус (язык). Язык содержит рецепторы, которые чувствуют различные вкусы. сладкий, кислый, соленый, горький и умами (вкус, присущий богатым белковым продуктам). Вкусовая информация помогает нам определять пищу и оценивать ее качество.

6. Равновесие (вестибулярный аппарат в ухе). Вестибулярный аппарат в ухе помогает нам ощущать равновесие и координацию движений. Он чувствует изменения положения головы и передает сигналы в мозг для поддержания равновесия.

Эти органы чувств работают вместе, чтобы предоставить нам полную картину о мире вокруг нас, позволяя воспринимать различные виды информации и реагировать на нее соответствующим образом.

Основные свойства информации.

1. *Достоверность*- одно из наиболее важных свойств информации - это ее достоверность. Информация должна быть точной и достоверной, чтобы мы могли полагаться на нее при принятии решений или совершении действий. Недостоверная информация может привести к ошибочным выводам и неправильным действиям.
2. *Полнота*- информация должна быть полной, чтобы предоставить нам всю необходимую информацию о ситуации или предмете. Неполная информация может привести к недопониманию или неправильным выводам.
3. *Точность*- информация должна быть точной и без ошибок. Неточная информация может привести к недопониманию или неправильным решениям.
4. *Актуальность*- информация должна быть актуальной и соответствовать текущему состоянию ситуации или предмета. Устаревшая информация может быть бесполезной или даже вредной.
5. *Понятность*- информация должна быть представлена таким образом, чтобы ее было легко понять и интерпретировать. Сложная или непонятная информация может вызвать путаницу или непонимание.
6. *Релевантность*- информация должна быть связана с темой или вопросом, который мы рассматриваем. Нерелевантная информация

может отвлечь нас от основной темы или привести к неправильным выводам.

7. *Доступность*- информация должна быть доступной в нужное время и место. Недоступная информация может препятствовать принятию решений или выполнению задач.

Рисунок 1.3. Свойства информации

Эти свойства помогают нам оценивать качество и значимость информации, а также делать осознанные и информированные решения в различных ситуациях.

Единицы измерения информации

Ответим на вопрос как измеряется информация, которая окружает нас в повседневной жизни, и какие единицы используются для этого.

Как мы можем измерить количество информации? Для этого существуют специальные единицы измерения. Давайте рассмотрим несколько из них.

1. Бит (bit). Бит - самая маленькая единица информации. Он представляет собой единичный символ, который может быть либо

0, либо 1. Например, биты используются для кодирования данных в компьютерных системах.
2. Байт (byte). Байт состоит из 8 битов. Он используется для хранения одного символа текста или одного буквенного символа на компьютере. Например, слово "hello" состоит из 5 байтов.
3. Килобайт (KB). Килобайт состоит из 1024 байтов. Он используется для измерения небольших объемов данных, таких как текстовые файлы или небольшие изображения.
4. Мегабайт (MB). Мегабайт состоит из 1024 килобайтов. Он используется для измерения средних объемов данных, таких как музыкальные файлы или фотографии.
5. Гигабайт (GB). Гигабайт состоит из 1024 мегабайтов. Он используется для измерения больших объемов данных, таких как видеофайлы или программы.
6. Терабайт (TB). Терабайт состоит из 1024 гигабайтов. Он используется для измерения очень больших объемов данных, таких как базы данных или хранилища в облаке.
Мы рассмотрели основные единицы измерения информации, которые помогают нам оценить объем данных в различных контекстах. Понимание этих единиц поможет нам лучше ориентироваться в мире информации и использовать ее более эффективно в нашей повседневной жизни.
Теперь рассмотрим более крупные единицы измерения информации.
7. Петабайт (PB). Петабайт состоит из 1024 терабайтов или 1,125,899,906,842,624 байтов. Эта единица измерения используется для описания огромных объемов данных, например, для хранения информации на серверах крупных компаний или в крупных исследовательских проектах.
8. Эксабайт (EB). Эксабайт состоит из 1024 петабайтов. Это огромное количество данных, которое может быть использовано для хранения информации в самых крупных глобальных сетях, таких как Интернет, или для обработки больших массивов данных в научных и коммерческих проектах.

9. Зеттабайт (ZB). Зеттабайт состоит из 1024 эксабайтов. Эта единица измерения информации представляет собой крайне огромный объем данных и может использоваться для хранения данных на глобальном уровне или для обработки информации в крупных научных проектах, таких как исследования космоса или геномные исследования.
10. Йоттабайт (YB). Йоттабайт состоит из 1024 зеттабайтов. Это астрономический объем данных, который в настоящее время является максимально возможным для практического использования. Его можно использовать для описания объемов информации в крупных мировых системах, таких как общие базы данных или хранилища данных на уровне стран или регионов.

Рисунок 1.4. Единицы измерения информации

Эти крупные единицы измерения информации представляют собой огромные объемы данных, которые становятся все более важными в современном мире, где информация играет ключевую роль во многих аспектах жизни, от научных исследований до коммерческих операций и общественной жизни.

Понятие информационной системы

Теперь перейдем к понятию информационной системы. Это уже более сложное понятие.

> Информационная система - это система, которая собирает, обрабатывает, хранит и распространяет информацию для

Давайте разберемся.

Пример 1. Представьте себе большой офис. Там работают люди, у них есть компьютеры, сеть интернета, базы данных с информацией о клиентах и продукции. Все это вместе и есть информационная система офиса, которая помогает работать более эффективно.

Пример 2. Возьмем интернет-магазин. Это тоже информационная система. Она содержит в себе каталог товаров, базу данных клиентов, систему оплаты и многое другое. Все это объединено для того, чтобы покупатели могли легко выбирать и заказывать товары.

Таким образом, информационные системы - это не просто компьютеры и программы. Это целые комплексы, объединяющие в себе различные технологии и ресурсы для обработки информации.

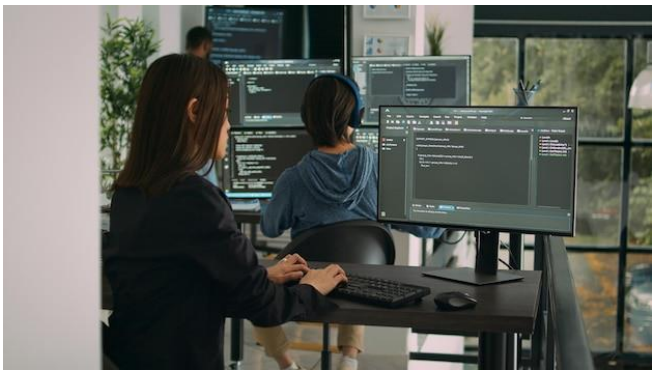

Рисунок 1.5. Применение информационной системы.

Вот пример рисунка 1.5, иллюстрирующего информационную систему.

На этом рисунке изображена простая информационная система, состоящая из четырех основных компонентов. пользователей, аппаратных средств (компьютеров), программного обеспечения и баз данных.

1. *Пользователи*- это люди, которые взаимодействуют с информационной системой, вводя данные, получая информацию или выполняя операции.
2. *Компьютеры (аппаратные средства)*- это устройства, на которых работает информационная система. Они могут быть как персональными компьютерами, так и серверами, используемыми для обработки и хранения данных.
3. *Программное обеспечение*- это программы и приложения, которые управляют работой информационной системы. Они могут включать в себя операционные системы, базы данных, приложения для работы с данными и другие программы.
4. *Базы данных*- это хранилища данных, используемые информационной системой для хранения информации. Они могут содержать различные типы данных, такие как текст, изображения, видео и многое другое.

Этот рисунок демонстрирует, как компоненты информационной системы взаимодействуют друг с другом для обработки, хранения и передачи информации, что делает ее полезной для пользователей. Информационная система - это специально организованный набор элементов, которые собирают, обрабатывают, хранят и передают информацию. Эти элементы могут включать в себя людей, компьютеры, программное обеспечение, базы данных и многое другое. Информационные системы могут быть очень разнообразными, от простых систем хранения данных до сложных корпоративных сетей.

Примеры и реальные факты

1. *Социальные сети*. Например, Facebook или Instagram - это информационные системы, которые позволяют людям обмениваться информацией, фотографиями и видео. Они собирают информацию о пользователях, их предпочтениях и взаимодействиях, чтобы предлагать персонализированный контент.

2. *Банковские системы*. Банки используют информационные системы для обработки транзакций, хранения данных клиентов и предоставления онлайн-банкинга. Это позволяет клиентам осуществлять операции со своими счетами и получать информацию о своих финансах в любое время и в любом месте.

3. *Медицинские информационные системы*. Врачи и медицинские учреждения используют информационные системы для управления медицинскими записями пациентов, назначения лечения и обмена данными между специалистами. Это помогает улучшить качество медицинского обслуживания и повысить безопасность пациентов.

4. *Образовательные информационные системы*. Школы и университеты используют информационные системы для управления учебными планами, записью студентов, оцениванием успеваемости и обмена учебными материалами. Это делает процесс обучения более эффективным и доступным.

5. *Транспортные информационные системы*. Городские и междугородние системы транспорта используют информационные системы для отслеживания расписания, управления билетами и обеспечения безопасности пассажиров. Например, системы GPS в автомобилях и на транспорте общего пользования помогают оптимизировать маршруты и избегать пробок.

Эти примеры демонстрируют, как информационные системы влияют на различные аспекты нашей жизни, улучшая коммуникацию, управление, принятие решений и повышая эффективность различных отраслей.
Сегодня мы рассмотрели понятия информации и информационной системы. Информация - это данные, приобретающие смысл. Информационная система - это комплекс технологий и ресурсов, предназначенных для работы с этой информацией.

Нужно помнить, что информация - это важнейший ресурс в современном мире, и умение эффективно управлять ею является ключом к успеху во многих областях жизни.

Технические и организационные меры противодействия утечке информации

Ответим на вопрос как предотвратить утечку информации через различные каналы. Это важно как для индивидуальной безопасности, так и для защиты конфиденциальных данных организаций. Для начала разберемся, что такое утечка информации и какие каналы она может использовать.

Что такое утечка информации?

Утечка информации – это неправомерное раскрытие конфиденциальных данных или передача информации третьим лицам без разрешения. Это может происходить через различные каналы: начиная от утери документов и заканчивая взломом компьютерных систем.

Возможные каналы утечки информации.

1. *Физические носители данных*. утеря или кража документов, USB-накопителей, ноутбуков и т.д.
2. *Компьютерные системы*. взлом компьютеров, кража паролей, использование вредоносных программ.
3. *Коммуникационные каналы*. перехват электронной почты, прослушивание телефонных разговоров.
4. *Социальная инженерия*. обман и манипуляции для получения доступа к информации.

Теперь перейдем к вопросу, каким образом мы можем защититься от утечки информации.

Рисунок 1.6. Носители информации

Пример рисунка 1.6., иллюстрирующего возможные каналы утечки информации. На этом рисунке показаны различные каналы, через которые может происходить утечка информации. физические носители данных (USB-накопитель), компьютерные системы (взлом компьютера), коммуникационные каналы (перехват электронной почты) и социальная инженерия (обман сотрудника). Этот рисунок помогает визуализировать различные аспекты проблемы утечки информации.

Технические меры противодействия

1. *Шифрование данных*. защита информации специальными алгоритмами, чтобы предотвратить доступ неавторизованных лиц.
2. *Использование брандмауэров и антивирусного ПО*. защита компьютерных систем от внешних атак и вредоносных программ.
3. *Многофакторная аутентификация*. использование нескольких методов подтверждения личности для доступа к системам.
4. *Аудит информационной безопасности*. постоянный контроль за доступом к данным и обнаружение возможных нарушений.

Организационные меры противодействия

1. *Политики безопасности*. установление правил использования информации и ответственности за её утечку.

2. *Обучение персонала*. проведение тренингов по информационной безопасности для повышения осведомленности сотрудников.
3. *Физическая безопасность*. контроль доступа к помещениям и хранилищам с конфиденциальной информацией.
4. *Регулярное обновление систем безопасности*. поддержание программного обеспечения и аппаратных средств в актуальном состоянии.
Защита информации – это процесс, требующий комплексного подхода. Только совместное использование технических и организационных мер позволит надежно защитить конфиденциальные данные от утечки.

Контрольные вопросы.
Понятие информации и ее виды, способы получения, хранения и обработки.
1. Что представляет собой информация, и какие основные виды информации выделены в информатике?
2. Какие способы получения информации вы можете назвать? Приведите примеры каждого из них.
3. Какие методы хранения информации существуют, и в чем их особенности?
4. Какие этапы обработки информации существуют, и что включает в себя каждый из них?
5. Что такое каналы распространения информации, и как их можно классифицировать?
6. Какие основные виды каналов распространения информации существуют?
7. Приведите примеры физических, электронных и социальных каналов распространения информации.
8. Какие факторы могут влиять на эффективность каналов распространения информации?
9. Какие технические меры могут быть приняты для защиты информации от утечки?

10. Какие организационные меры могут помочь предотвратить утечку информации в организации?
11. Какие каналы утечки информации могут существовать, и какие меры могут быть предприняты для их блокирования?
12. Почему важно применять комплексный подход, включающий как технические, так и организационные меры, для защиты информации от утечки?

Тесты для закрепления темы.

1. **Что представляет собой информация?**
   а) Мусорная почта
   б) Данные без смысла
   в) То, что дает знания или понимание
   г) Все вышеперечисленное
Ответ. в) То, что дает знания или понимание
2. **Какое определение соответствует информационной системе?**
   а) Случайное собрание компьютеров
   б) Набор элементов, собирающих, обрабатывающих, хранящих и передающих информацию
   в) Локальная библиотека
   г) Интернет-браузер
Ответ. б) Набор элементов, собирающих, обрабатывающих, хранящих и передающих информацию
3. **Какую функцию выполняют социальные сети в качестве информационной системы?**
   а) Только для загрузки фотографий
   б) Только для обмена сообщениями
   в) Позволяют пользователям обмениваться информацией и контентом
   г) Используются только для онлайн-игр
Ответ. в) Позволяют пользователям обмениваться информацией и контентом
4. **Зачем банкам нужны информационные системы?**

а) Только для хранения денег

б) Для обработки транзакций и управления данными клиентов

в) Для кредитования клиентов

г) Для организации вечеринок

Ответ. б) Для обработки транзакций и управления данными клиентов

5. **Какую роль играют информационные системы в медицинской сфере?**

а) Только для заказа медицинских препаратов

б) Для управления медицинскими записями пациентов и обмена данными между врачами

в) Только для проведения медицинских исследований

г) Для приготовления кофе в клиниках

Ответ. б) Для управления медицинскими записями пациентов и обмена данными между врачами

6. **Какую функцию выполняют образовательные информационные системы?**

а) Только для оформления студенческих билетов

б) Для управления учебными планами и оценивания успеваемости

в) Для организации студенческих вечеринок

г) Только для проведения лекций

Ответ. б) Для управления учебными планами и оценивания успеваемости

7. **Как информационные системы улучшают транспортную инфраструктуру?**

а) Только для продажи билетов

б) Для отслеживания расписания и обеспечения безопасности пассажиров

в) Только для фотосессий в поездах

г) Для организации экскурсий

Ответ. б) Для отслеживания расписания и обеспечения безопасности пассажиров

8. **Какую роль играют информационные системы в бизнесе?**

а) Только для заказа канцелярских товаров

б) Для управления производственными процессами и анализа данных

в) Только для организации корпоративных вечеринок

г) Для игр в офисе

Ответ. б) Для управления производственными процессами и анализа данных

9. **Какие выгоды приносят информационные системы в обществе?**

а) Увеличение количества пробок

б) Повышение эффективности коммуникации и улучшение управления

в) Только для онлайн-шопинга

г) Только для распространения сплетен

Ответ. б) Повышение эффективности коммуникации и улучшение управления

10. **Какую роль играют информационные системы в научных исследованиях?**

а) Только для написания отчетов

б) Для сбора и анализа данных

в) Только для проведения чайных церемоний

г) Для хранения фотографий

Ответ. б) Для сбора и анализа данных

11. **Какое из следующих утверждений является свойством информации?**

а) Информация всегда достоверна и точна

б) Информация всегда бесплатна для получения

в) Информация должна быть актуальной, точной и понятной

г) Информация всегда подвержена утере при передаче

Ответ. в) Информация должна быть актуальной, точной и понятной

12. **Что такое единица измерения информации?**

а) Единица измерения скорости передачи данных по сети

б) Единица измерения времени, затрачиваемого на обработку информации

в) Единица измерения количества информации или объема данных

г) Единица измерения частоты процессора

Ответ. в) Единица измерения количества информации или объема данных

13. **Какая единица измерения используется для оценки количества информации, передаваемой по сети?**

а) Мегапиксель

б) Бит

в) Килограмм

г) Литр

Ответ. б) Бит

14. **Что означает термин "бит" в контексте информации?**

а) Единица измерения времени

б) Единица измерения объема информации

в) Единица измерения расстояния

г) Единица измерения массы

Ответ. б) Единица измерения объема информации

15. **Какой термин используется для обозначения максимальной скорости передачи информации по сети?**

а) Максимальная пропускная способность

б) Минимальная пропускная способность

в) Оптимальная пропускная способность

г) Средняя пропускная способность

Ответ. а) Максимальная пропускная способность

16. **Что такое утечка информации?**

а) Раскрытие конфиденциальных данных с разрешения владельца

б) Передача информации третьим лицам без разрешения

в) Хранение данных на безопасном сервере

г) Обмен информацией между сотрудниками компании

Ответ. б) Передача информации третьим лицам без разрешения

17. **Какие из перечисленных являются возможными каналами утечки информации?**

а) Печатные издания

б) Телевизионные передачи

в) Физические носители данных

г) Космические спутники

Ответ. в) Физические носители данных

18. **Какая из следующих мер является технической мерой противодействия утечке информации?**

а) Обучение персонала

б) Контроль доступа к помещениям

в) Шифрование данных

г) Регулярные проверки безопасности

Ответ. в) Шифрование данных

19. **Что включает в себя организационные меры противодействия утечке информации?**

а) Антивирусное программное обеспечение

б) Контроль доступа к помещениям

в) Шифрование данных

г) Обновление компьютерных систем

Ответ. б) Контроль доступа к помещениям

§1.2. Защита информации и ее виды.

Защита информации и ее категории. Технические средства контроля сетевой безопасности. Риски в отношении данных в автоматизированных информационных системах. Необходимость защиты в автоматизированных информационных системах.

Защита информации и ее категории

Защита информации — один из самых важных аспектов в современном мире цифровых технологий. Начнем с определения. что такое информация и почему она так ценна?

Информация — это данные, которые имеют смысл и являются основой для принятия решений. Это может быть что угодно. от личных данных, таких как имена и адреса, до бизнес-планов, финансовой информации и государственных секретов. Под защитой информации мы понимаем комплекс мер, направленных

на предотвращение несанкционированного доступа, использования, раскрытия, изменения или уничтожения информации.

Подробно разберемся защиты информации и ее категориях.

Представьте, что информация — это как секрет, который вы храните в сейфе. Защита информации — это то, что помогает сохранить этот секрет безопасным от посторонних глаз.

Информация бывает разной, и каждый тип информации имеет свою степень ценности и важности. Рассмотрим основные категории информации.

1. **Личная информация-** это данные о людях, такие как имена, адреса, номера телефонов, адреса электронной почты и так далее. Защита личной информации важна, чтобы люди чувствовали себя безопасно и защищенно.

2. **Корпоративная информация-** это информация, которая принадлежит компаниям или организациям. Сюда входят бизнес-секреты, финансовые отчеты, планы развития и так далее. Защита корпоративной информации важна для сохранения конкурентных преимуществ и стабильности бизнеса.

3. **Государственная информация-** это данные, относящиеся к работе государственных органов и операциям. Сюда входят законы, военные стратегии, данные разведки и так далее. Защита государственной информации важна для обеспечения национальной безопасности и сохранения суверенитета страны.

Теперь, когда мы понимаем, какие типы информации существуют и почему они важны, давайте посмотрим, как мы можем защитить эту информацию.

Как мы защищаем информацию

Защита информации — это как ставить охрану вокруг вашего дома. Вот несколько способов, которые мы используем для защиты информации.

1. **Пароли и коды доступа-** это как ключи от вашего сейфа. Пароли помогают только тем, у кого есть разрешение, получить доступ к информации.

2. **Шифрование**- это как специальный код, который делает вашу информацию непонятной для посторонних. Если кто-то попытается прочитать зашифрованную информацию без ключа, ему будет очень трудно это сделать.

3. **Безопасные сети**- это как стены вокруг вашего дома. Они могут предотвратить попытки злоумышленников войти в вашу систему и украсть информацию.

4. **Обучение персонала**- это как обучение собаки охранять ваш дом. Хорошо обученные сотрудники знают, как правильно обращаться с конфиденциальной информацией и как распознавать потенциальные угрозы.

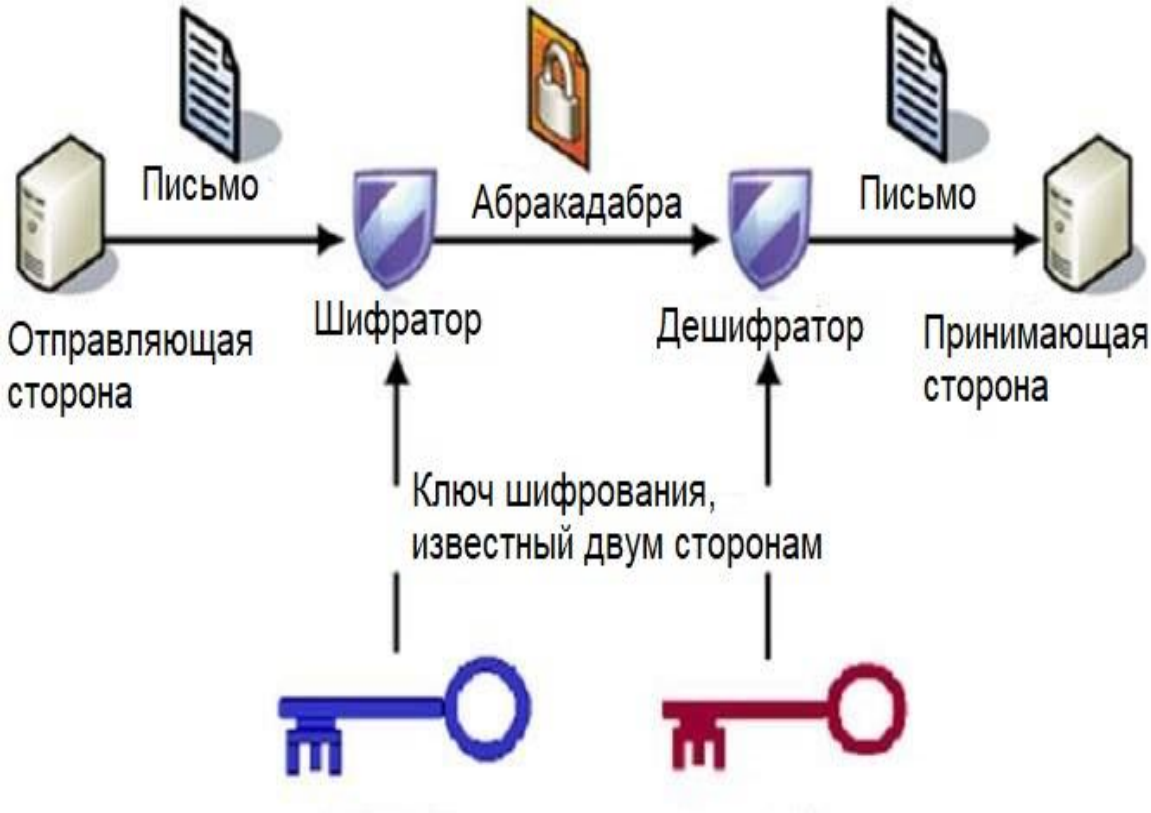

Рисунок 1.7. Защита информации

Методы и свойства защиты

Теперь, когда мы разобрались в том, как мы защищаем информацию, давайте посмотрим на то, какие риски могут возникнуть, если информация не защищена должным образом.

Риски в отношении данных

Представьте, что вы оставили свой дом без охраны. Вот что может случиться, если информация не защищена.

1. **Утеря данных**- это как потеря ключа от вашего сейфа. Если информация потеряется из-за сбоя оборудования или программного сбоя, это может привести к серьезным проблемам.

2. **Несанкционированный доступ**- это как взлом вашего сейфа. Если кто-то получит доступ к вашей информации без разрешения, это может привести к краже данных или даже к шантажу.

3. **Манипуляция данными**- это как изменение вашего дневника. Если кто-то изменит данные, это может привести к неправильным решениям и серьезным последствиям.

4. **Нарушение конфиденциальности**- это как разглашение ваших секретов. Если информация попадет в неправильные руки, это может нанести ущерб вашей репутации и привести к юридическим проблемам.

Теперь, когда мы разобрались в рисках, давайте посмотрим, почему важно защищать информацию.

Значимость защиты информации

Представьте, что информация — это как ваш семейный клад и вот почему защита информации так важна.

1. **Сохранение доверия**. Если вы не можете защитить конфиденциальность информации, люди потеряют доверие к вам и вашей организации.

2. **Соблюдение законодательства**. Многие страны имеют законы, требующие защиты информации. Несоблюдение этих законов может привести к серьезным штрафам и утрате репутации.

3. **Финансовые потери**. Утечка данных может привести к серьезным финансовым потерям из-за потери бизнеса, судебных исков и выплат компенсаций.

4. **Бизнес-процессы и эффективность**. Безопасные системы помогают обеспечить непрерывность бизнес-процессов и сохранить эффективность работы организации.

Теперь вы понимаете, как важно защищать информацию и какие шаги можно предпринять, чтобы это сделать.

Теперь, когда мы разобрались с категориями информации, давайте перейдем к техническим средствам контроля сетевой безопасности.

Технические средства контроля сетевой безопасности

Технические средства контроля сетевой безопасности поможет нам понять, какие инструменты используются для защиты компьютерных сетей от различных угроз. Давайте разберемся в этом вместе!

Что такое сетевая безопасность?

Прежде всего, давайте разберемся, что такое сетевая безопасность. Когда мы говорим о сетевой безопасности, мы имеем в виду защиту компьютерных сетей от различных угроз и атак, которые могут попытаться нарушить их работу или украсть конфиденциальные данные.

Зачем нам нужны технические средства контроля сетевой безопасности?

Технические средства контроля сетевой безопасности помогают нам обнаруживать и предотвращать угрозы в сети. Они действуют как наши "цифровые охранники", которые следят за тем, что происходит в сети, и реагируют на подозрительную активность.

Рассмотрим основные технические средства контроля сетевой безопасности.

1. *Брандмауэры (Firewalls)*. Брандмауэры - это своего рода фильтры, которые контролируют поток данных между вашим компьютером и интернетом. Они определяют, какие данные могут войти или выйти из вашей сети, основываясь на заданных правилах безопасности. Если данные не соответствуют этим правилам, брандмауэр блокирует их.

2. *Системы обнаружения вторжений (Intrusion Detection Systems, IDS).* Эти системы непрерывно мониторят сетевой трафик в поисках необычной или подозрительной активности. Если система обнаружит что-то подозрительное, она срабатывает и оповещает администратора о возможной атаке.

3. *Системы обнаружения аномалий (Anomaly Detection Systems, ADS)*. Подобно системам обнаружения вторжений, системы обнаружения аномалий анализируют сетевой трафик. Однако вместо того, чтобы искать конкретные типы атак, они ищут аномалии или необычное поведение, которое может указывать на потенциальную угрозу.

4. *Средства аутентификации*. Это инструменты, которые помогают удостоверить личность пользователя или устройства, прежде чем они получат доступ к сети. Например, это могут быть пароли, биометрическая идентификация (например, скан отпечатка пальца) или использование специальных устройств (таких как USB-ключи).

5. *Системы шифрования (Encryption)*. Шифрование - это процесс преобразования данных в зашифрованный формат, который невозможно понять без специального ключа. Это помогает защитить данные от несанкционированного доступа в случае их перехвата.

Технические средства контроля сетевой безопасности играют критическую роль в обеспечении безопасности компьютерных сетей. Они помогают нам защитить наши данные, предотвратить атаки и обеспечить непрерывную работу сети. Понимание и использование этих инструментов является ключом к эффективной защите сети.

Риски в отношении данных в автоматизированных информационных системах

Расскажем о рисках, связанных с данными в автоматизированных информационных системах. Данные играют огромную роль в нашей жизни, а автоматизированные системы помогают нам управлять этими данными. Однако, существуют определенные угрозы и риски, которые могут возникнуть. Давайте разберемся, какие это риски и как с ними бороться.

Что такое риски в отношении данных?

Представим, что данные — это как ваша ценная информация, которую вы храните на своем компьютере или телефоне. Риски в отношении данных — это все, что может угрожать безопасности или конфиденциальности этой информации. Это могут быть как технические проблемы, такие как вирусы или хакерские атаки, так и человеческие ошибки, например, случайное удаление файлов или утечка информации из-за невнимательности.

Примеры рисков в отношении данных

1. *Утеря данных*. Представьте, что вы работаете над важным проектом в своем компьютере, и внезапно происходит сбой системы или вы случайно удаляете файлы. Это может привести к потере всех ваших данных и серьезным проблемам с вашей работой или учебой.

2. *Хакерские атаки*. Как если бы кто-то пытался взломать ваш компьютер или сеть, чтобы получить доступ к вашим личным данным или конфиденциальной информации. Например, злоумышленники могут использовать вредоносные программы, чтобы украсть ваши пароли или банковские данные.

3. *Несанкционированный доступ*. Это когда кто-то получает доступ к вашей информации без вашего разрешения. Например, если вы оставите свой компьютер разблокированным и кто-то другой войдет в ваш аккаунт.

4. *Утечка конфиденциальной информации*. Это когда конфиденциальные данные попадают в неправильные руки. Например, если сотрудник компании случайно отправит электронное письмо с конфиденциальной информацией на неправильный адрес.

Как бороться с рисками в отношении данных?

Теперь, когда мы разобрались с некоторыми примерами рисков, давайте поговорим о том, как можно защитить наши данные.

1. Регулярное резервное копирование данных. Это как создание копии важных файлов на внешний жесткий диск или в

облако. Если случится что-то плохое, вы всегда сможете восстановить свои данные из резервной копии.

2. Использование антивирусного программного обеспечения. Антивирусные программы помогают защитить ваш компьютер от вредоносных программ и хакерских атак.

3. Установка обновлений программного обеспечения. Обновления программного обеспечения содержат исправления уязвимостей, которые могут использоваться злоумышленниками для атаки на ваш компьютер.

4. Обучение сотрудников о безопасности данных. Это важно, чтобы все сотрудники понимали, как правильно обращаться с конфиденциальной информацией и как распознавать потенциальные угрозы.

Теперь вы знаете, какие риски могут возникнуть в отношении данных и как их можно предотвратить. Это важно помнить, чтобы обеспечить безопасность ваших данных и личной информации.

Необходимость защиты в автоматизированных информационных системах

Ответим на вопрос- почему защита в автоматизированных информационных системах (АИС) играет ключевую роль в современном мире. Представьте, что ваша информация - это как ваше секретное досье с личными данными, которое вы храните в безопасном месте. Вот почему это так важно и зачем нам нужна защита в АИС.

1. *Соблюдение законодательства*. С момента вступления в силу **GDPR**, многие страны ужесточили требования по защите данных. Организации обязаны соблюдать эти законы, чтобы избежать серьезных штрафов и судебных разбирательств.

GDPR (General Data Protection Regulation) - это общий регламент по защите данных, который вступил в силу в Европейском союзе в мае 2018 года. Этот регламент устанавливает стандарты и правила для сбора, обработки и защиты личных данных граждан ЕС, а также устанавливает права и обязанности организаций, которые работают с этими данными.

Главная цель GDPR - обеспечить высокий уровень защиты личных данных граждан ЕС и сделать процесс сбора и использования данных более прозрачным и контролируемым.

Вот несколько ключевых моментов GDPR.

a) Согласие на обработку данных. Организации должны получать ясное и однозначное согласие от граждан ЕС на обработку их личных данных. Это означает, что организации должны четко объяснять, какие данные они собирают и как они будут использоваться.
b) Право на доступ к данным. Граждане ЕС имеют право запрашивать доступ к своим личным данным, а также получать информацию о том, как эти данные используются.
c) Право на исправление и удаление данных. Граждане ЕС имеют право требовать исправления или удаления своих личных данных, если они являются неточными или устаревшими, или если нет законных оснований для их обработки.
d) Обязательное уведомление о нарушении данных. Организации обязаны уведомлять контролирующий орган и затронутых граждан о нарушении безопасности данных в течение 72 часов после его обнаружения.
e) Штрафы за нарушение. GDPR предусматривает высокие штрафы за нарушение его положений - до 20 миллионов евро или 4% глобального оборота организации, в зависимости от того, что больше.

Главная идея GDPR - защита личной приватности и данных граждан ЕС, а также повышение ответственности и прозрачности в области обработки данных.

2. *Доверие пользователей*. Время от времени мы слышим о крупных утечках данных, и это оставляет негативное впечатление у пользователей. Если они не уверены в безопасности своих данных, они могут потерять доверие к организации и перестать пользоваться ее услугами.

3. *Финансовые потери*. Кибератаки могут привести к серьезным финансовым потерям. От восстановления систем и

компенсации клиентам до потери бизнеса и репутации - последствия могут быть катастрофическими.

4. *Бизнес-процессы и эффективность*. Автоматизированные информационные системы играют жизненно важную роль в современном бизнесе. Если они подвергаются атакам или утечкам данных, это может привести к прерыванию бизнес-процессов и потере эффективности, что в конечном итоге наносит ущерб репутации и прибыли организации.

Таким образом, защита информации в автоматизированных информационных системах не просто роскошь, а необходимость. Это обеспечивает законопослушность, сохраняет доверие пользователей, предотвращает финансовые потери и поддерживает бизнес-процессы на высоком уровне эффективности.

Контрольные вопросы.

1. Какие категории информации могут существовать в контексте защиты данных?
2. В чем заключается конфиденциальная информация и почему ее защита важна для организаций?
3. Что такое персональные данные и какие меры могут приниматься для их защиты?
4. Какие еще категории информации могут быть важны для защиты в различных сферах деятельности?
5. Какие технические средства могут использоваться для контроля сетевой безопасности?
6. Что такое брандмауэр и какие функции он выполняет в защите сети?
7. Какие инструменты мониторинга сети используются для выявления аномалий и инцидентов безопасности?
8. Какие меры безопасности могут быть реализованы на уровне сетевого оборудования, такого как маршрутизаторы и коммутаторы?
9. Какие риски могут возникать в отношении данных в автоматизированных информационных системах?

10. Что такое утечка данных и каковы ее последствия для организации?

11. Какие могут быть технические угрозы для данных в автоматизированных информационных системах?

12. Какие меры могут быть приняты для предотвращения рисков, связанных с данными, в информационных системах?

13. Почему защита данных в автоматизированных информационных системах является важной задачей для организаций?

14. Какие могут быть последствия для организации в случае утечки или компрометации данных?

15. Какие законодательные требования могут существовать относительно защиты данных в различных странах?

16. Какие принципы и методы могут быть применены для обеспечения безопасности и защиты данных в автоматизированных информационных системах?

Тесты для закрепления темы.

1. **Какие категории информации существуют по степени их конфиденциальности?**

a) Публичная, частично конфиденциальная, конфиденциальная, секретная

b) Обычная, личная, коммерческая, государственная

c) Низкий, средний, высокий, экстремальный

d) Внутренняя, внешняя, коммерческая, общественная

Ответ. a) Публичная, частично конфиденциальная, конфиденциальная, секретная

2. **Что означает термин "Утечка данных"?**

a) Нарушение системы безопасности

b) Неожиданное потеря информации

c) Зашифрованные данные

d) Хранение данных в облаке

Ответ. b) Неожиданное потеря информации

3**. Какое техническое средство используется для контроля потока данных между компьютером и интернетом?**

a) Антивирусное программное обеспечение

b) Системы обнаружения вторжений (IDS)

c) Брандмауэр (Firewall)

d) Шифрование данных

Ответ. c) Брандмауэр (Firewall)

4. **Что делают системы обнаружения аномалий (ADS)?**

a) Мониторят сетевой трафик в поисках необычной активности

b) Блокируют вредоносные программы на компьютере

c) Шифруют данные для безопасной передачи

d) Проверяют уровень шифрования паролей

Ответ. a) Мониторят сетевой трафик в поисках необычной активности

5**. Что может привести к серьезным финансовым потерям из-за потери бизнеса и судебных исков?**

a) Утечка данных

b) Вирус на компьютере

c) Необходимость обновления программного обеспечения

d) Создание резервной копии данных

Ответ. a) Утечка данных

6. **Что такое хакерская атака?**

a) Вирус, который блокирует доступ к компьютеру

b) Попытка получить несанкционированный доступ к системе

c) Автоматизированное обновление программного обеспечения

d) Программа для создания резервной копии данных

Ответ. b) Попытка получить несанкционированный доступ к системе

7. **Зачем нужна защита в автоматизированных информационных системах согласно GDPR?**

a) Для защиты от вредоносных программ

b) Для соблюдения законодательства о защите данных

c) Для улучшения производительности системы

d) Для увеличения количества данных

Ответ. b) Для соблюдения законодательства о защите данных

8. **Что может быть последствием нарушения безопасности данных в автоматизированных информационных системах?**

a) Потеря конфиденциальной информации и финансовые потери

b) Увеличение эффективности работы

c) Увеличение доверия пользователей к системе

d) Уменьшение количества атак на систему

Ответ. a) Потеря конфиденциальной информации и финансовые потери

9. **Какие меры безопасности могут использоваться для защиты конфиденциальной информации?**

a) Регулярные резервные копии

b) Общий доступ к данным

c) Шифрование данных

d) Использование общественных сетей Wi-Fi

Ответ. c) Шифрование данных

10. **Что подразумевается под категорией "публичная информация"?**

a) Информация, доступная только внутри компании

b) Информация, доступная всем без ограничений

c) Информация, доступная только после аутентификации

d) Информация, доступная только для конкретной группы пользователей

Ответ. b) Информация, доступная всем без ограничений

11. **Какое техническое средство используется для аутентификации пользователей перед доступом к сети?**

a) Антивирусное программное обеспечение

b) Системы обнаружения вторжений (IDS)

c) Средства шифрования

d) Системы аутентификации

Ответ. d) Системы аутентификации

12. **Какую функцию выполняют системы обнаружения вторжений (IDS)?**

a) Шифруют данные перед передачей по сети

b) Блокируют доступ к вредоносным веб-сайтам

c) Анализируют сетевой трафик на предмет подозрительной активности

d) Отслеживают и удаляют вирусы с компьютеров

Ответ. c) Анализируют сетевой трафик на предмет подозрительной активности

13. **Какие последствия могут возникнуть в результате утечки конфиденциальной информации?**

a) Увеличение доверия пользователей к системе

b) Финансовые потери и утрата репутации

c) Улучшение производительности системы

d) Уменьшение количества атак на систему

Ответ. b) Финансовые потери и утрата репутации

14. **Что означает термин "необходимость защиты в автоматизированных информационных системах"?**

a) Защита данных не требуется

b) Защита данных обязательна для соблюдения законодательства и предотвращения угроз безопасности

c) Защита данных полностью находится в компетенции пользователей

d) Защита данных не может быть обеспечена

Ответ. b) Защита данных обязательна для соблюдения законодательства и предотвращения угроз безопасности

15. **Какие из перечисленных мер являются методами защиты информации от несанкционированного доступа?**

a) Регулярное резервное копирование данных

b) Проведение обучения сотрудников по правилам безопасности

c) Шифрование данных

d) Использование общедоступных облаков для хранения информации

Ответ. b) Проведение обучения сотрудников по правилам безопасности

16. **Какие данные могут быть отнесены к категории "конфиденциальная"?**

a) Имя пользователя в социальной сети

b) Адрес электронной почты

c) Медицинская история пациента

d) Название любимого фильма

Ответ. c) Медицинская история пациента

17. **Какой тип атаки могут предотвратить системы обнаружения вторжений (IDS)?**

a) Атаки типа DDoS (распределенное отказоустойчивое атака)

b) Вирусы, распространяемые через вредоносные веб-сайты

c) Попытки несанкционированного доступа к сети

d) Шпионские программы, отправляющие конфиденциальную информацию на удаленный сервер

Ответ. c) Попытки несанкционированного доступа к сети

18. **Какое устройство используется для мониторинга и анализа сетевого трафика?**

a) Маршрутизатор

b) Коммутатор

c) Система обнаружения вторжений (IDS)

d) Сетевой адаптер

Ответ. c) Система обнаружения вторжений (IDS)

19. **Какие из ниже перечисленных событий являются потенциальными рисками для автоматизированных информационных систем?**

a) Резервное копирование данных

b) Утечка конфиденциальной информации

c) Обновление программного обеспечения

d) Проведение обучения сотрудников по правилам безопасности

Ответ. b) Утечка конфиденциальной информации

20. **Что может привести к финансовым потерям и утрате доверия со стороны клиентов?**

a) Обучение сотрудников по правилам безопасности

b) Утечка конфиденциальной информации

c) Регулярное обновление программного обеспечения

d) Создание резервной копии данных

Ответ. b) Утечка конфиденциальной информации

§1.3. Основные понятия информационной безопасности.

Необходимость обеспечения информационной безопасности. Основы существующих рисков в отношении информации. Риски в отношении информации в информационных системах. Основные понятия информационной безопасности и ее классификация.

Необходимость обеспечения информационной безопасности.

Что на сегодняшний день становится все более актуальным в нашем цифровом мире – об информационной безопасности. Давайте начнем с простого вопроса. Почему нам важно заботиться об этом?

Представьте, что информация – это ценный ресурс, такой же важный, как деньги или время. Она может быть личной (как ваше имя или адрес) или деловой (как финансовые отчеты или планы компании). Теперь представьте, что кто-то, кто не имеет права на эту информацию, получает к ней доступ. Это может привести к серьезным последствиям.

1. *Утрата конфиденциальности*. Ваша личная информация или конфиденциальные данные вашей компании могут быть скомпрометированы, что может привести к утечке личной

информации, краже идентификационных данных или даже к финансовым потерям.

2. *Нарушение целостности данных*. Если информация изменяется или портится злоумышленниками, это может привести к ошибкам в принятии решений или даже к потере данных.

3. *Угроза доступности данных*. Атаки, такие как отказ в обслуживании (DDoS), могут привести к недоступности важных ресурсов или услуг, что может нанести ущерб вашему бизнесу или личной жизни.

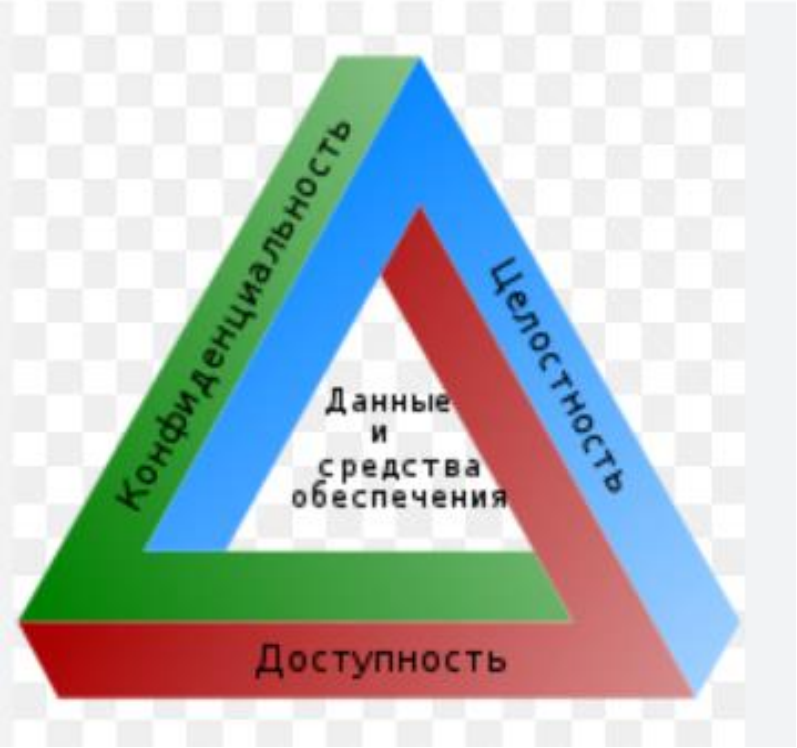

Рисунок 1.8. Обеспечение безопасности

Информационная безопасность

Теперь вы, вероятно, спросите. "Что мы можем сделать, чтобы защитить себя и наши данные?"

Вот несколько простых шагов.

1. *Создайте сильные пароли и используйте двухфакторную аутентификацию*. Пароли должны быть длинными, содержать комбинацию букв, цифр и специальных символов. Двухфакторная аутентификация добавляет еще один слой защиты, требуя не только пароль, но и другой элемент, такой как одноразовый код.

2. *Обновляйте программное обеспечение*. Регулярные обновления программного обеспечения помогают исправлять уязвимости, которые могут быть использованы злоумышленниками для взлома вашей системы.

3. *Будьте осторожны в интернете*. Не открывайте подозрительные ссылки или вложения в электронных письмах, не делитесь личной информацией на ненадежных сайтах, используйте антивирусное программное обеспечение.

4. *Обучение и осведомленность*. Понимание основных принципов информационной безопасности и умение распознавать потенциальные угрозы помогут вам защитить себя и ваши данные.

Пример . Представьте, что вы владеете крупной компанией, которая хранит чувствительные данные своих клиентов, такие как персональная информация, банковские реквизиты и коммерческая информация. Недавно вы услышали о волне кибератак, целью которых стали компании в вашей отрасли. Несанкционированный доступ к вашим системам мог бы привести к серьезным последствиям, включая утечку конфиденциальной информации, финансовые потери, ущерб репутации и даже правовые проблемы.

Чтобы защитить себя от этих угроз, вам необходимо обеспечить высокий уровень информационной безопасности. Это может включать в себя регулярное обновление программного обеспечения, установку многоуровневых систем защиты, шифрование данных, обучение сотрудников правилам безопасности информации и многое другое. Без таких мер предосторожности ваша компания может стать уязвимой для атак и попасть в серьезные проблемы.

Информационная безопасность играет ключевую роль в нашей цифровой жизни. Защита наших данных – это ответственность каждого из нас, и следуя простым шагам безопасности, мы можем сделать наш цифровой мир более безопасным для всех.

Основы существующих рисков в отношении информации.

Поговорим о рисках, связанных с информацией, которые существуют в нашем мире. Это важно, потому что понимание этих рисков поможет нам лучше защитить наши данные и сохранить безопасность в цифровой среде.

Итак, давайте начнем с того, что такое риск в отношении информации? Это возможность того, что наша информация может быть украдена, повреждена или использована неправильно. Как и в реальной жизни, у нас есть определенные угрозы, которые мы должны учитывать.

1. *Кибератаки*. Это когда злоумышленники пытаются взломать наши системы или сети, чтобы получить доступ к нашей информации. Они могут использовать вредоносные программы, фишинговые атаки или другие методы, чтобы проникнуть в наши компьютеры или сети.

2. *Утечка данных*. Это случается, когда наша личная или деловая информация попадает в руки злоумышленников из-за неправильной защиты или утечки данных от организаций, с которыми мы имеем дело.

3. *Нарушение конфиденциальности*. Это когда наша личная информация становится доступной для посторонних лиц без нашего разрешения. Например, если наши личные сообщения или данные банковского счета попадают в общий доступ из-за небезопасных настроек конфиденциальности.

4. *Потеря данных*. Это может произойти из-за сбоя в системе, атаки злоумышленников или ошибки человека. Важные файлы могут быть повреждены или уничтожены, что приведет к потере важной информации.

Теперь, когда мы знаем о некоторых основных рисках, связанных с информацией, что мы можем сделать, чтобы защитить себя?

1. *Обновляйте программное обеспечение и используйте антивирусное ПО*. Это поможет предотвратить атаки и защитить ваши устройства от вредоносных программ.

2. *Создавайте крепкие пароли и не делитесь ими*. Это поможет предотвратить взлом вашей учетной записи или сети.
3. *Будьте осторожны в интернете*. Не открывайте подозрительные ссылки или вложения, не делитесь личной информацией на ненадежных сайтах.
4. *Регулярно делайте резервные копии данных*. Это поможет восстановить информацию в случае потери или повреждения файлов.

Таким образом, понимание основных рисков в отношении информации поможет нам принимать меры предосторожности и обеспечивать безопасность нашей цифровой жизни.

Риски в отношении информации в информационных системах

Это важно, потому что информационные системы играют огромную роль в нашей повседневной жизни, и нам важно понимать, как защитить нашу информацию в этом цифровом мире.

Начнем с определения. что такое информационные системы? Это просто компьютерные системы, которые собирают, обрабатывают и хранят информацию. Выясним и поговорим о рисках, которые могут возникнуть в этих системах.

1. *Уязвимости программного обеспечения*. Когда программное обеспечение не обновляется или содержит ошибки, оно становится уязвимым для атак. Злоумышленники могут использовать эти уязвимости, чтобы получить доступ к вашей информации.
2. *Неавторизованный доступ*. Если не установлены правильные меры безопасности, злоумышленники могут получить доступ к информации, к которой у них нет права доступа. Это может привести к утечке данных или нанести ущерб вашей компании.
3. *Потеря данных*. Если не сделаны резервные копии данных или не установлена надежная система хранения данных, то информация может быть утрачена из-за сбоев в системе или атак злоумышленников.
4. *Социальная инженерия*. Это когда злоумышленники используют манипуляцию и обман, чтобы убедить людей раскрыть свои личные

данные или предоставить доступ к системам. Например, они могут представляться сотрудниками компании и попросить ваш пароль.

Теперь, когда мы знаем о рисках, что мы можем сделать, чтобы защитить себя и наши информационные системы?

1. *Регулярно обновляйте программное обеспечение*. Это поможет исправить уязвимости и защитить систему от атак.
2. *Используйте сильные пароли и двухфакторную аутентификацию*. Это поможет предотвратить несанкционированный доступ к вашим учетным записям.
3. *Обучайте сотрудников*. Обучение персонала по безопасности информации поможет им распознавать угрозы и предотвращать атаки.
4. *Регулярно делайте резервные копии данных*. Это поможет восстановить информацию в случае ее потери или повреждения.

Понимание рисков в отношении информации в информационных системах поможет нам принимать меры предосторожности и обеспечивать безопасность наших данных.

Основы информационной безопасности и ее классификация

Что помогает нам защитить нашу личную информацию, данные компаний и государств от различных угроз в цифровом мире? Начнем с основных понятий информационной безопасности.

1. ***Конфиденциальность.*** Это защита информации от несанкционированного доступа. Например, когда вы делитесь своим паролем только с теми, кому вы доверяете, вы обеспечиваете конфиденциальность вашей информации.

Пример. Представьте, что у вас есть учетная запись в онлайн-банке, содержащая чувствительную финансовую информацию. Для обеспечения конфиденциальности этой информации вы используете пароль. Вы делитесь этим паролем только с теми, кому доверяете, например, вашим супругом или финансовым консультантом. Как результат, только эти люди имеют доступ к вашему банковскому аккаунту.

Этот пример иллюстрирует, как конфиденциальность обеспечивается путем ограничения доступа к конкретным

данным только для авторизованных пользователей. Пароль служит механизмом защиты, который гарантирует, что только те, у кого есть правильные учетные данные, могут получить доступ к конфиденциальной информации. Таким образом, даже если кто-то пытается получить доступ к вашему банковскому аккаунту без вашего разрешения, их попытки будут неудачными из-за отсутствия правильного пароля.

2. ***Целостность***. Это гарантия того, что информация не будет изменена или повреждена без вашего согласия. Например, если вы отправляете документ по электронной почте, вы хотите быть уверены, что он не будет изменен по пути.

Пример. Предположим, что вы отправляете важный документ по электронной почте своему коллеге. Этот документ содержит важные финансовые данные или стратегические планы вашей компании. Прежде чем отправить документ, вы применяете к нему электронную подпись, которая гарантирует его целостность.

После того как документ отправлен, в процессе его передачи через интернет возможны различные угрозы, такие как вредоносные программы или попытки взлома. Но благодаря электронной подписи и механизмам шифрования, которые гарантируют его целостность, ваш коллега может быть уверен, что документ, который он получил, идентичен тому, который был отправлен вами.

Этот пример показывает, что целостность обеспечивает защиту от несанкционированных изменений или повреждений данных в процессе их передачи или хранения. Благодаря этой мере безопасности получатель может быть уверен, что информация, которую он получает, остается неповрежденной и неизменной.

3. ***Доступность***. Это обеспечение доступа к информации в нужное время и место. Например, если вы хотите получить доступ к своим фотографиям на облачном хранилище, вы ожидаете, что они будут доступны в любое время.

Пример. Предположим, что вы используете облачное хранилище для хранения своих фотографий, документов и других файлов. Важным аспектом для вас является доступность этих файлов в любое время и из любого места.

Например, вы сейчас на отдыхе за границей и вам внезапно потребовалась фотография вашего паспорта для заполнения какой-то формы. Благодаря облачному хранилищу и доступности, которую оно предоставляет, вы можете легко получить доступ к своим файлам через интернет, даже находясь в отдаленном месте, и найти нужный вам документ в нужный момент.

Этот пример показывает, что доступность информации означает не только ее хранение в безопасном месте, но и гарантирует возможность мгновенного доступа к ней в любой момент времени и из любого места с помощью интернета. Таким образом, вы можете быть уверены, что ваша информация доступна, когда это необходимо, что существенно облегчает вашу повседневную жизнь и работу.

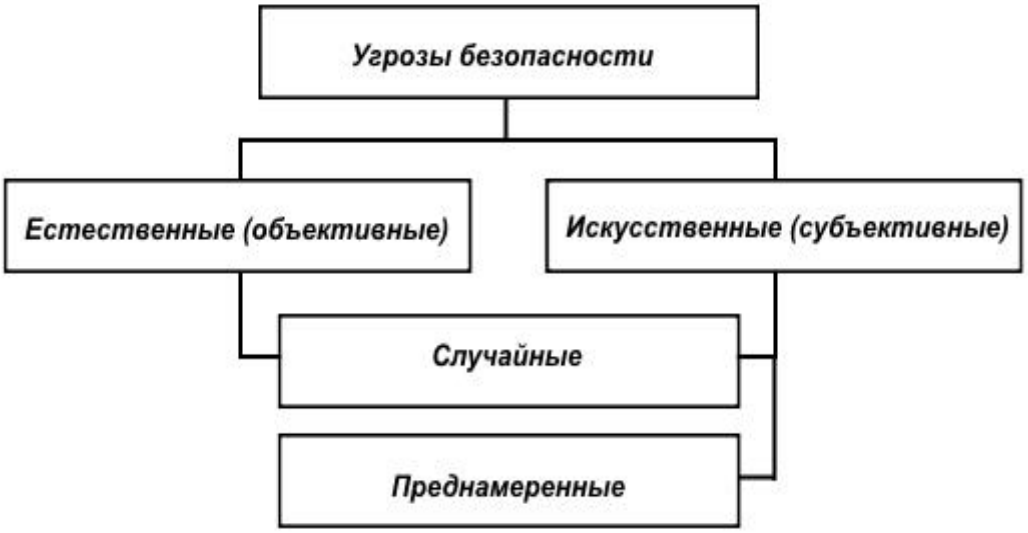

Рисунок 1.9. Угрозы безопасности

Теперь давайте поговорим о **классификации информационной безопасности**. Она делится на три категории.

1. **Техническая безопасность**. Это использование технических средств для защиты информации. Например, установка

антивирусного программного обеспечения или настройка брандмауэров на компьютере.

Техническая безопасность подразумевает использование различных технологий и программ для защиты вашей информации от вредоносных атак и нежелательного доступа. Давайте представим, что ваш компьютер - это ваш дом, а ваши файлы и данные - ценные вещи внутри. Чтобы защитить свой дом и все, что в нем, вы устанавливаете замки на двери и окна. В мире компьютеров это аналогично установке антивирусного программного обеспечения и настройке брандмауэра.

Антивирусная программа работает, как ваш охранник, сканируя все входящие и исходящие файлы на компьютере, чтобы обнаружить и уничтожить вредоносные программы, которые могут попытаться ворваться и навредить вашей системе. Брандмауэр, с другой стороны, действует как невидимый забор вокруг вашего дома, контролируя, какие программы и службы могут получать доступ к вашему компьютеру из интернета и блокируя любые потенциально опасные соединения.

Вместе эти технические меры безопасности обеспечивают защиту вашего компьютера и данных, помогая вам чувствовать себя уверенно в онлайне и предотвращая потенциальные угрозы из интернета.

2. **Организационная безопасность**. Это разработка и реализация политик, процедур и обучения для защиты информации. Например, обучение сотрудников по безопасности информации или установка правил доступа к конфиденциальной информации в компании.

Организационная безопасность - это как создание и внедрение правил и процедур в компании, чтобы защитить ее информацию. Давайте представим, что ваша компания - это замок, а ваша информация - это сокровища внутри него. Организационная безопасность, это как создание хорошо продуманных правил и процедур, чтобы обеспечить безопасность замка и защитить сокровища внутри.

Например, ваша компания может проводить обучение сотрудников по правилам безопасности информации. Это как если бы вы учили охранников замка, как определять потенциальных злоумышленников и как действовать в случае опасности. Обучение помогает сотрудникам понять, как защищать важные данные компании и как реагировать на возможные угрозы.

Также, компания может установить правила доступа к конфиденциальной информации. Например, только определенные люди с правильными ключами могут получить доступ к важным комнатам в замке. Точно так же, в вашей компании могут быть установлены правила, кто и как может получить доступ к конфиденциальным данным, чтобы обеспечить их безопасность.

Все эти меры вместе создают организационную безопасность, которая помогает защитить информацию компании от угроз и обеспечить безопасность ее операций.

3. **Физическая безопасность**. Это защита физических ресурсов, таких как серверные комнаты или бумажные документы. Например, установка систем контроля доступа или использование сейфов для хранения важных документов.

Конечно, вот пример, который объясняет физическую безопасность простыми словами.

Физическая безопасность - это забота о защите всего, что можно потрогать, включая помещения и материальные вещи. Давайте представим, что ваш дом - это ваша компания, а ваши серверные комнаты или бумажные документы - это самые ценные вещи внутри. Так же, как вы заботитесь о том, чтобы ваш дом был защищен от незваных гостей, вы также заботитесь о защите ваших серверов и документов от неприглашенных посетителей и потенциальных угроз.

Например, вы можете установить системы контроля доступа к вашим серверным комнатам, чтобы только авторизованные сотрудники имели доступ к важной информации. Это подобно использованию ключа, чтобы заблокировать и разблокировать дверь вашего дома. Или вы можете хранить важные бумажные

документы в сейфах, чтобы обеспечить дополнительный уровень защиты от кражи или повреждения.

Такие меры обеспечивают безопасность физических ресурсов вашей компании, помогая предотвратить доступ к ним для неправомочных лиц и защищая их от различных рисков. Понимание основ информационной безопасности и ее классификации поможет нам лучше защитить наши данные и информацию в цифровом мире.

Контрольные вопросы.

1. Почему обеспечение информационной безопасности является важным аспектом для организаций и частных лиц?
2. Какие могут быть последствия нарушения информационной безопасности для организаций и частных лиц?
3. Какие факторы способствуют росту важности информационной безопасности в современном мире?
4. Какие основные принципы лежат в основе обеспечения информационной безопасности?
5. Какие типы угроз могут быть направлены на информацию?
6. Какие могут быть источники угроз для информации в современном мире?
7. Какие факторы могут увеличить уязвимость информации перед различными угрозами?
8. Какие последствия могут возникнуть в случае реализации угроз для информации?
9. Что представляют собой риски в информационных системах?
10. Какие типы угроз могут возникать для информации в информационных системах?
11. Какие факторы могут повлиять на безопасность информационных систем?
12. Каким образом управление рисками в информационных системах помогает обеспечить их безопасность?
13. Что включает в себя понятие информационной безопасности?

14. Какие основные составляющие информационной безопасности вы знаете?
15. Какие классификации информационной безопасности существуют?
16. Какие меры могут быть предприняты для обеспечения каждого из аспектов информационной безопасности?

Тесты для закрепления темы.

1. **Что означает конфиденциальность информации?**
   - а) Защита от вирусов
   - б) Защита от несанкционированного доступа
   - в) Защита от повреждения данных
   - г) Защита от перехвата сетевого трафика

Ответ. б) Защита от несанкционированного доступа

2**. Что означает целостность данных?**
   - а) Защита от потери информации
   - б) Защита от изменения информации без разрешения
   - в) Защита от вредоносных программ
   - г) Защита от несанкционированного доступа

Ответ. б) Защита от изменения информации без разрешения

3. **Что означает доступность информации?**
   - а) Возможность получения информации в нужное время и место
   - б) Защита информации от утери
   - в) Защита от изменения информации
   - г) Защита от несанкционированного доступа

Ответ. а) Возможность получения информации в нужное время и место

4. **Какая из перечисленных относится к технической безопасности?**
   - а) Обучение персонала по безопасности информации
   - б) Установка антивирусного программного обеспечения
   - в) Установка политик доступа к информации

- г) Разработка процедур реагирования на инциденты безопасности

Ответ. б) Установка антивирусного программного обеспечения

5. **Какая из перечисленных относится к организационной безопасности?**

- а) Установка биометрических замков на дверях серверной комнаты
- б) Разработка политики доступа к конфиденциальной информации
- в) Регулярное обновление программного обеспечения
- г) Установка огневых стен для защиты сети

Ответ. б) Разработка политики доступа к конфиденциальной информации

6. **Какая из перечисленных относится к физической безопасности?**

- а) Установка брандмауэров на серверах
- б) Обучение сотрудников по безопасности информации
- в) Установка систем контроля доступа к серверной комнате
- г) Использование криптографических методов шифрования данных

Ответ. в) Установка систем контроля доступа к серверной комнате

7. **Что такое информационная безопасность?**

- а) Защита информации от изменения
- б) Защита информации от доступа только для определенных лиц
- в) Защита информации от потери
- г) Защита информации от всех угроз

Ответ. б) Защита информации от доступа только для определенных лиц

8. **Как можно обеспечить безопасность пароля?**

- а) Использовать короткие пароли
- б) Использовать пароли, состоящие из личной информации
- в) Использовать длинные и сложные пароли
- г) Использовать один и тот же пароль для всех аккаунтов

Ответ. в) Использовать длинные и сложные пароли

9. **Что такое фишинг?**

- а) Вид рыбалки
- б) Атака, при которой злоумышленник выдает себя за доверенное лицо для получения личной информации
- в) Способ обучения плаванию
- г) Программа для обнаружения вирусов

Ответ. б) Атака, при которой злоумышленник выдает себя за доверенное лицо для получения личной информации

10. **Какие из перечисленных относятся к технической безопасности?**

- а) Физическая защита серверной комнаты
- б) Установка антивирусного программного обеспечения
- в) Разработка политики доступа к конфиденциальной информации
- г) Обучение сотрудников по безопасности информации

Ответ. б) Установка антивирусного программного обеспечения

11**. Какие из перечисленных относятся к организационной безопасности?**

- а) Регулярное обновление программного обеспечения
- б) Установка систем контроля доступа к серверной комнате
- в) Обучение сотрудников по безопасности информации
- г) Установка брандмауэров на серверах

Ответ. в) Обучение сотрудников по безопасности информации

12. **Какие из перечисленных относятся к физической безопасности?**

- а) Установка брандмауэров на серверах
- б) Разработка политики доступа к конфиденциальной информации
- в) Установка систем контроля доступа к серверной комнате
- г) Установка антивирусного программного обеспечения

Ответ. в) Установка систем контроля доступа к серверной комнате

13. **Что такое двухфакторная аутентификация?**

- а) Подтверждение личности с помощью двух документов

- б) Способ защиты, требующий два разных метода аутентификации, например, пароля и одноразового кода
- в) Способ кодирования информации для защиты от несанкционированного доступа
- г) Метод обучения сотрудников по безопасности информации

Ответ. б) Способ защиты, требующий два разных метода аутентификации, например, пароля и одноразового кода

14. **Что такое антивирусное программное обеспечение?**
- а) Программа для удаления нежелательной почты
- б) Программа для создания резервных копий данных
- в) Программа для обнаружения и удаления вредоносных программ с компьютера
- г) Программа для шифрования информации

Ответ. в) Программа для обнаружения и удаления вредоносных программ с компьютера

15. **Что такое шифрование данных?**
- а) Процесс удаления данных с жесткого диска
- б) Процесс обучения алгоритмов на основе данных
- в) Процесс преобразования информации в нечитаемый формат с целью защиты от несанкционированного доступа
- г) Процесс резервного копирования данных на внешний носитель

Ответ. в) Процесс преобразования информации в нечитаемый формат с целью защиты от несанкционированного доступа

16**. Какие из перечисленных относятся к технической безопасности?**
- а) Обучение сотрудников по безопасности информации
- б) Установка антивирусного программного обеспечения
- в) Разработка политики доступа к конфиденциальной информации
- г) Установка систем контроля доступа к серверной комнате

Ответ. б) Установка антивирусного программного обеспечения

17. **Какие из перечисленных относятся к организационной безопасности?**

- а) Разработка процедур реагирования на инциденты безопасности
- б) Установка систем контроля доступа к серверной комнате
- в) Обучение сотрудников по безопасности информации
- г) Установка брандмауэров на серверах

Ответ. в) Обучение сотрудников по безопасности информации

18**. Какие из перечисленных относятся к физической безопасности?**

- а) Установка брандмауэров на серверах
- б) Разработка политики доступа к конфиденциальной информации
- в) Установка систем контроля доступа к серверной комнате
- г**)** Установка антивирусного программного обеспечения

Ответ. в) Установка систем контроля доступа к серверной комнате

19. **Что представляет собой аутентификация?**

а) Процесс шифрования данных

б) Процесс проверки подлинности пользователя или системы

в) Метод анонимизации данных

г) Техника резервного копирования информации

Ответ. б) Процесс проверки подлинности пользователя или системы

20. **Что такое угроза информационной безопасности?**

а) Возможность потери данных

б) Действие или событие, которое может нанести ущерб информации или информационной системе

в) Шифрование данных

г) Политика доступа к информации

Ответ. б) Действие или событие, которое может нанести ущерб информации или информационной системе

2-ГЛАВА. Методы защиты информации

§2.4. Основы защиты информации.

Стенографическая (stegano) защита информации. Методы стенографической защиты информации. Современная компьютерная стенография, перспективы и ее основные задачи. Компьютерная стенография маскировка программного обеспечения. Защита авторских прав. Информация о стенографических программах.

Стенографическая (stegano) защита информации.

Поговорим о стенографической защите информации. Это интересная тема, которая касается способов скрытия секретной информации в других данных таким образом, чтобы это было невидимо для посторонних.

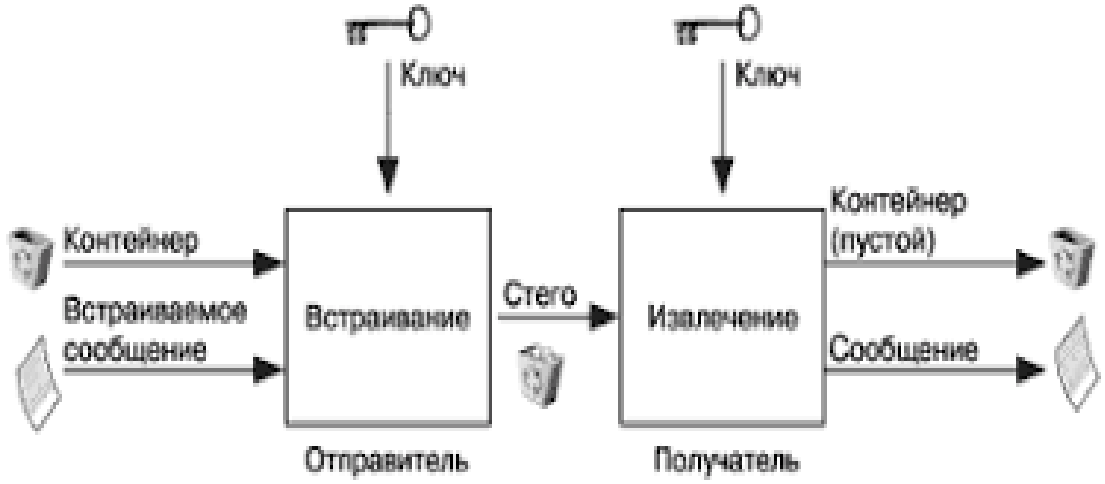

Рисунок 2.1. Стенографическая защита информации

Основные положения стенографии

Возможно, вы слышали о стенографии в контексте изображений. Да, это то же самое слово, что и "стенография" в письменном контексте, но в этом случае оно имеет немного другой смысл. В стенографии изображений мы можем скрывать информацию внутри обычных изображений таким образом, чтобы это не было заметно человеческому глазу. Например, мы можем изменить некоторые пиксели в изображении так, чтобы они несла некую секретную информацию, и в то же время, кажется, что изображение осталось без изменений.

Для этого используются различные методы, один из самых распространенных - LSB (Least Significant Bit) метод. Этот метод заключается в том, что мы изменяем наименее значимый бит каждого цветового канала пикселя изображения таким образом, чтобы он содержал информацию, которую мы хотим скрыть. Поскольку изменения крайне малы, они обычно не видны невооруженным глазом.

Но стеганография не ограничивается только изображениями. Ее также можно применять к другим форматам данных, таким как звуковые файлы, видео и даже текстовые документы. Основная идея остается такой же. скрыть информацию внутри других данных таким образом, чтобы это было незаметно.

Стеганография

Однако, как и любая другая технология, стеганография может быть использована и в злых целях. Например, злоумышленники могут использовать стеганографию для скрытой передачи вредоносного кода или конфиденциальной информации через видео или звуковые файлы.

Рисунок 3.2. Стеганография

Поэтому важно понимать, как защититься от таких атак и как обнаружить скрытую информацию.

Методы стеганографической защиты информации.

Существует множество методов обнаружения стеганографии, но некоторые из них могут быть довольно сложными. Например,

это может включать в себя анализ статистических свойств изображения или звукового файла, чтобы обнаружить изменения, которые могли быть внесены стеганографическими методами.

Вот несколько основных методов стеганографической защиты информации.

1. **LSB (Least Significant Bit).** Этот метод заключается в замене наименее значимых битов данных (обычно в изображениях, звуковых файлах или видео) на биты секретной информации. Поскольку изменения минимальны, они обычно незаметны для человеческого восприятия.

2**. Изменение формата файла.** Этот метод заключается в изменении формата файла, чтобы внедрить секретную информацию. Например, скрытый текст может быть записан в комментарии файла, что может быть неочевидно для обычного просмотра.

3. **Изменение метаданных**. Этот метод включает в себя изменение метаданных файла (например, даты создания, авторства и т. д.) для скрытия информации.

4. **Изменение шрифтов и форматирования текста**. В текстовых документах можно изменять шрифты, размеры или форматирование символов, чтобы скрыть информацию. Например, можно использовать специальные символы или комбинации символов, чтобы передать секретное сообщение.

5. **Использование шума**. В звуковых файлах можно добавить шум или искажения, которые содержат скрытую информацию. Это может быть сделано, например, путем изменения частот или амплитуды звуковых волн.

6. **Использование скрытых каналов**. Этот метод включает использование неожиданных каналов для передачи информации, например, использование малоиспользуемых или неиспользуемых битов в сетевом трафике или протоколах.

Эти методы представляют лишь небольшую часть разнообразных способов стеганографической защиты информации,

и каждый из них может быть настроен и модифицирован в зависимости от конкретных требований и ситуаций.

В целом, стенографическая защита информации - это интересная и важная область в области кибербезопасности, которая требует как технических знаний, так и понимания возможных угроз и способов защиты от них.

Рассмотрим пример стенографической защиты информации с использованием изображений.

Представьте, что у вас есть обычное изображение пейзажа с озером, лесом и небом. Это изображение может быть представлено в виде матрицы пикселей, где каждый пиксель представляет собой комбинацию красного, зеленого и синего цветовых каналов.

Теперь предположим, что вы хотите передать некоторое секретное сообщение вашему другу через это изображение, но вы не хотите, чтобы кто-то другой узнал о нем. Вы можете использовать стеганографию для скрытия этого сообщения в изображении таким образом, чтобы это было незаметно.

Один из методов стеганографии, как я упоминал ранее, это LSB (Least Significant Bit) метод. Суть его заключается в том, что мы заменяем наименее значимый бит каждого цветового канала пикселя изображения на биты нашего секретного сообщения. Поскольку эти изменения очень малы, человеческий глаз не замечает их, и изображение остается практически неизменным визуально.

Таким образом, мы можем внедрить наше секретное сообщение в изображение, не привлекая нежелательного внимания. После этого наш друг, который знает о нашей методике, сможет извлечь это сообщение из изображения, используя тот же самый метод.

Это один из примеров использования стеганографии для защиты информации, но методика применима и к другим типам данных, таким как звуковые файлы или текстовые документы.

Современная компьютерная стенография, перспективы и ее основные задачи.

Конечно, давайте поговорим о современной компьютерной стенографии, ее перспективах и основных задачах. Это увлекательная и важная область в сфере информационной безопасности, которая заслуживает нашего внимания.

Что такое компьютерная стенография?

Компьютерная стенография - это наука о скрытии информации внутри другой информации таким образом, чтобы это было незаметно для посторонних. Представьте, что вы отправляете файл с изображением своему другу, но внутри этого изображения также скрыто секретное сообщение, которое видит только ваш друг. Или вы загружаете звуковой файл, а внутри него скрыто аудио, которое может быть расшифровано только специальным образом. Это и есть компьютерная стенография.

Перспективы современной компьютерной стенографии

С развитием технологий современная компьютерная стенография становится все более утонченной и сложной. Сегодняшние алгоритмы и методы стенографии могут скрывать информацию в различных типах данных, включая изображения, аудио, видео и текстовые файлы. Благодаря этому, стенографические методы становятся более эффективными и трудноразличимыми для обнаружения.

Основные задачи компьютерной стенографии

1. *Защита конфиденциальной информации*. Одной из основных задач стенографии является защита конфиденциальной информации от несанкционированного доступа. С помощью стенографических методов данные могут быть скрыты и переданы таким образом, чтобы только авторизованный получатель мог их раскрыть.

2. *Скрытая передача информации*. Еще одной важной задачей стенографии является возможность передавать информацию скрыто, не привлекая внимания третьих лиц. Это может быть

полезно, например, для шпионажа или обмена секретными данными в условиях повышенной конфиденциальности.

3. *Обеспечение целостности данных*. Стенографические методы также могут использоваться для обеспечения целостности данных. Например, цифровые подписи могут быть скрыты внутри файлов для подтверждения их подлинности и неповрежденности.

4. *Прикрытие передачи информации*. Стенография может использоваться для прикрытия передачи информации, чтобы скрыть факт коммуникации между отправителем и получателем.

В целом, современная компьютерная стенография играет важную роль в обеспечении безопасности информации и обмена секретными данными. Она продолжает развиваться, и будущее этой области обещает еще больше инноваций и новых методов для скрытой передачи информации.

Компьютерная стенография маскировка программного обеспечения.

Конечно, давайте поговорим о компьютерной стенографии в контексте маскировки программного обеспечения. Это интересная тема, которая касается скрытия программного кода или действий программы таким образом, чтобы это было незаметно для пользователя или других программ.

Что такое компьютерная стенография в контексте маскировки программного обеспечения?

Компьютерная стенография в контексте маскировки программного обеспечения - это метод, при котором программное обеспечение скрывает своё существование или свои действия от пользователей или других программ. Это может быть сделано различными способами, от изменения имени файла или папки до скрытого выполнения задач в операционной системе.

Примеры компьютерной стенографии в маскировке программного обеспечения.

1. **Руткиты.** Руткиты - это вредоносные программы, которые скрывают своё присутствие в системе, модифицируя её компоненты. Например, они могут изменять системные файлы или

драйверы таким образом, чтобы антивирусные программы не могли обнаружить их.

2. **Скрытые процессы**. Некоторые программы могут скрывать свои рабочие процессы от диспетчера задач операционной системы. Это может быть сделано путем изменения атрибутов процесса или использования специальных техник инъекций в другие процессы.

3. **Скрытые файлы и папки**. Программы могут создавать скрытые файлы или папки, которые не видны обычному пользователю при обзоре файловой системы. Например, скрытые файлы могут использоваться для хранения конфигурационной информации или других данных, которые программе нужно сохранить невидимыми.

4. **Скрытые сетевые активности**. Некоторые программы могут маскировать свою сетевую активность, чтобы они не были обнаружены международными брандмауэрами или интрузионными системами обнаружения.

Почему это важно?

Маскировка программного обеспечения может использоваться как для добрых, так и для злых целей. С одной стороны, это может быть использовано для защиты конфиденциальности данных или для предотвращения обнаружения вредоносного программного обеспечения. С другой стороны, это также может быть использовано злоумышленниками для скрытой передачи вредоносных действий или для обхода мер безопасности.

В любом случае, понимание методов компьютерной стенографии в контексте маскировки программного обеспечения важно для обеспечения безопасности информации и защиты от возможных угроз.

Защита авторских прав.

Конечно, давайте поговорим о защите авторских прав в онлайн-среде. Это важная тема, особенно с учетом распространения цифрового контента в интернете и возможностей его незаконного использования. Основные аспекты защиты

авторских прав и способы борьбы с нарушениями, а также приведем конкретные примеры.

1. **Защита авторских прав в интернете**

С ростом популярности интернета и онлайн-контента стало все сложнее обеспечить защиту авторских прав. В интернете легко копировать, распространять и использовать чужие работы без разрешения владельца авторских прав. Однако существуют методы и механизмы защиты, которые помогают авторам защитить свои права и бороться с нарушителями.

2. **Механизмы защиты авторских прав**

Авторские права и лицензии. Первым шагом к защите авторских прав является регистрация авторских прав на произведение и установление лицензионных условий, которые определяют права и обязанности пользователей относительно использования контента.

Технические средства защиты. Существуют различные технические средства защиты, такие как цифровые подписи, шифрование и технологии DRM (Digital Rights Management), которые помогают ограничить доступ к контенту и предотвратить его незаконное копирование и распространение.

Автоматизированные системы мониторинга. Многие правообладатели используют специальные программные системы для мониторинга интернета на предмет нарушений авторских прав. Такие системы могут автоматически обнаруживать нарушения и принимать меры по их пресечению.

3. **Примеры нарушений авторских прав в интернете**

Незаконное скачивание и распространение контента. Это одна из наиболее распространенных форм нарушения авторских прав. Например, когда пользователь скачивает музыку, фильмы или книги из интернета без разрешения автора или правообладателя.

Пиратство и торрент-трекеры. На торрент-трекерах и в сети BitTorrent часто можно найти копии фильмов, музыки, программ и другого контента, которые распространяются без согласия правообладателей.

Незаконные копии веб-сайтов и блогов. Иногда содержимое веб-сайтов или блогов копируется и используется без разрешения авторов, что также является нарушением авторских прав.

4. **Защита авторских прав в действии**

Примером успешной защиты авторских прав в интернете может служить работа специализированных компаний, которые предоставляют услуги по мониторингу и борьбе с нарушениями. Например, YouTube использует систему Content ID, которая автоматически обнаруживает нарушения авторских прав в видео и позволяет правообладателям принимать меры, такие как блокировка или монетизация контента.

Защита авторских прав в интернете является важной задачей для сохранения интеллектуальной собственности и справедливого вознаграждения за творческий труд. Различные

Информация о стенографических программах.

Конечно, давайте поговорим о стенографических программах. Это программы, которые позволяют скрывать информацию внутри других файлов таким образом, чтобы это было незаметно для человеческого взгляда или обычных методов анализа файлов. Давайте рассмотрим основные аспекты таких программ и некоторые популярные примеры.

Что такое стенографические программы?

Стенографические программы - это специализированные инструменты, которые позволяют скрывать конфиденциальную информацию внутри других файлов, таких как изображения, аудио или видео, без видимых изменений для обычного наблюдателя. Это может быть использовано для защиты конфиденциальности данных или для скрытой передачи информации.

Как они работают?

Эти программы используют различные методы стеганографии для встраивания скрытой информации в носитель, например, в изменение пикселей изображения, манипуляции с битами аудиофайлов или даже внесение изменений в кодировку текстовых

файлов. Обычно они предоставляют пользователю интерфейс для выбора файла, который будет использоваться в качестве носителя, и ввода секретного сообщения или файла для скрытия.

Примеры стенографических программ.

1. **OpenStego.** Это бесплатная и открытая стенографическая программа с отличным набором функций. Она поддерживает различные методы стеганографии и позволяет скрывать данные в изображениях, аудиофайлах и тексте.
2. **Steghide.** Еще одна популярная программа, предоставляющая возможности стеганографии. Steghide поддерживает скрытие данных в изображениях и аудиофайлах с использованием различных алгоритмов шифрования.
3. **OutGuess.** Эта программа специализируется на скрытии информации в изображениях с минимальными изменениями в самом изображении. Она широко используется для стеганографии в изображениях с низким качеством, таких как фотографии в социальных сетях.

Зачем они нужны? Стенографические программы могут быть полезны для защиты конфиденциальной информации, такой как пароли, ключи шифрования или другие секретные данные. Они также могут использоваться для скрытой передачи информации, например, при обмене секретными сообщениями между агентами или для защиты коммерческих секретов.

Важно помнить. Хотя стенография может быть эффективным методом скрытия информации, она не является непреодолимой. Если злоумышленник получит доступ к скрытому файлу или узнает о методе стеганографии, он может попытаться раскрыть скрытую информацию. Поэтому важно использовать дополнительные методы защиты информации в сочетании со стенографией для обеспечения максимальной безопасности данных.

Контрольные вопросы.

1. Что представляет собой стенография?
2. Какие основные принципы лежат в основе стенографической защиты информации?

3. Какие типы файлов могут использоваться в стеганографии для скрытия информации?
4. Какие могут быть применения стеганографической защиты информации в современном мире?
5. Что такое LSB (Least Significant Bit) метод?
6. Как работает метод скрытия информации в частотной области?
7. Какие еще методы используются в стеганографии помимо LSB и частотной области?
8. Какие факторы могут повлиять на эффективность стеганографической защиты информации?
9. Какие основные задачи решает современная компьютерная стеганография?
10. Какие технологические тенденции определяют перспективы развития компьютерной стеганографии?
11. Каким образом компьютерная стеганография может быть использована в целях безопасности информации?
12. Каковы преимущества и недостатки современной компьютерной стеганографии?
13. Что такое компьютерная стеганография в контексте маскировки программного обеспечения?
14. Какие методы маскировки программного обеспечения используются в компьютерной стеганографии?
15. Какие могут быть применения маскировки программного обеспечения в современном мире?
16. Каким образом маскировка программного обеспечения связана с безопасностью информации?
17. Что представляют собой авторские права и почему они важны в интернете?
18. Какие могут быть методы защиты авторских прав в онлайн-среде?
19. Какие могут быть последствия нарушения авторских прав в интернете?
20. Какие технологии используются для борьбы с нарушениями авторских прав в интернете?

21. Что представляют собой стенографические программы?
22. Какие типы файлов могут использоваться для скрытия информации с помощью стенографических программ?
23. Какие примеры стенографических программ вы знаете?
24. Для чего могут использоваться стенографические программы и каковы возможные риски их использования?

Тесты для закрепления темы.

1. **Что такое стенографическая защита информации?**
   а) Процесс перевода текста на другой язык
   б) Метод скрытия секретной информации в других данных
   в) Система шифрования сообщений
   г) Метод аутентификации пользователей
   Ответ. б) Метод скрытия секретной информации в других данных
2. **Какой из следующих методов является одним из наиболее распространенных в стенографической защите информации?**
   а) RSA
   б) AES
   в) LSB
   г) HMAC
   Ответ. в) LSB
3. **Какие данные можно использовать для стеганографической защиты информации?**
   а) Только текстовые документы
   б) Только изображения
   в) Только звуковые файлы
   г) Различные форматы данных, включая изображения, звуковые файлы и текстовые документы
   Ответ. г) Различные форматы данных, включая изображения, звуковые файлы и текстовые документы
4. **Какие могут быть потенциальные угрозы стенографической защиты информации?**
   а) Невозможность скрыть информацию
   б) Раскрытие секретной информации третьим лицам

в) Только атаки на стеганографические программы

г) Только возможность перехвата данных при передаче

Ответ. б) Раскрытие секретной информации третьим лицам

5. **Что представляет собой компьютерная стенография?**

а) Процесс кодирования паролей

б) Метод скрытия информации внутри другой информации

в) Создание цифровой подписи для файлов

г) Метод шифрования электронной почты

Ответ. б) Метод скрытия информации внутри другой информации

6. **Какой из следующих форматов данных может быть использован для стенографической передачи информации?**

а) Только текстовые файлы

б) Только изображения

в) Только аудиофайлы

г) Различные типы файлов, включая текстовые, изображения, аудио и видео

Ответ. г) Различные типы файлов, включая текстовые, изображения, аудио и видео

7. **Какой из следующих методов является наиболее распространенным в компьютерной стенографии?**

а) RSA

б) AES

в) LSB

г) HMAC

Ответ. в) LSB

8**. Какова основная задача компьютерной стенографии?**

а) Повышение скорости передачи данных

б) Защита конфиденциальной информации

в) Оптимизация производительности компьютера

г) Создание вирусов

Ответ. б) Защита конфиденциальной информации

9. **Какие из перечисленных методов могут использоваться для компьютерной стенографии?**

а) Изменение метаданных файлов

б) Использование скрытых каналов в сети

в) Скрытая передача информации через текстовые документы

г) Все вышеперечисленные методы

Ответ. г) Все вышеперечисленные методы

10. **Какой из перечисленных способов НЕ является примером компьютерной стеганографии в маскировке программного обеспечения?**

а) Изменение имени файла или папки

б) Создание скрытых файлов и папок

в) Публичное оповещение о программе

г) Скрытие процессов в операционной системе

Ответ. в) Публичное оповещение о программе

11. **Как называются вредоносные программы, которые скрывают своё присутствие в системе, модифицируя её компоненты?**

а) Вирусы

б) Руткиты

в) Троянские кони

г) Черви

Ответ. б) Руткиты

12. **Какой из следующих методов НЕ связан с маскировкой программного обеспечения?**

а) Скрытие сетевой активности

б) Скрытие процессов

в) Использование аутентификации

г) Создание скрытых файлов и папок

Ответ. в) Использование аутентификации

13. **Какой метод маскировки программного обеспечения включает в себя создание скрытых файлов или папок, которые не видны обычному пользователю?**

а) Скрытие сетевой активности

б) Скрытие процессов

в) Создание руткитов

г) Создание скрытых файлов и папок

Ответ. г) Создание скрытых файлов и папок

14. **Какой из перечисленных методов является примером компьютерной стеганографии в маскировке программного обеспечения?**

а) Публичное оповещение о программе

б) Изменение метаданных файла

в) Скрытие процессов в операционной системе

г) Создание цифровой подписи для файла

Ответ. в) Скрытие процессов в операционной системе

15. **Что представляют собой авторские права в интернете?**

а) Возможность бесплатно копировать контент

б) Защита прав владельца контента на его использование и распространение

в) Необходимость публикации контента под открытой лицензией

г) Процесс автоматической публикации контента в сети Интернет

Ответ. б) Защита прав владельца контента на его использование и распространение

16. ***Какие из перечисленных методов являются механизмами защиты авторских прав в интернете?***

а) Цифровые подписи

б) Публичное представление работы

в) Открытая лицензия

г) Все вышеперечисленные

Ответ. а) Цифровые подписи

17. **Какой из следующих примеров является нарушением авторских прав в интернете?**

а) Публикация работы с разрешением автора и указанием ссылки на источник

б) Использование материалов с сайта с открытой лицензией для коммерческих целей без разрешения

в) Комментирование на блоге с цитированием кратких выдержек из статьи с указанием автора

г) Публикация собственных фотографий в социальных сетях

Ответ. б) Использование материалов с сайта с открытой лицензией для коммерческих целей без разрешения

19. **Какая технология используется для автоматического обнаружения нарушений авторских прав на видеоконтенте в YouTube?**

а) Цифровые подписи

б) Система Content ID

в) DRM (Управление цифровыми правами)

г) Публичные лицензии

Ответ. б) Система Content ID

20. **Какие могут быть последствия нарушения авторских прав в интернете?**

а) Потеря доступа к интернету

б) Штрафные санкции и судебные разбирательства

в) Бесплатное распространение контента

г) Продвижение автора и его работ

Ответ. б) Штрафные санкции и судебные разбирательства

21. **Что представляют собой стенографические программы?**

а) Программы для написания стенографических текстов

б) Инструменты для скрытия информации внутри других файлов

в) Приложения для расшифровки секретных сообщений

г) Программы для анализа аудиоспектров

Ответ. б) Инструменты для скрытия информации внутри других файлов

22. **Какие типы файлов могут использоваться для скрытия информации с помощью стенографических программ?**

а) Только текстовые файлы

б) Только аудиофайлы

в) Различные типы файлов, такие как изображения, аудио и текст

г) Только исполняемые файлы

Ответ. в) Различные типы файлов, такие как изображения, аудио и текст

23. **Какие программы являются примерами стенографических программ?**

а) Photoshop и Adobe Premiere

б) Microsoft Word и Excel

в) Steghide и OpenStego

г) Google Chrome и Mozilla Firefox

Ответ. в) Steghide и OpenStego

24. **Для чего могут использоваться стенографические программы?**

а) Только для шифрования файлов

б) Только для создания скрытых архивов

в) Для защиты конфиденциальной информации и скрытой передачи данных

г) Только для создания стеганографических изображений

Ответ. в) Для защиты конфиденциальной информации и скрытой передачи данных

25. **Каковы возможные риски использования стенографических программ?**

а) Риск неправильного отображения скрытой информации

б) Риск потери исходной информации

в) Риск обнаружения скрытой информации и нарушения безопасности

г) Все вышеперечисленное

Ответ. г) Все вышеперечисленное

§2.5. Основы криптосистемы.

Понятие криптографии. Основы криптосистемы. Криптографическая защита. Криптографические системы и связанные с ними примеры. Цель и задачи криптографии. Криптографическая защита. Методы криптографической защиты информации. Принципы криптографической защиты информации.

Понятие криптографии.

Криптография — это наука о защите информации от несанкционированного доступа и подделки путем ее шифрования.

Она имеет древние корни и играла важную роль во многих исторических событиях, начиная с времен древних цивилизаций до современности. Суть криптографии заключается в том, чтобы передать сообщение таким образом, чтобы его могли прочитать только те, кому оно адресовано.

Основные цели криптографии включают конфиденциальность (сообщение может быть прочитано только теми, кому оно предназначено), целостность (сообщение не было изменено в процессе передачи) и аутентификацию (проверка подлинности отправителя сообщения).

С развитием компьютерной технологии криптография стала играть все более важную роль в сфере информационной безопасности. Современная криптография включает в себя использование сложных математических алгоритмов для шифрования данных, а также разработку криптографических протоколов и систем, обеспечивающих защиту информации в цифровой среде.

Применение криптографии включает в себя защиту конфиденциальности персональной информации, банковских данных, коммерческой тайны, государственных секретов и многого другого. Она также играет важную роль в обеспечении безопасности сетей связи, интернет-протоколов, электронной коммерции и цифровых платежей.

Рисунок 2.3. Понятие криптографии

Тем не менее, криптография постоянно развивается, поскольку с появлением новых вычислительных мощностей и методов взлома возникают новые вызовы и угрозы для безопасности информации. Поэтому постоянные исследования и инновации в области криптографии остаются важной составляющей в сфере информационной безопасности.

Основы криптосистемы.

1. **Введение в криптосистемы**.

Криптосистема - это система, используемая для шифрования и дешифрования информации с целью обеспечения ее конфиденциальности.

Основные цели криптосистем. конфиденциальность, целостность и аутентификация.

2. **Основные компоненты криптосистемы**.

а) *Шифр*. Математический алгоритм, применяемый для шифрования данных.

б) *Ключ*. Параметр, используемый вместе с шифром для шифрования и дешифрования информации.

в) *Протоколы*. Совокупность правил и процедур, определяющих способы использования шифров и ключей для обмена зашифрованной информацией.

3. **Основные типы криптосистем**.

а) *Симметричные криптосистемы*. Используют один и тот же ключ для шифрования и дешифрования данных. Примеры. AES, DES.

б) *Асимметричные криптосистемы*. Используют разные ключи для шифрования и дешифрования данных. Примеры. RSA, ECC.

4. **Принцип работы криптосистем**.

В симметричных криптосистемах. Отправитель и получатель используют один и тот же секретный ключ для шифрования и дешифрования сообщений.

В асимметричных криптосистемах. Каждый участник имеет пару ключей - открытый и закрытый. Отправитель шифрует сообщение открытым ключом получателя, и только получатель может расшифровать его с помощью своего закрытого ключа.

5. **Применение криптосистем**.

Криптосистемы применяются в различных областях, включая защиту конфиденциальной информации в сети Интернет, обеспечение безопасности электронной почты, аутентификацию пользователей и защиту цифровых подписей.

6. **Важность безопасности криптосистем**.

Безопасность криптосистем является критически важной, поскольку любые уязвимости или недостатки могут привести к разглашению конфиденциальной информации или возможности несанкционированного доступа.

В заключение, криптосистемы играют важную роль в обеспечении конфиденциальности и безопасности информации. Понимание их основных принципов и компонентов необходимо для разработки и реализации надежных систем защиты данных.

Криптографическая защита.

Криптографическая защита – это метод обеспечения безопасности информации путем использования различных криптографических техник. Она играет ключевую роль в современном мире, где цифровая информация становится все более ценной и подверженной угрозам.

Основная задача криптографической защиты заключается в том, чтобы предотвратить несанкционированный доступ к конфиденциальным данным и защитить их от несанкционированных изменений. Это достигается путем применения различных методов шифрования, которые делают данные непонятными и недоступными для тех, кто не имеет права доступа.

Основные принципы криптографической защиты включают конфиденциальность, целостность и аутентификацию. Конфиденциальность гарантирует, что только авторизованные пользователи могут получить доступ к информации. Целостность обеспечивает, что данные не были изменены в процессе передачи или хранения. Аутентификация подтверждает подлинность отправителя и получателя данных.

Существует два основных типа криптографической защиты. *симметричная и асимметричная*. В *симметричной криптографии* используется один и тот же ключ для шифрования и дешифрования данных, в то время как в *асимметричной криптографии* используются пары ключей – открытый и закрытый.

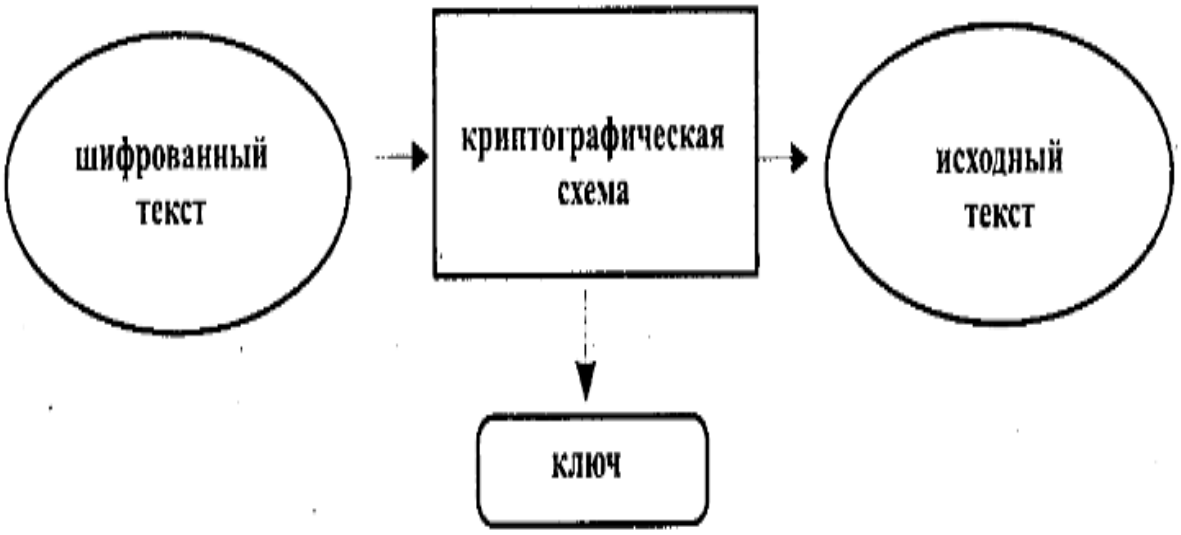

Рисунок 2.4. Шифрование текста

Шифрование файлов

Применение криптографической защиты распространяется на множество областей, включая информационную безопасность, электронную коммерцию, банковское дело, медицину и многое другое. Она используется для защиты персональных данных, финансовых транзакций, корпоративных секретов и государственных секретов.

Криптографическая защита является неотъемлемой частью современной информационной безопасности и играет важную роль в обеспечении конфиденциальности и целостности данных в цифровой эпохе**.**

Криптографические системы и связанные с ними примеры.

Криптография - это наука о безопасной передаче информации. Основной задачей криптографии является защита данных от несанкционированного доступа, а также обеспечение их конфиденциальности, целостности и аутентификации.

Симметричные криптосистемы. Используют один и тот же ключ для шифрования и дешифрования данных. Примеры. DES, AES.

Асимметричные криптосистемы. Используют пару ключей - открытый и закрытый. Открытый ключ используется для шифрования, а закрытый - для дешифрования. Примеры. RSA, ECC.

Примеры криптографических систем.

1. *DES (Data Encryption Standard).* Одна из первых симметричных криптосистем, разработанная в 1970-х годах. Использует 56-битные ключи и является стандартом для шифрования данных в различных системах.

2. *AES (Advanced Encryption Standard).* Симметричная криптосистема, разработанная в 2001 году как замена для DES. Использует 128-, 192- или 256-битные ключи и является одним из наиболее надежных алгоритмов шифрования.

3. *RSA (Rivest–Shamir–Adleman).* Одна из наиболее известных асимметричных криптосистем, основанная на математической проблеме факторизации больших простых чисел. RSA широко используется для создания цифровых подписей и защиты данных в сети Интернет.

4. *ECC (Elliptic Curve Cryptography).* Асимметричная криптосистема, основанная на математических проблемах эллиптических кривых. ECC обладает высокой стойкостью к атакам и является одним из наиболее эффективных методов шифрования для устройств с ограниченными ресурсами, таких как смартфоны и интернет-подключенные устройства.

Криптографические системы играют ключевую роль в обеспечении безопасности данных в цифровой эпохе. Понимание различий между симметричными и асимметричными криптосистемами, а также знание примеров таких систем, помогает разработчикам и специалистам по информационной безопасности выбирать наиболее подходящие методы защиты для конкретных задач и систем.

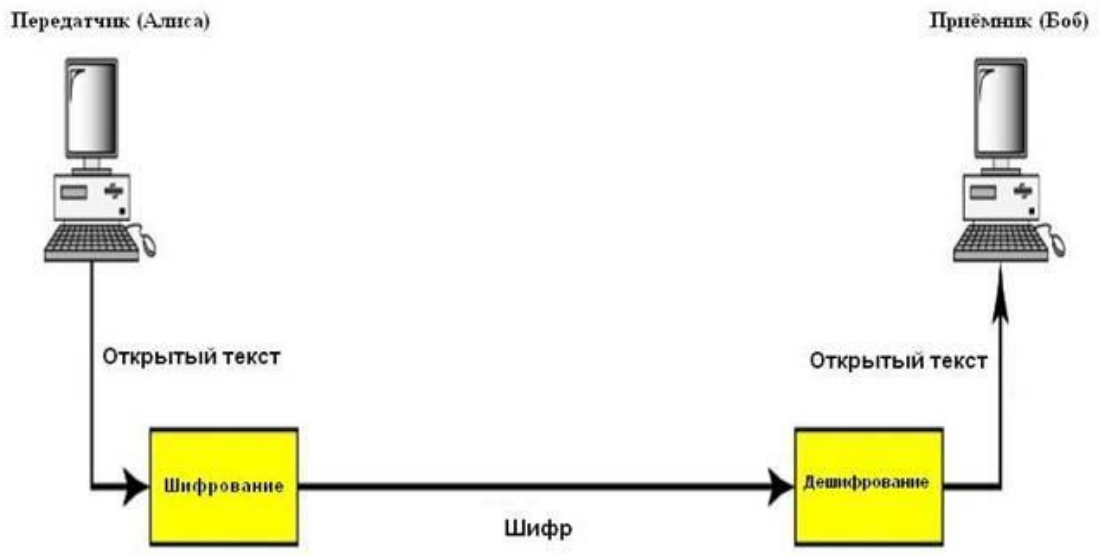

Рисунок 2.4. Криптографические методы защиты

Цель и задачи криптографии.

Криптография - это наука о методах обеспечения конфиденциальности, целостности и аутентификации информации путем ее шифрования и подписывания. Она играет важную роль в защите данных от несанкционированного доступа и использования.

Цели криптографии

Конфиденциальность. Одной из основных целей криптографии является обеспечение конфиденциальности информации. Это означает, что только авторизованные пользователи должны иметь доступ к зашифрованным данным, и никто другой не должен иметь возможность их прочитать.

Целостность. Криптография также направлена на обеспечение целостности данных. Это означает, что информация не должна изменяться незамеченной сторонними лицами в процессе передачи или хранения.

Аутентификация. Еще одной целью криптографии является обеспечение аутентификации, то есть подтверждение подлинности и идентификации участников обмена информацией. Это позволяет убедиться, что данные отправлены и получены именно от тех лиц, которые они утверждают.

Задачи криптографии

Шифрование. Одной из основных задач криптографии является разработка методов шифрования, которые позволяют скрыть содержание сообщений от несанкционированных лиц.

Расшифрование. Криптография также занимается разработкой методов расшифрования, позволяющих получателю сообщения правильно восстановить исходную информацию из зашифрованного текста.

Аутентификация. Криптографические методы используются для проверки подлинности данных, например, при проверке цифровых подписей или аутентификации пользователей.

Цифровая подпись. Еще одной задачей криптографии является разработка методов создания и проверки цифровых подписей, которые обеспечивают подлинность и неотказуемость сообщений.

Цель и задачи криптографии связаны с обеспечением безопасности информации в цифровой среде. Понимание этих целей и задач помогает разработчикам и специалистам по информационной безопасности выбирать наиболее подходящие методы защиты данных и обеспечивать их безопасность.

Криптографическая защита.

Криптографическая защита. Основы и Примеры

Криптографическая защита - это набор методов и технологий, используемых для обеспечения безопасности информации путем ее шифрования и подписывания. Она играет важную роль в современном мире, где безопасность данных становится все более критической.

Основные принципы криптографической защиты

Конфиденциальность. Один из основных принципов криптографии, который обеспечивает защиту данных от несанкционированного доступа. Путем шифрования информации только авторизованные пользователи могут получить доступ к ней.

Целостность. Еще один важный принцип, который гарантирует, что данные не были изменены в процессе передачи

или хранения. При использовании криптографической защиты даже незначительные изменения в данных будут обнаружены.

Аутентификация. Принцип, обеспечивающий проверку подлинности и идентификации участников обмена информацией. Это позволяет убедиться, что данные отправлены и получены именно от тех лиц, которые они утверждают.

Примеры криптографической защиты

Шифрование данных. Примером криптографической защиты является использование шифрования для скрытия содержания сообщений от несанкционированных лиц. Например, алгоритм AES (Advanced Encryption Standard) используется для шифрования данных в различных системах и приложениях.

Цифровая подпись. Еще одним примером является использование цифровых подписей для обеспечения аутентификации и подлинности данных. Например, алгоритм RSA (Rivest-Shamir-Adleman) используется для создания цифровых подписей, которые можно проверить на подлинность.

SSL/TLS протоколы. Эти протоколы обеспечивают защищенное соединение между клиентом и сервером в сети Интернет. Они используют криптографические методы для шифрования и аутентификации данных, обеспечивая конфиденциальность и безопасность во время передачи.

Криптографическая защита играет ключевую роль в обеспечении безопасности информации в цифровой эпохе. Понимание основных принципов и примеров криптографической защиты помогает разработчикам и специалистам по информационной безопасности выбирать наиболее эффективные методы защиты данных.

Методы криптографической защиты информации.

Шифрование - это процесс преобразования исходного текста в нечитаемую форму (шифр) с использованием специального ключа. Это один из наиболее распространенных методов криптографической защиты. Примером шифрования является алгоритм AES (Advanced Encryption Standard), который шифрует

данные с использованием ключа и делает их непонятными для неавторизованных лиц.

Цифровые подписи

Цифровая подпись - это метод криптографической защиты, который используется для подтверждения подлинности и целостности документа или сообщения. Она создается путем хеширования документа и шифрования хеш-значения с использованием закрытого ключа отправителя. Примером цифровой подписи является алгоритм RSA (Rivest-Shamir-Adleman), который широко используется для создания электронных подписей в электронных документах и электронной почте.

Протоколы безопасности

Протоколы безопасности - это наборы правил и процедур, которые обеспечивают защиту данных при их передаче через открытые сети, такие как интернет. Примером таких протоколов являются SSL (Secure Sockets Layer) и его более современная версия TLS (Transport Layer Security), которые используются для обеспечения защищенного соединения между веб-браузером и сервером во время онлайн-транзакций и передачи конфиденциальной информации.

Хеширование

Хеширование - это процесс преобразования произвольного входного значения в фиксированную строку фиксированной длины (хеш-значение). Хеш-значение обычно используется для проверки целостности данных. Примером алгоритма хеширования является SHA-256 (Secure Hash Algorithm 256-bit), который создает 256-битное хеш-значение для входных данных и широко используется для проверки целостности файлов и паролей.

Аутентификация

Аутентификация - это процесс проверки подлинности участников обмена информацией. Это важный метод криптографической защиты, который гарантирует, что только правильные пользователи имеют доступ к данным или ресурсам.

Примерами аутентификации являются пароли, биометрические данные (например, отпечатки пальцев) и аутентификационные токены.

Принципы криптографической защиты информации.

1. Конфиденциальность

Конфиденциальность - это принцип, гарантирующий, что только авторизованные лица имеют доступ к конфиденциальной информации. В криптографии это достигается путем шифрования данных. Пример. когда вы отправляете личное сообщение через зашифрованный мессенджер, только вы и получатель, имеющий ключ, могут прочитать его, что обеспечивает конфиденциальность вашего общения.

2. Целостность

Целостность обеспечивает гарантию, что данные остаются нетронутыми и неизменными во время передачи или хранения. Для этого используется метод хеширования, который создает уникальное "отпечаток" данных. Если данные изменятся, хеш-значение также изменится. Например, когда вы загружаете файл из интернета, хеш-сумма файла предоставляет возможность проверить его целостность.

3. Аутентификация

Аутентификация - это процесс проверки подлинности участников обмена информацией. Она гарантирует, что участник, с которым вы взаимодействуете, является тем, за кого себя выдает. Пример. когда вы входите в свой аккаунт в онлайн-банке, используя пароль и логин, банк аутентифицирует вас перед предоставлением доступа к вашим финансовым данным.

4. Неотказуемость

Принцип неотказуемости обеспечивает гарантию, что отправитель не может отказаться от отправленного сообщения или действия. Это достигается через использование цифровой подписи, которая ассоциирует сообщение с конкретным отправителем. Например, когда вы подписываете электронный документ своим цифровым ключом, вы не можете отказаться от его авторства.

5. Доступность

Доступность обеспечивает гарантию того, что данные доступны для авторизованных пользователей в нужное время и место. Хотя это не является непосредственно частью криптографии, она важна для общей защиты информации. Например, когда вы получаете доступ к онлайн-сервису, его система должна быть доступна для вас в любое удобное для вас время.

Контрольные вопросы.

1. Что такое криптография?
2. Какие основные цели преследует криптография?
3. Что такое криптосистема?
4. Какие основные компоненты включает в себя криптосистема?
5. Какие методы используются для криптографической защиты информации?
6. Какие принципы лежат в основе криптографической защиты?
7. Приведите примеры криптографических систем.
8. Какие примеры алгоритмов шифрования вы можете назвать?
9. Какие цели преследует криптография?
10. Какие задачи решает криптография для обеспечения безопасности информации?
11. Что такое цифровая подпись и как она используется для криптографической защиты?
12. Какие методы шифрования данных вы можете назвать?
13. Что обеспечивает принцип конфиденциальности в криптографической защите информации?
14. Какой принцип обеспечивает гарантию того, что данные остаются нетронутыми и неизменными во время передачи или хранения?

Тесты для закрепления темы.

1. **Что представляет собой криптография?**

a) Изучение криптовалют

b) Наука о защите информации путем шифрования

c) Методика хранения паролей

d) Технология анонимного серфинга в интернете

Ответ. b) Наука о защите информации путем шифрования

2. **Какие основные цели криптографии?**

a) Креативное программирование

b) Защита от вирусов

c) Конфиденциальность, целостность, аутентификация

d) Ускорение работы компьютера

Ответ. c) Конфиденциальность, целостность, аутентификация

3. **Какие методы используются в современной криптографии для шифрования данных?**

a) Секретные рукописи

b) Математические алгоритмы

c) Гаджеты и устройства

d) Криптоключи

Ответ. b) Математические алгоритмы

4. **В каких областях применяется криптография?**

a) Только в банковском секторе

b) Только в правительственных структурах

c) В сфере информационной безопасности, интернет-протоколов, электронной коммерции и многих других

d) Только в области телекоммуникаций

Ответ. c) В сфере информационной безопасности, интернет-протоколов, электронной коммерции и многих других

5. **Что представляет собой ключ в криптосистеме?**

a) Математический алгоритм для шифрования данных

b) Параметр, используемый вместе с шифром для шифрования и дешифрования информации

c) Правила и процедуры для обмена зашифрованной информацией

d) Система, обеспечивающая конфиденциальность данных

Ответ. b) Параметр, используемый вместе с шифром для шифрования и дешифрования информации

6. **Какие типы криптосистем существуют?**

a) Только симметричные

b) Только асимметричные

c) Симметричные и асимметричные

d) Трехсторонние

Ответ. c) Симметричные и асимметричные

7. **В чем заключается принцип работы симметричных криптосистем?**

a) Отправитель и получатель используют разные ключи для шифрования и дешифрования данных

b) Отправитель и получатель используют один и тот же ключ для шифрования и дешифрования данных

c) Каждый участник имеет пару ключей - открытый и закрытый

d) Ключи генерируются автоматически

Ответ. b) Отправитель и получатель используют один и тот же ключ для шифрования и дешифрования данных

8. **Для чего применяются криптосистемы?**

a) Только для шифрования текстовых сообщений

b) Только для защиты банковских данных

c) Для обеспечения конфиденциальности, целостности и аутентификации информации

d) Для ускорения работы компьютеров

Ответ. c) Для обеспечения конфиденциальности, целостности и аутентификации информации

9. **Какие компоненты входят в состав криптосистемы?**

a) Только шифр

b) Только ключ

c) Шифр, ключ и протоколы

d) Протоколы и алгоритмы

Ответ. c) Шифр, ключ и протоколы

10. **Что представляет собой криптографическая защита?**

a) Метод обучения нейронных сетей

b) Способ защиты информации с использованием криптографических методов

c) Алгоритм сжатия данных

d) Процесс взлома компьютерных систем

Ответ. b) Способ защиты информации с использованием криптографических методов

11. **Какие основные принципы криптографической защиты?**

a) Секретность и обман

b) Конфиденциальность, целостность и аутентификация

c) Скорость и производительность

d) Простота и удобство использования

Ответ. b) Конфиденциальность, целостность и аутентификация

12. **Какие типы криптографической защиты существуют?**

a) Только симметричная

b) Только асимметричная

c) Симметричная и асимметричная

d) Трехсторонняя

Ответ. c) Симметричная и асимметричная

13. **В чем различие между симметричной и асимметричной криптографией?**

a) Симметричная использует один ключ, а асимметричная два ключа

b) Симметричная использует два ключа, а асимметричная один ключ

c) Симметричная быстрее, чем асимметричная

d) Асимметричная использует только открытый ключ

Ответ. a) Симметричная использует один ключ, а асимметричная два ключа

14. **Для чего применяется криптографическая защита?**

a) Только для шифрования текстовых сообщений

b) Только для скрытия информации от пользователей

c) Для обеспечения конфиденциальности, целостности и аутентификации информации

d) Для ускорения работы интернета

Ответ. c) Для обеспечения конфиденциальности, целостности и аутентификации информации

15. **Какие основные типы криптографических систем существуют?**

a) Только симметричные

b) Только асимметричные

c) Симметричные и асимметричные

d) Трехсторонние

Ответ. c) Симметричные и асимметричные

16. **Какой из приведенных алгоритмов является примером симметричной криптосистемы?**

a) RSA

b) AES

c) ECC

d) SHA-256

Ответ. b) AES

17. **Какой из приведенных алгоритмов является примером асимметричной криптосистемы?**

a) DES

b) AES

c) RSA

d) HMAC

Ответ. c) RSA

18. **В чем основное различие между симметричными и асимметричными криптосистемами?**

a) Симметричные используют один и тот же ключ для шифрования и дешифрования, а асимметричные - пару ключей.

b) Симметричные используют пару ключей, а асимметричные - один ключ.

c) Симметричные используют только открытый ключ, а асимметричные - только закрытый.

d) Симметричные работают быстрее, чем асимметричные.

Ответ. a) Симметричные используют один и тот же ключ для шифрования и дешифрования, а асимметричные - пару ключей.

19. **Для чего применяются криптографические системы?**

a) Только для шифрования текстовых сообщений

b) Только для скрытия информации от пользователей

c) Для обеспечения конфиденциальности, целостности и аутентификации информации

d) Для ускорения работы интернета

Ответ. c) Для обеспечения конфиденциальности, целостности и аутентификации информации

20. **Какая из перечисленных не является целью криптографии?**

a) Конфиденциальность

b) Целостность

c) Аутентификация

d) Сжатие данных

Ответ. d) Сжатие данных

21. **Какую из перечисленных задач криптографии называют "шифрованием"?**

a) Проверка подлинности данных

b) Сокрытие содержания сообщений от несанкционированных лиц

c) Создание и проверка цифровых подписей

d) Хранение информации в зашифрованном виде

Ответ. b) Сокрытие содержания сообщений от несанкционированных лиц

22. **Какой из следующих методов не является частью задач криптографии?**

a) Расшифрование

b) Аутентификация

c) Сжатие данных

d) Цифровая подпись

Ответ. c) Сжатие данных

23. **Какие из перечисленных являются основными целями криптографии?**

a) Сжатие данных, обеспечение конфиденциальности, ускорение работы систем

b) Конфиденциальность, целостность, аутентификация

c) Шифрование, создание цифровых подписей, управление доступом

d) Ответы a) и c)

Ответ. b) Конфиденциальность, целостность, аутентификация

24. **Какая задача криптографии связана с проверкой подлинности сообщений?**

a) Шифрование

b) Аутентификация

c) Расшифрование

d) Сжатие данных

Ответ. b) Аутентификация

25. **Какая из перечисленных не является целью криптографической защиты?**

a) Конфиденциальность

b) Целостность

c) Аутентификация

d) Сжатие данных

Ответ. d) Сжатие данных

26. **Какой принцип криптографической защиты обеспечивает проверку подлинности и идентификацию участников обмена информацией?**

a) Конфиденциальность

b) Целостность

c) Аутентификация

d) Сжатие данных

Ответ. c) Аутентификация

27. **Какой протокол обеспечивает защищенное соединение между клиентом и сервером в сети Интернет?**

a) HTTP

b) FTP

c) SSL/TLS

d) DNS

Ответ. c) SSL/TLS

28. **Какой из методов криптографической защиты используется для скрытия содержания сообщений от несанкционированных лиц?**

a) Цифровая подпись

b) Шифрование данных

c) Аутентификация

d) Сжатие данных

Ответ. b) Шифрование данных

29. **Какая задача криптографии направлена на гарантирование того, что данные не были изменены в процессе передачи или хранения?**

a) Шифрование

b) Аутентификация

c) Расшифрование

d) Целостность

Ответ. d) Целостность

30. **Какой из следующих методов криптографической защиты используется для создания электронных подписей?**

a) Шифрование данных

b) Цифровые подписи

c) Протоколы безопасности

d) Хеширование

Ответ. b) Цифровые подписи

31. **Какой алгоритм широко используется для шифрования данных с использованием ключа?**

a) RSA

b) SHA-256

c) AES

d) SSL

Ответ. c) AES

32. **Какой метод криптографической защиты используется для обеспечения защиты данных при их передаче через интернет?**

a) Хеширование

b) Аутентификация

c) Протоколы безопасности

d) Цифровые подписи

Ответ. c) Протоколы безопасности

33. **Какой из методов криптографической защиты используется для проверки целостности данных?**

a) Шифрование данных

b) Цифровые подписи

c) Хеширование

d) Аутентификация

Ответ. c) Хеширование

34. **Какой метод криптографической защиты направлен на проверку подлинности участников обмена информацией?**

a) Протоколы безопасности

b) Цифровые подписи

c) Аутентификация

d) Шифрование данных

Ответ. c) Аутентификация

35. **Что обеспечивает принцип конфиденциальности в криптографической защите информации?**

a) Гарантию, что данные остаются нетронутыми и неизменными во время передачи или хранения.

b) Проверку подлинности участников обмена информацией.

c) Гарантию, что только авторизованные лица имеют доступ к конфиденциальной информации.

d) Гарантию доступности данных для авторизованных пользователей.

Ответ. c) Гарантию, что только авторизованные лица имеют доступ к конфиденциальной информации.

36. **Какой метод криптографической защиты используется для проверки целостности данных?**

a) Шифрование данных

b) Цифровые подписи

c) Хеширование

d) Аутентификация

Ответ. c) Хеширование

37. **Какой принцип обеспечивает гарантию того, что отправитель не может отказаться от отправленного сообщения или действия?**

a) Конфиденциальность

b) Целостность

c) Аутентификация

d) Неотказуемость

Ответ. d) Неотказуемость

38. **Какой принцип криптографической защиты обеспечивает гарантию доступности данных для авторизованных пользователей?**

a) Конфиденциальность

b) Целостность

c) Аутентификация

d) Доступность

Ответ. d) Доступность

39. **Какой метод криптографической защиты используется для подтверждения подлинности и целостности документа или сообщения?**

a) Шифрование данных

b) Цифровые подписи

c) Протоколы безопасности

d) Аутентификация

Ответ. b) Цифровые подписи

§2.6. Безопасность в информационных системах.

Несанкционированное распространение информации и способы ее устранения.

Влиятельные части информационных систем.

Программно-технические средства несанкционированного доступа к информации.

Несанкционированное распространение информации и способы ее устранения.

Несанкционированное распространение информации — это ситуация, когда конфиденциальные или личные данные становятся доступными для людей, которые не должны иметь к ним доступ. Это может произойти по разным причинам. ошибки сотрудников, хакерские атаки, утечки данных и даже намеренные действия внутри компании. Такие инциденты могут привести к серьезным последствиям, включая финансовые потери, утрату репутации и юридические проблемы.

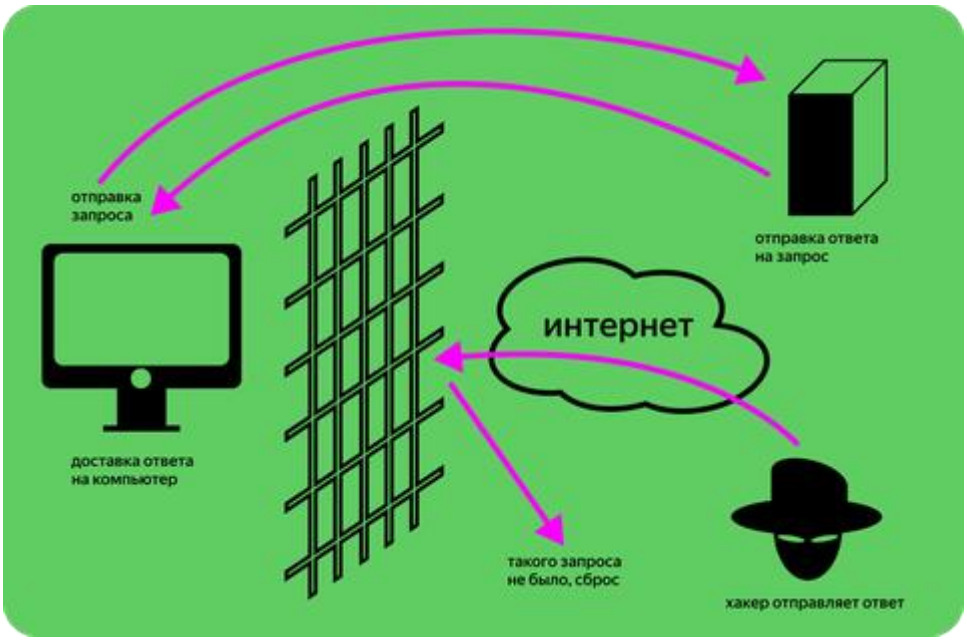

Рисунок 2.5. Технология защиты информации

Примеры реальных инцидентов

1. Утечка данных Facebook в 2019 году. Более 540 миллионов записей пользователей, включая имена, комментарии, лайки и другие данные, были обнаружены на общедоступных серверах. Это произошло из-за неправильного обращения с данными третьих сторон, которые использовали платформу.

2. Атака на Equifax в 2017 году. Хакеры получили доступ к личной информации 147 миллионов человек, включая номера социального страхования, адреса и даты рождения. Причиной послужили уязвимости в веб-приложении компании, которые не были своевременно устранены.

3. Инцидент с Marriott International в 2018 году. Хакеры получили доступ к данным более 500 миллионов клиентов. Взломанная информация включала номера паспортов, даты рождения и информацию о бронировании. Утечка продолжалась несколько лет, прежде чем была обнаружена.

Способы устранения и предотвращения

1. Обучение сотрудников. Одним из ключевых методов предотвращения утечек информации является регулярное обучение сотрудников. Они должны понимать важность защиты данных и знать, как правильно обращаться с конфиденциальной информацией. Например, использование сложных паролей и двухфакторной аутентификации может значительно снизить риск утечек.

2. Использование шифрования. Шифрование данных как в покое, так и при передаче помогает защитить информацию от несанкционированного доступа. Даже если данные будут украдены, они будут бесполезны без ключа для расшифровки.

3. Регулярное обновление программного обеспечения. Обновление систем и приложений позволяет устранить уязвимости, которые могут быть использованы хакерами для доступа к информации. Это включает не только операционные системы и приложения, но и любое сетевое оборудование.

4. Мониторинг и анализ. Постоянный мониторинг сетевого трафика и системных логов помогает быстро выявлять подозрительную активность. Современные системы анализа могут автоматически определять потенциальные угрозы и реагировать на них.

5. Контроль доступа. Ограничение доступа к информации на основе должностных обязанностей сотрудников помогает

уменьшить риск внутренней утечки данных. Только те, кому действительно необходимо иметь доступ к конфиденциальной информации, должны его получать.

6. План реагирования на инциденты. Наличие плана на случай утечки информации позволяет быстро и эффективно реагировать на инциденты. Это включает в себя уведомление пострадавших, работу с правоохранительными органами и восстановление систем.

Несанкционированное распространение информации является серьезной угрозой для любой организации. Примеры с Facebook, Equifax и Marriott показывают, каковы могут быть последствия таких инцидентов. Однако правильные меры по обучению сотрудников, шифрованию данных, обновлению программного обеспечения и контролю доступа могут существенно снизить риски. Важно помнить, что защита данных — это постоянный процесс, требующий внимания и ресурсов.

Влиятельные части информационных систем.

Информационные системы (ИС) — это комплекс взаимосвязанных компонентов, которые собирают, обрабатывают, хранят и распространяют информацию. Эти системы играют ключевую роль в современной жизни, оказывая влияние на все сферы деятельности, от бизнеса до здравоохранения. Рассмотрим наиболее влиятельные части информационных систем и реальные примеры их применения.

1. Аппаратное обеспечение (Hardware)

Аппаратное обеспечение включает в себя физические компоненты информационных систем, такие как серверы, компьютеры, сети и другие устройства.

Пример. В 2018 году компания Amazon запустила проект Amazon Go — магазины без кассиров, где покупатели могут просто взять товары и выйти, а система автоматически списывает деньги с их счета. Это стало возможным благодаря множеству камер, датчиков и серверов, которые мгновенно обрабатывают данные о движении товаров и людях.

2. Программное обеспечение (Software)

Программное обеспечение — это набор программ и приложений, которые управляют аппаратным обеспечением и выполняют специфические задачи.

Пример. Microsoft Office, используемый миллионами людей по всему миру, включает в себя программы для обработки текстов, создания таблиц, презентаций и управления электронной почтой. Этот пакет программного обеспечения значительно повысил эффективность работы офисных сотрудников.

3. Данные (Data)

Данные являются сердцем информационных систем. Это может быть текст, цифры, изображения или любой другой вид информации, который система обрабатывает и хранит.

Пример. Система управления реляционными базами данных (РСУБД) Oracle используется крупными корпорациями для хранения и управления огромными объемами данных. Например, банки используют Oracle для хранения информации о счетах клиентов и транзакциях.

4. Сети (Networking)

Сети обеспечивают связь между различными компонентами информационной системы, позволяя им обмениваться данными и работать вместе.

Пример. Интернет — это глобальная сеть, которая связывает миллионы компьютеров по всему миру. Без интернета многие современные сервисы, такие как социальные сети, облачные хранилища и онлайн-магазины, просто не могли бы существовать.

5. Люди (People)

Люди — это пользователи и администраторы информационных систем. Они проектируют, управляют и используют системы для достижения своих целей.

Пример. В компаниях, таких как Google, тысячи инженеров, разработчиков и аналитиков работают над созданием и улучшением сервисов, таких как поисковая система Google Search, которая ежедневно помогает миллионам людей находить необходимую информацию.

6. Процессы (Processes)

Процессы включают в себя процедуры и правила, по которым данные обрабатываются и используются в информационных системах.

Пример. В медицинских учреждениях системы электронных медицинских записей (EMR) стандартизируют процесс записи, хранения и доступа к медицинским данным пациентов. Это значительно улучшает качество медицинского обслуживания и снижает вероятность ошибок.

Информационные системы состоят из нескольких влиятельных частей. аппаратного и программного обеспечения, данных, сетей, людей и процессов. Каждый из этих компонентов играет важную роль в эффективной работе системы. Реальные примеры, такие как Amazon Go, Microsoft Office, базы данных Oracle, Интернет, Google и медицинские системы EMR, демонстрируют, как информационные системы улучшают повседневную жизнь и бизнес-процессы.

Программно-технические средства несанкционированного доступа к информации

В современном мире киберугрозы становятся все более изощренными, и важно понимать, какие методы и инструменты используют злоумышленники для получения несанкционированного доступа к информации, а также как можно защититься от таких угроз.

Несанкционированный доступ к информации — это получение информации без разрешения владельца. Злоумышленники могут использовать различные программные и технические средства для этого. Такие действия могут привести к утечке конфиденциальных данных, финансовым потерям, утрате репутации и другим серьезным последствиям.

Основные виды программно-технических средств

1. Вирусы и черви

Пример. Вирус WannaCry, появившийся в 2017 году, поразил сотни тысяч компьютеров по всему миру. Он использовал уязвимость в операционной системе Windows для шифрования данных на зараженных устройствах и требовал выкуп за их разблокировку.

2. Троянские программы

Трояны маскируются под легитимное программное обеспечение, но выполняют скрытые вредоносные действия.

Пример. Троян Emotet, обнаруженный в 2014 году, изначально предназначался для кражи банковских данных. Позднее он эволюционировал в платформу для доставки других видов вредоносного ПО.

3. Шпионское ПО (Spyware)

Шпионское ПО скрытно устанавливается на компьютеры и собирает информацию о пользователе.

Пример. Программа Pegasus, разработанная израильской компанией NSO Group, использовалась для слежки за журналистами, активистами и политиками. Она может получать доступ к микрофону, камере и личным данным на мобильных устройствах.

4. Клавиатурные шпионы (Keyloggers)

Keylogger записывает каждое нажатие клавиши на клавиатуре, что позволяет злоумышленникам получить доступ к паролям и другим конфиденциальным данным.

Пример. В 2019 году был обнаружен Keylogger в программном обеспечении HP Touchpoint Analytics, которое установлено на компьютерах HP. Он записывал действия пользователей без их ведома.

5. Руткиты (Rootkits)

Руткиты скрывают наличие других вредоносных программ на устройстве, что делает их трудными для обнаружения.

Пример. Руткит Sony BMG, обнаруженный в 2005 году, устанавливался на компьютеры пользователей при

воспроизведении лицензионных аудиодисков компании Sony. Он скрывал свои действия и делал систему уязвимой для других атак.

Способы защиты от несанкционированного доступа

1. Антивирусное программное обеспечение

Использование современных антивирусных программ помогает обнаруживать и удалять вредоносные программы до того, как они смогут нанести вред.

2. Обновление программного обеспечения

Регулярное обновление операционных систем и приложений позволяет устранить уязвимости, которые могут быть использованы злоумышленниками.

Пример. Уязвимость EternalBlue, использованная вирусом WannaCry, была устранена в обновлении Windows. Однако компьютеры, не получившие это обновление, оставались уязвимыми.

3. Фаерволы (Firewalls)

Фаерволы контролируют сетевой трафик и могут блокировать подозрительные подключения.

4. Шифрование данных

Шифрование данных делает их бесполезными для злоумышленников, если они получат к ним доступ.

Пример. Протокол HTTPS обеспечивает шифрование данных, передаваемых между веб-браузером и сервером, что защищает информацию от перехвата.

5. Обучение сотрудников

Обучение сотрудников основам кибербезопасности помогает предотвратить атаки, связанные с человеческим фактором, такие как фишинг.

Хотелось бы подчеркнуть, что киберугрозы становятся все более сложными и разнообразными. Понимание того, какие программно-технические средства используются для несанкционированного доступа к информации, и знание методов защиты являются ключевыми для обеспечения безопасности данных. Примеры вирусов, троянов, шпионского ПО и других

угроз показывают, насколько серьезными могут быть последствия атак. Однако с помощью современных средств защиты и правильного подхода к безопасности можно значительно снизить риски.

Контрольные вопросы.

Контрольные вопросы по теме "Несанкционированное распространение информации и способы ее устранения"

1. Что такое несанкционированное распространение информации?
2. Приведите примеры реальных инцидентов, связанных с утечкой данных.
3. Какую роль играют ошибки сотрудников в несанкционированном распространении информации?
4. Каким образом хакеры могут получить доступ к конфиденциальным данным?
5. Какие меры могут предотвратить несанкционированное распространение информации?
6. Объясните, как шифрование данных помогает защитить информацию.
7. Почему регулярное обновление программного обеспечения важно для безопасности данных?
8. Как мониторинг и анализ сетевого трафика помогают предотвратить утечки данных?
9. В чем заключается роль контроля доступа в защите информации?
10. Что включает в себя план реагирования на инциденты утечки данных?

Контрольные вопросы по теме "Влиятельные части информационных систем"

1. Какие основные компоненты входят в состав информационной системы?

2. Объясните роль аппаратного обеспечения в информационных системах.

3. Приведите пример использования программного обеспечения в бизнесе.

4. Почему данные считаются сердцем информационных систем?

5. Как сети обеспечивают взаимодействие компонентов информационных систем?

6. Какая роль отводится людям в информационных системах?

7. Что такое процессы в контексте информационных систем?

8. Приведите пример системы, использующей реляционные базы данных для управления информацией.

9. Как Интернет влияет на функционирование информационных систем?

10. Объясните, как системы электронных медицинских записей (EMR) улучшают качество медицинского обслуживания.

Контрольные вопросы по под теме "Программно-технические средства несанкционированного доступа к информации"

1. Что такое несанкционированный доступ к информации?

2. Опишите, как вирусы и черви могут использоваться для несанкционированного доступа.

3. Приведите пример троянской программы и объясните ее действие.

4. Как шпионское ПО собирает информацию о пользователях?

5. Что такое клавиатурные шпионы (keyloggers) и как они работают?

6. Объясните, что такое руткиты и как они скрывают своё присутствие.

7. Какие меры могут предотвратить установку вредоносного ПО?

8. Почему важно регулярно обновлять программное обеспечение?

9. Как фаерволы помогают защитить информацию от несанкционированного доступа?

10. Объясните, как шифрование данных защищает их от злоумышленников.

11. Почему обучение сотрудников основам кибербезопасности является важной мерой защиты?

Эти вопросы помогут студентам оценить понимание по каждой из-под тем и их способность применять знания на практике.

Тесты по теме.

1. **Что такое несанкционированное распространение информации?**

- a) Законное использование данных
- b) Получение информации только руководителями
- c) Распространение конфиденциальной информации без разрешения владельца
- d) Обмен информацией внутри компании

Ответ. c) Распространение конфиденциальной информации без разрешения владельца

2. **Какую роль играют ошибки сотрудников в несанкционированном распространении информации?**

- a) Ошибки сотрудников не влияют на безопасность данных
- b) Ошибки сотрудников могут приводить к утечкам данных
- c) Ошибки сотрудников всегда защищают данные
- d) Ошибки сотрудников редко случаются

Ответ. b

3. **Что может предотвратить несанкционированное распространение информации?**

- a) Игнорирование обновлений программного обеспечения
- b) Регулярное обучение сотрудников основам кибербезопасности
- c) Доступ ко всем данным для всех сотрудников

- d) Использование простых паролей

Ответ. b) Регулярное обучение сотрудников основам кибербезопасности

4. **Почему важно шифрование данных?**

- a) Оно делает данные быстрее
- b) Оно делает данные менее доступными для авторизованных пользователей
- c) Оно защищает данные от несанкционированного доступа
- d) Оно делает данные более дорогостоящими

Ответ. c

5. **Что включает в себя план реагирования на инциденты утечки данных?**

- a) Уведомление пострадавших, работа с правоохранительными органами и восстановление систем
- b) Удаление всех данных
- c) Увеличение количества сотрудников
- d) Закрытие компании

Ответ. a

6. **Какие основные компоненты входят в состав информационной системы?**

- a) Только аппаратное обеспечение
- b) Аппаратное и программное обеспечение, данные, сети, люди и процессы
- c) Только программное обеспечение
- d) Только данные и сети

Ответ. b

7. **Какую роль играют люди в информационных системах?**

- a) Только используют системы
- b) Проектируют, управляют и используют системы
- c) Только проектируют системы

- d) Не играют никакой роли

Ответ. b) Проектируют, управляют и используют системы

8. **Почему данные считаются сердцем информационных систем?**

- a) Данные являются единственным компонентом ИС
- b) Без данных системы не могут выполнять свои функции
- c) Данные всегда являются публичными
- d) Данные не важны для работы ИС

Ответ. b) Без данных системы не могут выполнять свои функции

9. **Что такое процессы в контексте информационных систем?**

- a) Набор физических устройств
- b) Процедуры и правила, по которым данные обрабатываются и используются
- c) Только программное обеспечение
- d) Набор пользователей системы

Ответ. b) Процедуры и правила, по которым данные обрабатываются и используются

10**. Как Интернет влияет на функционирование информационных систем?**

- a) Затрудняет обмен данными между системами
- b) Обеспечивает глобальную связь и доступ к ресурсам
- c) Делает системы уязвимыми для вирусов
- d) Исключает необходимость в аппаратном обеспечении

Ответ. b) Обеспечивает глобальную связь и доступ к ресурсам

11. **Что такое несанкционированный доступ к информации?**

- a) Доступ к информации, разрешенный владельцем
- b) Получение информации без разрешения владельца

- c) Передача данных внутри компании
- d) Открытый доступ к публичной информации

Ответ. b) Получение информации без разрешения владельца

12. **Какую роль играют вирусы и черви в несанкционированном доступе к информации?**

- a) Они защищают данные
- b) Они обучают сотрудников
- c) Они могут использовать уязвимости для получения доступа к данным
- d) Они увеличивают производительность систем

Ответ. c) Они могут использовать уязвимости для получения доступа к данным

13. **Что делает троянская программа?**

- a) Она улучшает работу программного обеспечения
- b) Она выполняет скрытые вредоносные действия, маскируясь под легитимное ПО
- c) Она защищает систему от вирусов
- d) Она увеличивает скорость работы системы

Ответ. b) Она выполняет скрытые вредоносные действия, маскируясь под легитимное ПО

14. **Что такое клавиатурные шпионы (keyloggers)?**

- a) Программы для ускорения работы клавиатуры
- b) Программы для записи каждого нажатия клавиши
- c) Программы для изменения языка ввода
- d) Программы для очистки клавиатуры

Ответ. b) Программы для записи каждого нажатия клавиши

15. **Как фаерволы помогают защитить информацию от несанкционированного доступа?**

- a) Они блокируют обновления программного обеспечения

- b) Они контролируют сетевой трафик и блокируют подозрительные подключения
- c) Они отключают интернет-соединение
- d) Они увеличивают скорость интернета

Ответ. b) Они контролируют сетевой трафик и блокируют подозрительные подключения

3-ГЛАВА. Методы защиты и защиты информации в сети, Интернет-системе и электронной почте

§3.7. Организация защиты сети Интернет

Основы организации сетевой защиты. Способы обеспечения защиты в сетях. Основные направления защиты информации в компьютерных сетях. Слабые стороны компьютерных сетей. Методы обеспечения безопасности данных в интернет-системе-классификация способов несанкционированного доступа в интернет. Влиятельные части ваших информационных систем. Защита электронной почты.

Основы организации сетевой защиты

Этот аспект информационной безопасности стал критически важным в современном мире, где данные являются ценнейшим ресурсом. Мы рассмотрим ключевые элементы сетевой защиты, их функции и приведем примеры из реальной жизни.

1. Введение в сетевую защиту

Сетевая защита — это комплекс мер и технологий, направленных на защиту компьютерных сетей от различных угроз. Основная цель сетевой защиты — обеспечить конфиденциальность, целостность и доступность данных.

2. Основные угрозы для сетей

- Вирусы и черви. Программы, которые распространяются через сети и заражают устройства. Пример. вирус ILOVEYOU, который нанес ущерб в размере $10 миллиардов в 2000 году.
- Атаки на отказ в обслуживании (DDoS). Атаки, которые перегружают сеть или сервер, делая их недоступными для пользователей. Пример. в 2016 году атака на Dyn DNS привела к отключению крупных сайтов, таких как Twitter и Netflix.
- Фишинг. Мошенничество, при котором злоумышленники пытаются получить конфиденциальную информацию, выдавая себя за доверенных лиц.

Пример. фишинговая атака на компанию Target в 2013 году, в результате которой было украдено 40 миллионов номеров кредитных карт.

Рисунок 4.1. Защита сети интернет

3. Основные компоненты сетевой защиты

1. Брандмауэры (Firewall)

Брандмауэры — это устройства или программы, которые контролируют и фильтруют сетевой трафик между внутренней сетью и внешними сетями. Они могут блокировать неавторизованный доступ и предотвращать атаки.

Пример. В компании использовали брандмауэр, чтобы блокировать доступ к подозрительным IP-адресам, что помогло предотвратить проникновение вредоносного ПО.

2. Системы обнаружения и предотвращения вторжений (IDS/IPS)

IDS/IPS анализируют сетевой трафик в реальном времени для обнаружения подозрительной активности. IDS уведомляют администратора о возможной атаке, в то время как IPS могут автоматически блокировать вредоносный трафик.

Пример. В 2019 году компания Cisco обнаружила с помощью IDS попытку взлома своей сети и смогла оперативно предотвратить утечку данных.

3. Виртуальные частные сети (VPN)

VPN создают защищенное соединение через интернет, шифруя данные и обеспечивая конфиденциальность. Они часто используются для безопасного доступа сотрудников к корпоративной сети из удаленных мест.

Пример. Сотрудники компании использовали VPN для удаленной работы, что помогло защитить конфиденциальную информацию от перехвата.

4. Антивирусное программное обеспечение

Антивирусные программы сканируют устройства на наличие вредоносного ПО и удаляют его. Они регулярно обновляются для защиты от новых угроз.

Пример. После обнаружения трояна на компьютере сотрудника, антивирусная программа McAfee помогла удалить вредоносное ПО и предотвратить его распространение по сети.

4. Лучшие практики по обеспечению сетевой безопасности

1. Регулярное обновление ПО. Обновления часто содержат патчи для уязвимостей, которые могут быть использованы злоумышленниками.

Пример. Компания Microsoft ежемесячно выпускает обновления безопасности, известные как "Patch Tuesday", что помогает защищать пользователей от новых угроз.

2. Обучение сотрудников. Сотрудники должны знать основные правила безопасности, такие как не открывать подозрительные письма и не устанавливать неизвестные программы.

Пример. В 2021 году компания Google провела обучение по кибербезопасности для своих сотрудников, что снизило количество фишинговых атак на 50%.

3. Использование сильных паролей и многофакторной аутентификации (MFA). Сильные пароли и MFA делают учетные записи более защищенными от взлома.

Пример. Внедрение многофакторной аутентификации в банке помогло предотвратить несанкционированный доступ к счетам клиентов.

Сетевая защита — это многослойный процесс, требующий комплексного подхода и постоянного внимания. Использование брандмауэров, IDS/IPS, VPN и антивирусного ПО, а также обучение сотрудников и регулярное обновление систем помогут обеспечить безопасность сети и защитить важные данные.

Способы обеспечения защиты в сетях.

На сегодняшний день защита сетей является ключевым аспектом для компаний и частных лиц, ведь киберугрозы становятся всё более изощрёнными. Мы обсудим основные методы защиты, их применение и приведем реальные примеры.

1. Введение в защиту сетей

Защита сетей включает в себя использование различных технологий и практик для предотвращения несанкционированного доступа, утечек данных и других киберугроз. Основная цель — обеспечить безопасность информации, целостность и доступность систем.

2. Основные способы защиты сетей

1. Брандмауэры (Firewall)

Брандмауэры создают барьер между вашей внутренней сетью и внешними сетями, контролируя входящий и исходящий трафик. Они могут быть аппаратными или программными и настроены на блокировку подозрительных или неавторизованных соединений.

Пример. В 2020 году компания Equifax, столкнувшись с утечкой данных, усилила свою защиту с помощью новейших брандмауэров.

Это помогло предотвратить дальнейшие атаки и защищать личную информацию миллионов клиентов.

2. Системы обнаружения и предотвращения вторжений (IDS/IPS)

IDS (системы обнаружения вторжений) и IPS (системы предотвращения вторжений) анализируют сетевой трафик для выявления подозрительной активности. IDS уведомляют администратора о потенциальных угрозах, а IPS могут автоматически блокировать вредоносные действия.

Пример. В 2019 году компания Cisco использовала систему IPS для защиты своих сетей и предотвратила масштабную атаку на свои серверы, выявив и блокировав вредоносный трафик в реальном времени.

3. Виртуальные частные сети (VPN)

VPN создают защищённое соединение между устройствами через интернет, шифруя данные. Это позволяет сотрудникам безопасно подключаться к корпоративной сети из любой точки мира.

Пример. в условиях пандемии COVID-19 многие компании, включая Microsoft, перешли на удалённую работу. Использование VPN помогло защитить конфиденциальные данные и обеспечило безопасный доступ сотрудников к корпоративным ресурсам.

4. Антивирусное и антишпионское программное обеспечение

Антивирусные программы сканируют устройства на наличие вредоносного ПО и удаляют его. Антишпионское ПО защищает от программ-шпионов, которые собирают информацию без ведома пользователя.

Пример. В 2017 году компания Sony использовала обновленное антивирусное ПО после крупной атаки на их сеть. Это помогло предотвратить повторные инциденты и защитить важные данные компании.

5. Многофакторная аутентификация (MFA)

MFA требует от пользователей предоставления нескольких форм идентификации перед доступом к системе. Обычно это комбинация пароля и временного кода, отправленного на мобильное устройство.

Пример. Банк Америки внедрил многофакторную аутентификацию для всех онлайн-транзакций, что значительно уменьшило количество мошеннических операций и повысило доверие клиентов к системе онлайн-банкинга.

3. Дополнительные методы защиты

1. Шифрование данных

Шифрование преобразует данные в код, который можно прочитать только с помощью ключа дешифрования. Это защищает данные даже в случае их перехвата.

Пример. WhatsApp использует сквозное шифрование для всех сообщений, что обеспечивает безопасность личной переписки пользователей даже в случае, если сообщения будут перехвачены.

2. Сегментация сети

Сегментация сети разделяет сеть на несколько сегментов, ограничивая распространение атаки. Это помогает минимизировать ущерб и упрощает управление безопасностью.

Пример. В 2016 году компания Target внедрила сегментацию сети после утечки данных, что помогло предотвратить повторение инцидентов и обеспечило дополнительный уровень защиты.

3. Политики безопасности и обучение сотрудников

Создание и внедрение политик безопасности, а также регулярное обучение сотрудников помогает уменьшить человеческий фактор в киберугрозах. Обучение включает в себя распознавание фишинговых атак, безопасное использование паролей и т.д.

Пример. В 2021 году Google провела обширную программу обучения сотрудников по кибербезопасности, что снизило количество успешных фишинговых атак на компанию.

Эффективная защита сети требует комплексного подхода и использования различных методов. Брандмауэры, IDS/IPS, VPN, антивирусное ПО, MFA, шифрование, сегментация сети и обучение сотрудников — все эти меры способствуют созданию надежной системы безопасности. Постоянное совершенствование этих мер и адаптация к новым угрозам являются ключевыми для обеспечения устойчивости и защиты данных.

Основные направления защиты информации в компьютерных сетях.

Угрозы кибербезопасности растут с каждым годом, и успешная защита данных требует комплексного подхода. В этой лекции мы рассмотрим основные направления защиты информации в компьютерных сетях, подкрепив их реальными примерами и фактами.

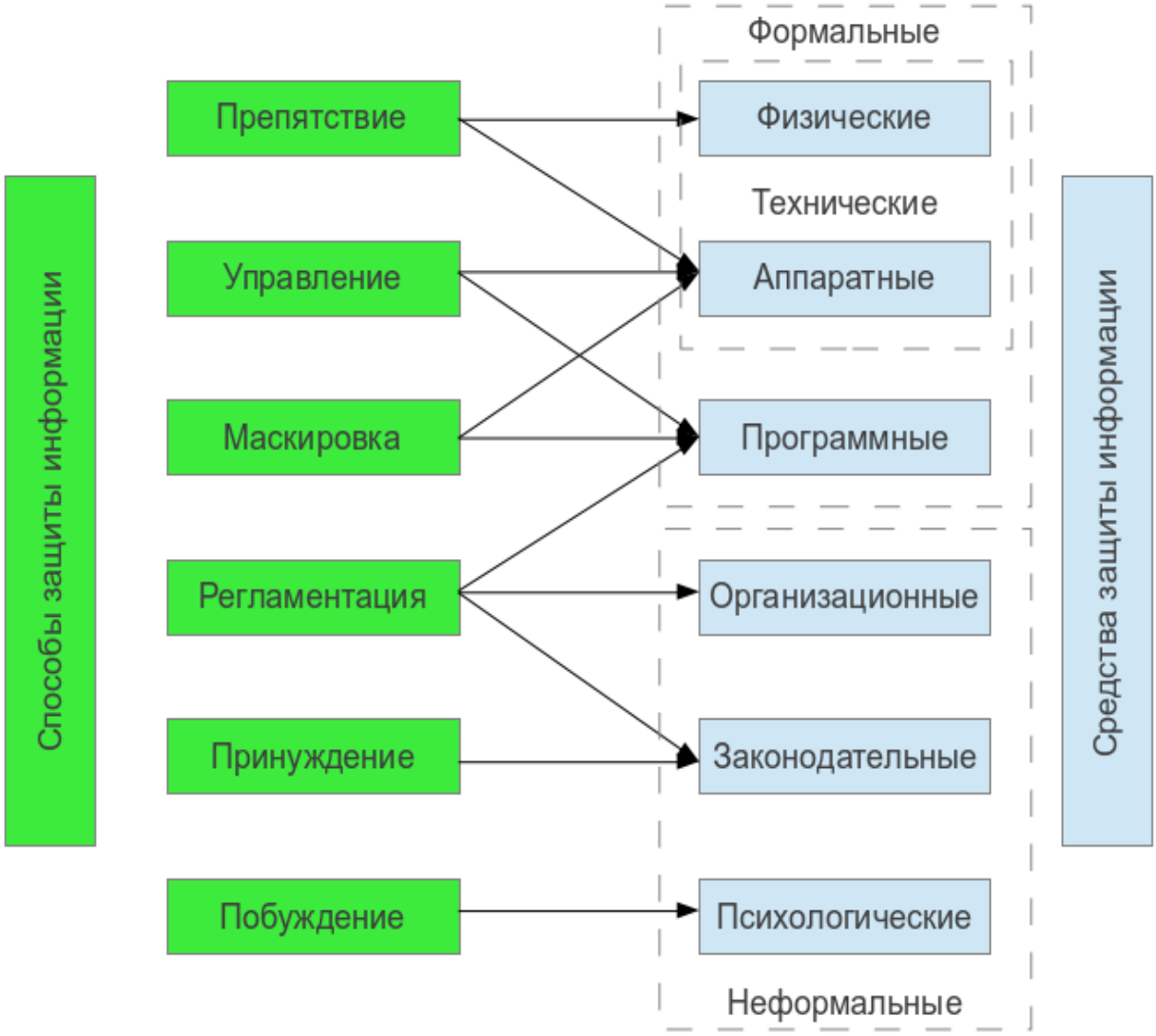

Рисунок 5.2. Средства защиты информации

Методы защиты информации

1. Аутентификация и управление доступом

Аутентификация

Аутентификация — это процесс проверки подлинности пользователя или устройства. Целью является подтверждение того, что пользователь действительно тот, за кого себя выдает.

Пример. Использование двухфакторной аутентификации (2FA) в Google. Когда вы входите в свой аккаунт Google, вам нужно ввести не только пароль, но и код, отправленный на ваш телефон.

Управление доступом

Управление доступом включает в себя разрешение или ограничение прав пользователей на доступ к ресурсам сети. Это помогает минимизировать риски, связанные с несанкционированным доступом.

Пример. В корпоративных сетях часто используется система ролей (RBAC — Role-Based Access Control), где права доступа распределяются в зависимости от должности сотрудника.

2. Шифрование данных

Шифрование — это процесс преобразования информации в код, который невозможно прочитать без специального ключа. Шифрование защищает данные как при передаче по сети, так и при хранении.

Пример. Протокол HTTPS обеспечивает шифрование данных между веб-браузером и сервером, что защищает информацию от перехвата злоумышленниками.

3. Защита от вредоносного ПО

Защита от вредоносного ПО (вирусов, троянов, червей) включает в себя использование антивирусного программного обеспечения и регулярное обновление систем для устранения уязвимостей.

Пример. В 2017 году вирус WannaCry поразил множество компьютеров по всему миру, шифруя данные и требуя выкуп. Компании, которые вовремя обновили свои системы безопасности, избежали этой атаки.

4. Межсетевые экраны (фаерволы)

Межсетевые экраны контролируют входящий и исходящий трафик на основе заранее определенных правил безопасности. Они помогают предотвратить несанкционированный доступ и атаки на сеть.

Пример. Использование корпоративного фаервола для защиты локальной сети компании от внешних угроз и ограничение доступа к определенным ресурсам из внешнего интернета.

5. Обнаружение и предотвращение вторжений (IDS/IPS)

Системы обнаружения (IDS) и предотвращения (IPS) вторжений мониторят сетевой трафик и могут автоматически блокировать подозрительную активность.

Пример. Система Snort — один из популярных инструментов IDS, используемый для анализа сетевого трафика и выявления подозрительных действий на основе сигнатур.

6. Резервное копирование данных

Регулярное резервное копирование данных позволяет восстанавливать информацию в случае утраты или повреждения. Это критически важно для защиты от атак, таких как шифровальщики.

Пример. Многие компании используют облачные сервисы для автоматического резервного копирования данных, что позволяет быстро восстановить информацию после кибератаки.

7. Обучение и осведомленность пользователей

Обучение пользователей основам кибербезопасности и регулярное проведение тренингов помогает снизить риски, связанные с человеческим фактором.

Пример. Корпоративные тренинги по фишингу, где сотрудники учатся распознавать мошеннические письма и не раскрывать конфиденциальную информацию.

Комплексная защита информации в компьютерных сетях включает в себя множество направлений. от аутентификации и шифрования до использования фаерволов и IDS/IPS систем. Важно постоянно обновлять и совершенствовать меры безопасности, чтобы противостоять новым угрозам. Только так можно обеспечить надежную защиту данных и инфраструктуры от кибератак.

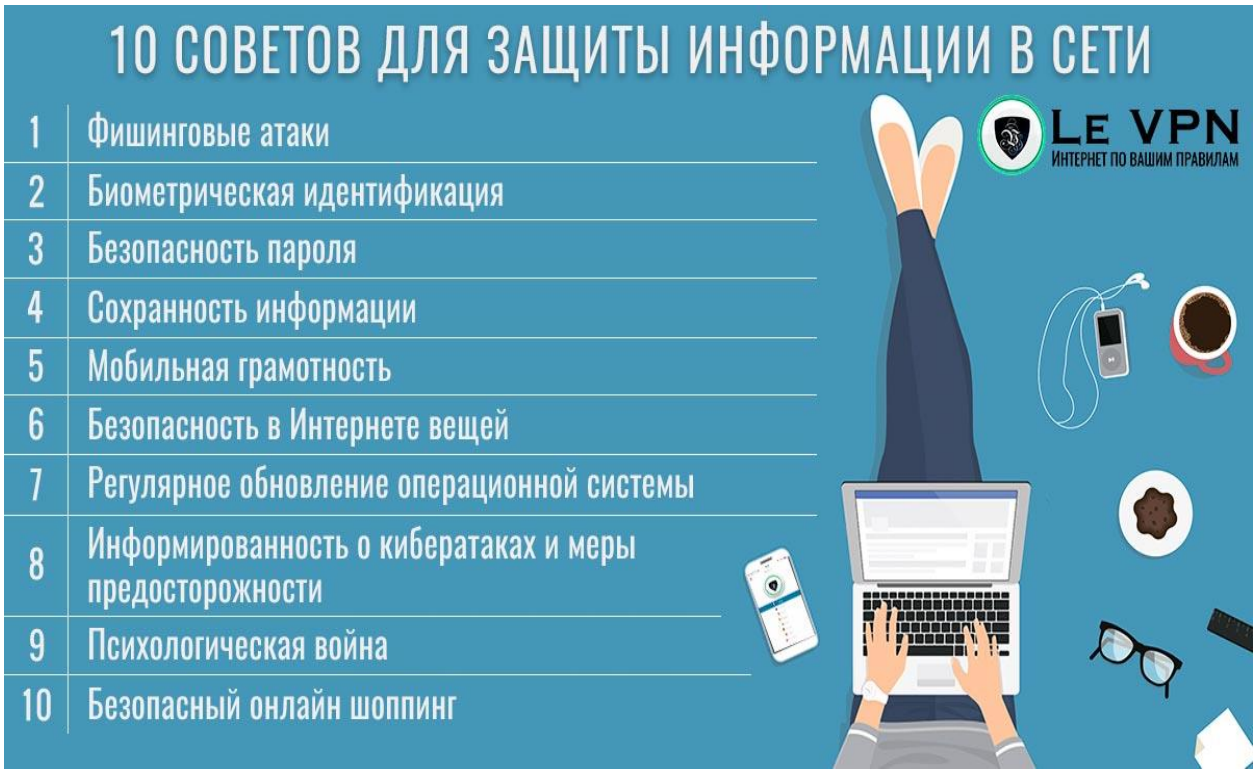

Рисунок 6.3. Советы для защиты информации в сети

Слабые стороны компьютерных сетей.

Современные компьютерные сети представляют собой сложные системы, обеспечивающие взаимодействие между различными устройствами и пользователями. Несмотря на все усилия по защите, сети остаются уязвимыми перед множеством угроз. В этой лекции мы рассмотрим слабые стороны компьютерных сетей, иллюстрируя их реальными примерами и фактами.

1. Уязвимости программного обеспечения

Уязвимости в операционных системах и приложениях

Программное обеспечение содержит ошибки и уязвимости, которые могут быть использованы злоумышленниками для атак.

Пример. Уязвимость EternalBlue в операционных системах Windows позволила вирусу WannaCry в 2017 году поразить тысячи компьютеров по всему миру. Уязвимость позволяла вредоносному ПО распространяться без участия пользователя, шифруя данные и требуя выкуп.

2. Человеческий фактор

Ошибки пользователей и сотрудников

Человеческий фактор остается одной из самых слабых сторон безопасности компьютерных сетей. Пользователи могут совершать ошибки, которые открывают двери для атак.

Пример. В 2016 году в результате фишинговой атаки был скомпрометирован аккаунт Джона Подесты, главы предвыборного штаба Хиллари Клинтон. Подеста ошибочно предоставил свои учетные данные, что привело к утечке большого объема конфиденциальной информации.

3. Недостаточное шифрование данных

Неиспользование или неправильное использование шифрования

Шифрование данных критично для защиты информации при передаче по сети. Однако, если шифрование не используется или используется неправильно, данные становятся уязвимыми.

Пример. В 2013 году компания Target стала жертвой кибератаки, в результате которой было похищено 40 миллионов кредитных карт. Злоумышленники получили доступ к данным, так как шифрование было недостаточно эффективно использовано в точках продаж.

4. Сетевые атаки

DDoS-атаки (Distributed Denial of Service)

DDoS-атаки направлены на перегрузку сетевых ресурсов, делая их недоступными для пользователей.

Пример. В 2016 году произошла масштабная DDoS-атака на провайдера Dyn, что привело к недоступности таких популярных сервисов, как Twitter, Reddit и Netflix. Атака использовала ботнет из IoT-устройств, взламывая их и направляя трафик на серверы Dyn.

5. Недостатки конфигурации сетевого оборудования

Неправильная настройка роутеров и других устройств

Ошибки в настройке сетевого оборудования могут стать причиной уязвимостей.

Пример. В 2018 году было обнаружено, что многие маршрутизаторы MikroTik были неправильно настроены, что позволило злоумышленникам использовать их для майнинга

криптовалюты. Хакеры эксплуатировали неправильные настройки, чтобы внедрить вредоносный код на устройства.

6. Отсутствие обновлений и патчей

Невыполнение обновлений безопасности

Регулярные обновления и патчи необходимы для устранения известных уязвимостей. Пренебрежение ими увеличивает риск атак.

Пример. В 2017 году атака NotPetya поразила многие компании по всему миру, в том числе Maersk, одна из крупнейших судоходных компаний. Вирус использовал уязвимость, для которой уже был выпущен патч, но системы Maersk не были своевременно обновлены.

7. Недостаток мониторинга и обнаружения угроз

Отсутствие систем IDS/IPS

Многие сети не имеют достаточно развитых систем мониторинга и обнаружения угроз, что позволяет атакам оставаться незамеченными. Пример. В 2018 году сеть отелей Marriott подверглась утечке данных, затронувшей 500 миллионов клиентов. Атака оставалась незамеченной в течение четырех лет, что указывает на недостаток эффективных систем мониторинга. Компьютерные сети обладают множеством слабых сторон, от уязвимостей в программном обеспечении до человеческого фактора и недостатков в конфигурации оборудования. Для эффективной защиты необходимо применять комплексный подход, включая регулярное обновление систем, обучение пользователей и использование современных технологий мониторинга и обнаружения угроз. Только так можно минимизировать риски и обеспечить надежную защиту информации в сетях.

Методы обеспечения безопасности данных в интернет-системе-классификация способов несанкционированного доступа в интернет.

С ростом числа пользователей и объемов данных увеличивается и количество угроз. В этой лекции мы рассмотрим методы

обеспечения безопасности данных в интернет-системах и классификацию способов несанкционированного доступа, подкрепив их реальными примерами.

Методы обеспечения безопасности данных в интернет-системе

1. Аутентификация и управление доступом

Аутентификация — это процесс проверки подлинности пользователя или устройства. Основные методы аутентификации включают использование паролей, биометрических данных и двухфакторную аутентификацию (2FA).

Пример. Вход в аккаунт Google с использованием 2FA, где помимо пароля требуется ввести код, отправленный на телефон.

Управление доступом — это ограничение прав пользователей на доступ к ресурсам сети. Обычно используется система ролей (RBAC — Role-Based Access Control).

Пример. В крупной корпорации доступ к конфиденциальным данным имеет только узкий круг сотрудников в зависимости от их должностных обязанностей.

2. Шифрование данных

Шифрование — это процесс преобразования информации в код, который невозможно прочитать без специального ключа. Шифрование применяется для защиты данных при передаче и хранении.

Пример. Протокол HTTPS, используемый для безопасного соединения между браузером и веб-сервером, предотвращает перехват данных злоумышленниками.

3. Межсетевые экраны (фаерволы)

Межсетевые экраны контролируют входящий и исходящий трафик на основе заранее определенных правил безопасности, предотвращая несанкционированный доступ.

Пример. Использование корпоративного фаервола для защиты внутренней сети компании от внешних угроз и ограничения доступа к определенным ресурсам.

4. Обнаружение и предотвращение вторжений (IDS/IPS)

Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) анализируют сетевой трафик и выявляют подозрительную активность.

Пример. Snort — популярная IDS-система, используемая для мониторинга сетевого трафика и выявления атак на основе сигнатур.

5. Регулярное обновление и патчинг

Обновление программного обеспечения и применение патчей устраняют известные уязвимости, предотвращая эксплуатацию уязвимостей злоумышленниками.

Пример. После обнаружения уязвимости в Windows, Microsoft выпускает патчи, которые пользователи должны установить для защиты своих систем.

6. Резервное копирование данных

Резервное копирование позволяет восстанавливать данные в случае их утраты или повреждения.

Пример. Использование облачных сервисов для автоматического резервного копирования данных, что помогает восстановить информацию после кибератаки.

7. Обучение и осведомленность пользователей

Обучение пользователей основам кибербезопасности снижает риски, связанные с человеческим фактором.

Пример. Проведение корпоративных тренингов по фишингу, где сотрудники учатся распознавать мошеннические письма и не раскрывать конфиденциальную информацию.

Классификация способов несанкционированного доступа в интернет

1. Фишинг

Фишинг — это метод социальной инженерии, при котором злоумышленники пытаются обманным путем получить конфиденциальные данные, такие как пароли и номера кредитных карт.

Пример. В 2016 году фишинговая атака на главу предвыборного штаба Хиллари Клинтон Джона Подесту привела к утечке большого объема конфиденциальной информации.

2. SQL-инъекции

SQL-инъекции — это метод, при котором злоумышленники вставляют вредоносный код в запросы SQL, чтобы получить доступ к данным базы данных.

Пример. В 2011 году хакерская группа LulzSec использовала SQL-инъекции для взлома сайтов, таких как Sony Pictures, что привело к утечке данных миллионов пользователей.

3. Атаки типа "отказ в обслуживании" (DDoS)

DDoS-атаки направлены на перегрузку сетевых ресурсов, делая их недоступными для пользователей.

Пример. В 2016 году масштабная DDoS-атака на провайдера Dyn привела к недоступности таких популярных сервисов, как Twitter и Netflix.

4. Малварь (вредоносное ПО)

Малварь — это вредоносное программное обеспечение, которое может использоваться для кражи данных, шпионажа или нанесения вреда системе.

Пример. Вирус WannaCry в 2017 году шифровал данные на компьютерах и требовал выкуп за их расшифровку.

5. Атаки "человек посередине" (MitM)

MitM-атаки происходят, когда злоумышленник перехватывает и изменяет коммуникации между двумя сторонами без их ведома.

Пример. MitM-атака на Wi-Fi-сети, где злоумышленник перехватывает данные, передаваемые между пользователем и точкой доступа.

6. Кража учетных данных

Кража учетных данных включает в себя получение доступа к учетным записям пользователей через взлом или фишинг.

Пример. В 2012 году утечка данных LinkedIn привела к краже миллионов учетных записей пользователей.

7. Эксплуатация уязвимостей нулевого дня

Уязвимости нулевого дня — это уязвимости, которые неизвестны разработчикам ПО и не имеют патчей.

Пример. Атака Stuxnet, использующая уязвимости нулевого дня для поражения иранских ядерных объектов в 2010 году.

Защита данных в интернет-системах требует комплексного подхода, включающего использование различных методов безопасности и постоянное обновление систем. Классификация способов несанкционированного доступа позволяет лучше понимать угрозы и разрабатывать эффективные меры защиты. Только так можно обеспечить надежную защиту информации в современном цифровом мире.

Влиятельные части ваших информационных систем.

Информационные системы являются важнейшей частью любой современной организации. Они включают в себя оборудование, программное обеспечение, сети, данные и процессы, которые вместе обеспечивают управление и обработку информации. В этой лекции мы рассмотрим наиболее влиятельные части информационных систем, которые играют ключевую роль в их функционировании, и приведем реальные примеры, иллюстрирующие их значимость.

1. Аппаратное обеспечение

Сервера и хранилища данных

Сервера выполняют центральные вычислительные задачи и управляют ресурсами сети. Хранилища данных обеспечивают сохранность больших объемов информации.

Пример. В 2018 году компания Facebook столкнулась с перебоями в работе из-за отказа одного из своих дата-центров. Это привело к временной недоступности платформы для миллионов пользователей по всему миру, подчеркивая важность надежного оборудования.

Рабочие станции и периферийные устройства

Рабочие станции и периферийные устройства (принтеры, сканеры) необходимы для выполнения повседневных задач сотрудников.

Пример. В 2019 году международная авиакомпания British Airways столкнулась с массовыми задержками рейсов из-за сбоя в системе регистрации на рабочих станциях в аэропортах. Это показало, как важна надежность рабочих станций для непрерывной работы бизнеса.

2. Программное обеспечение

Операционные системы

Операционные системы (ОС) управляют аппаратным обеспечением и обеспечивают платформу для выполнения приложений.

Пример. В 2017 году вирус WannaCry поразил компьютеры, работающие на Windows, используя уязвимости в ОС. Это привело к масштабным сбоям в работе больниц, компаний и государственных учреждений, демонстрируя критическую важность обновлений ОС.

Прикладное программное обеспечение

Прикладное программное обеспечение включает в себя приложения, используемые для выполнения специфических задач.

Пример. В 2016 году сбой в ПО для торговли акциями компании Knight Capital Group привел к неправильным сделкам и убыткам в размере 440 миллионов долларов всего за 45 минут. Это происшествие показало, как важно тестирование и поддержка приложений в реальном времени.

3. Сетевые компоненты

Маршрутизаторы и коммутаторы

Маршрутизаторы и коммутаторы управляют потоком данных в сети, обеспечивая соединение между устройствами.

Пример. В 2016 году атака на маршрутизаторы DNS-провайдера Dyn привела к масштабным перебоям в работе таких сайтов, как Twitter, Reddit и Netflix. Это инцидент подчеркнул критическую роль сетевых компонентов в доступности интернет-ресурсов.

Беспроводные сети и точки доступа

Беспроводные сети и точки доступа обеспечивают соединение мобильных устройств с интернетом и локальной сетью.

Пример. В 2018 году обнаружение уязвимости в протоколе WPA2 (KRACK) показало, что беспроводные сети могут быть уязвимыми к атакам, и потребовало от всех производителей срочных обновлений для устранения угрозы.

3. Данные и базы данных

Хранение данных

Базы данных и системы управления базами данных (СУБД) обеспечивают структурированное хранение и доступ к данным.

Пример. В 2012 году утечка данных LinkedIn, в результате которой были скомпрометированы пароли миллионов пользователей, показала, насколько важно защищать данные и использовать современные методы шифрования и хэширования.

Аналитика и обработка данных

Аналитические инструменты и платформы для обработки данных позволяют извлекать ценные инсайты из больших объемов информации.

Пример. Использование аналитической платформы Hadoop в Walmart для анализа покупательского поведения клиентов помогло компании оптимизировать ассортимент товаров и увеличить продажи.

5. Политики безопасности и управление рисками

Политики безопасности

Политики безопасности определяют правила и процедуры для защиты информационных систем от угроз.

Пример. Внедрение политики минимизации прав доступа в компании Google (Least Privilege Access) помогло значительно снизить риски утечек данных, обеспечив доступ к информации только тем сотрудникам, которым это необходимо для выполнения их обязанностей.

Управление рисками

Управление рисками включает в себя оценку и уменьшение потенциальных угроз для информационных систем.

Пример. После атаки на Target в 2013 году, компания внедрила более строгие меры управления рисками, включая регулярные аудиты безопасности и тестирование на проникновение, что помогло предотвратить повторные инциденты.

6. Пользователи и обучение

Обучение пользователей

Обучение сотрудников основам кибербезопасности помогает снизить риски, связанные с человеческим фактором.

Пример. В 2018 году компания Wombat Security провела тренинг по фишингу для сотрудников. Результаты показали, что обучение помогло снизить количество случаев успешных фишинговых атак на 40%.

Управление пользователями

Управление пользователями включает в себя создание, удаление и контроль учетных записей и прав доступа.

Пример. В крупной компании с десятками тысяч сотрудников внедрение системы единого входа (Single Sign-On) упростило управление учетными записями и повысило уровень безопасности доступа к корпоративным ресурсам.

Влиятельные части информационных систем включают в себя аппаратное обеспечение, программное обеспечение, сетевые компоненты, данные, политики безопасности и пользователей. Все эти элементы играют ключевую роль в обеспечении надежности и безопасности информационной системы. Понимание их значимости и грамотное управление ими помогают минимизировать риски и обеспечить бесперебойную работу бизнеса.

Защита электронной почты.

Электронная почта (e-mail) — один из самых распространенных способов общения в современном мире, как в личной, так и в деловой сфере. Однако, именно из-за своей популярности электронная почта часто становится мишенью для кибератак. В этой лекции мы подробно рассмотрим различные

методы защиты электронной почты, подкрепив их реальными примерами.

1. Шифрование электронной почты

Симметричное и асимметричное шифрование

Шифрование помогает защитить содержимое электронной почты от несанкционированного доступа. Существуют два основных типа шифрования. симметричное (один ключ используется для шифрования и расшифрования) и асимметричное (используются два ключа — публичный и приватный).

Пример. Программа PGP (Pretty Good Privacy) использует асимметричное шифрование для защиты сообщений. При отправке зашифрованного письма получатель может расшифровать его только с помощью своего приватного ключа, который никому не известен.

2. Антифишинг и антиспам технологии

Обнаружение фишинговых писем

Фишинговые атаки направлены на получение конфиденциальной информации путем обмана пользователей. Современные анти фишинговые технологии анализируют содержимое писем и их отправителей для выявления подозрительных сообщений.

Пример. В 2016 году через фишинговое письмо был взломан аккаунт Джона Подесты, главы предвыборного штаба Хиллари Клинтон. В письме содержалась ссылка на поддельную страницу Google, где Подеста ввел свои учетные данные. Современные антифишинговые фильтры могли бы заблокировать такое письмо.

3. Двухфакторная аутентификация (2FA)

Защита учетной записи дополнительным фактором

Двухфакторная аутентификация требует от пользователя ввести не только пароль, но и второй фактор аутентификации (например, код, отправленный на телефон).

Пример. Google предлагает двухфакторную аутентификацию для своих пользователей. Даже если злоумышленник узнает ваш

пароль, без доступа к вашему телефону он не сможет войти в аккаунт.

4. Обновления и патчи безопасности

Регулярное обновление программного обеспечения

Важность своевременного обновления программного обеспечения невозможно переоценить. Устаревшие версии могут содержать уязвимости, которые могут быть использованы злоумышленниками.

Пример. В 2018 году Microsoft обнаружила уязвимость в своем почтовом клиенте Outlook, которая позволяла злоумышленникам удаленно выполнять код. Важность установки патчей безопасности стала очевидной, когда эта уязвимость была устранена в следующем обновлении.

5. Обучение пользователей

Повышение осведомленности о киберугрозах

Обучение пользователей основам кибербезопасности помогает предотвратить многие атаки. Пользователи должны быть осведомлены о рисках, связанных с открытием подозрительных писем и вложений.

Пример. В 2019 году компания JPMorgan Chase провела кампанию по обучению своих сотрудников распознаванию фишинговых писем. В результате удалось значительно снизить число успешных фишинговых атак на корпоративную почту.

6. Использование защитных инструментов

Антивирусные программы и фаерволы

Антивирусные программы и фаерволы защищают электронную почту от вредоносного ПО, которое может быть вложено в письма или ссылки.

Пример. В 2020 году антивирусная программа Symantec помогла предотвратить распространение вредоносного ПО Emotet через вложения в электронных письмах. Emotet был обнаружен и заблокирован еще до того, как пользователи успели открыть зараженные файлы.

7. Политики управления доступом

Ограничение прав доступа

Политики управления доступом помогают ограничить круг лиц, которые могут получить доступ к конфиденциальной информации, отправляемой по электронной почте.

Пример. В 2021 году компания Apple внедрила строгие политики управления доступом для своей внутренней почтовой системы. Это позволило минимизировать риски утечки конфиденциальной информации, ограничив доступ к ней только авторизованным пользователям.

8. Резервное копирование

Восстановление данных при утрате

Регулярное резервное копирование писем и данных помогает восстановить информацию в случае утраты или кибератаки.

Пример. В 2017 году компания Sony Pictures пострадала от кибератаки, в результате которой были утрачены значительные объемы данных. Однако, благодаря регулярным резервным копиям, компания смогла восстановить важную информацию и минимизировать последствия атаки.

Защита электронной почты требует комплексного подхода, включающего использование шифрования, антифишинговых и антиспам технологий, двухфакторной аутентификации, регулярных обновлений, обучения пользователей, защитных инструментов, политик управления доступом и резервного копирования. Только при соблюдении всех этих мер можно обеспечить надежную защиту электронной почты от различных угроз и сохранить конфиденциальность и целостность информации.

Контрольные вопросы.

1. Что включает в себя понятие сетевой защиты?
2. Какие основные компоненты входят в состав системы сетевой защиты?
3. Какова роль межсетевого экрана (файрвола) в сетевой защите?

4. Назовите основные способы защиты информации в компьютерных сетях.
5. В чем заключается принцип работы системы обнаружения вторжений (IDS)?
6. Какова роль шифрования в защите данных в сетях?
7. Какие существуют направления защиты информации в сетях?
8. Как защита данных различается на уровне передачи и уровне хранения?
9. Какую роль играет аутентификация пользователей в защите сетей?
10. Какие основные уязвимости существуют в компьютерных сетях?
11. Как атаки типа DDoS могут повлиять на работу сети?
12. В чем заключаются угрозы безопасности, связанные с социальным инжинирингом?
13. Какие методы используются для обеспечения безопасности данных в интернет-системах?
14. Какова роль SSL/TLS в защите данных при их передаче в интернете?
15. Какие меры могут быть предприняты для защиты веб-приложений от атак типа XSS и SQL-инъекций?
16. Какие основные способы несанкционированного доступа в интернет существуют?
17. В чем заключается угроза фишинга и как с ней бороться?
18. Как работает атака "человек посередине" (MITM) и как ей противодействовать?
19. Какие компоненты информационной системы являются наиболее критичными для обеспечения её безопасности?
20. Как может быть использована сегментация сети для повышения безопасности?
21. В чем важность резервного копирования данных для обеспечения устойчивости информационной системы?
22. Какие меры можно предпринять для защиты электронной почты от взлома?

23. Как работает шифрование электронной почты и какие существуют его виды?
24. Какие основные угрозы безопасности связаны с электронной почтой и как им противостоять?

Тесты для закрепления темы.

1. **Что включает в себя понятие сетевой защиты?**

a) Только использование антивирусов

b) Использование межсетевых экранов, антивирусов, систем обнаружения вторжений

c) Только настройку сетевых маршрутизаторов

-) Только шифрование данных

Ответ. b) Использование межсетевых экранов, антивирусов, систем обнаружения вторжений

2. **В чем заключается принцип работы системы обнаружения вторжений (IDS)?**

- **a)** Предотвращение всех входящих соединений
- b) Мониторинг сетевой активности и оповещение о подозрительных действиях
- c) Шифрование всех передаваемых данных
- d) Удаление вредоносного ПО

Ответ. b) Мониторинг сетевой активности и оповещение о подозрительных действиях

3. **Какие существуют направления защиты информации в сетях?**

- a) Физическая защита, шифрование, резервное копирование
- b) Только физическая защита и шифрование
- c) Только антивирусное ПО и фаерволы
- d) Только резервное копирование данных

Ответ. a) Физическая защита, шифрование, резервное копирование

4. **Как атаки типа DDoS могут повлиять на работу сети?**

- a) Увеличивают скорость передачи данных

- b) Нарушают доступность сетевых ресурсов
- c) Повышают уровень безопасности сети
- d) Шифруют передаваемые данные

Ответ. b) Нарушают доступность сетевых ресурсов

5. **Какова роль SSL/TLS в защите данных при их передаче в интернете?**

- a) Снижение затрат на оборудование
- b) Ускорение передачи данных
- c) Шифрование данных для защиты от перехвата
- d) Удаление вредоносного ПО

Ответ. c) Шифрование данных для защиты от перехвата

6. **В чем заключается угроза фишинга и как с ней бороться?**

- a) Угроза отказа в обслуживании; использовать файрволы
- b) Угроза перехвата данных; использовать шифрование
- c) Угроза кражи учетных данных через поддельные сайты; повышать осведомленность пользователей
- d) Угроза изменения данных; использовать резервное копирование

Ответ. c) Угроза кражи учетных данных через поддельные сайты; повышать осведомленность пользователей

7. **Какие компоненты информационной системы являются наиболее критичными для обеспечения её безопасности?**

- a) Маршрутизаторы и свичи
- b) Пользовательские рабочие станции
- c) Сетевые кабели
- d) Серверы и базы данных

Ответ. d) Серверы и базы данных

8. **Какие меры можно предпринять для защиты электронной почты от взлома?**

- a) Использовать только один пароль для всех аккаунтов
- b) Регулярно менять пароли и использовать двухфакторную аутентификацию
- c) Никогда не проверять почту с мобильных устройств

- d) Не использовать антивирусные программы

Ответ. b) Регулярно менять пароли и использовать двухфакторную аутентификацию

9. **Какая из следующих технологий используется для создания защищенного соединения между двумя сетями через интернет?**

- a) IDS
- b) VPN
- c) NAT
- d) DMZ

Ответ. b) VPN

10. **Что такое межсетевой экран (файрвол)?**

- a) Устройство для ускорения интернет-соединения
- b) Система для фильтрации входящего и исходящего трафика на основе заданных правил безопасности
- c) Программа для резервного копирования данных
- d) Программа для управления паролями

Ответ. b) Система для фильтрации входящего и исходящего трафика на основе заданных правил безопасности

11. **Какой метод используется для обеспечения целостности данных?**

- a) Антивирусное ПО
- b) Файрвол
- c) Хеширование
- d) VPN

Ответ. c) Хеширование

12. **Какое из следующих является примером социальной инженерии?**

- a) Брутфорс атака на пароли
- b) Использование шпионского ПО для кражи данных
- c) Обман пользователей с целью получения конфиденциальной информации
- d) Сканирование портов для обнаружения уязвимостей

Ответ. c) Обман пользователей с целью получения конфиденциальной информации

13. **Что из перечисленного является примером многофакторной аутентификации?**

- a) Использование пароля и ответа на секретный вопрос
- b) Использование пароля и одноразового кода, отправленного на телефон
- c) Использование двух разных паролей
- d) Использование пароля и анонимного прокси-сервера

Ответ. b) Использование пароля и одноразового кода, отправленного на телефон

14**. Какая атака направлена на перехват и изменение коммуникаций между двумя сторонами без их ведома?**

- a) Фишинг
- b) DDoS
- c) Атака "человек посередине" (MITM)
- d) SQL-инъекция

Ответ. c) Атака "человек посередине" (MITM)

15. **Почему сегментация сети важна для безопасности?**

- a) Повышает скорость передачи данных
- b) Упрощает администрирование сети
- c) Ограничивает распространение угроз внутри сети
- d) Увеличивает стоимость оборудования

Ответ. c) Ограничивает распространение угроз внутри сети

16. **Какой из следующих методов может помочь защитить электронную почту от спама?**

- a) Использование VPN
- b) Установка фильтров спама
- c) Шифрование электронной почты
- d) Использование сложных паролей

Ответ. b) Установка фильтров спама

§3.8. Сетевая безопасность

Взаимодействие устройств, протоколов, механизмов аутентификации с интерфейсом и другими компонентами, а

также с технологиями. Политика глобального управления безопасностью в рамках сети организации. Формирование локальной политики безопасности. Внедрение локальных политик безопасности во все устройства защиты информации.

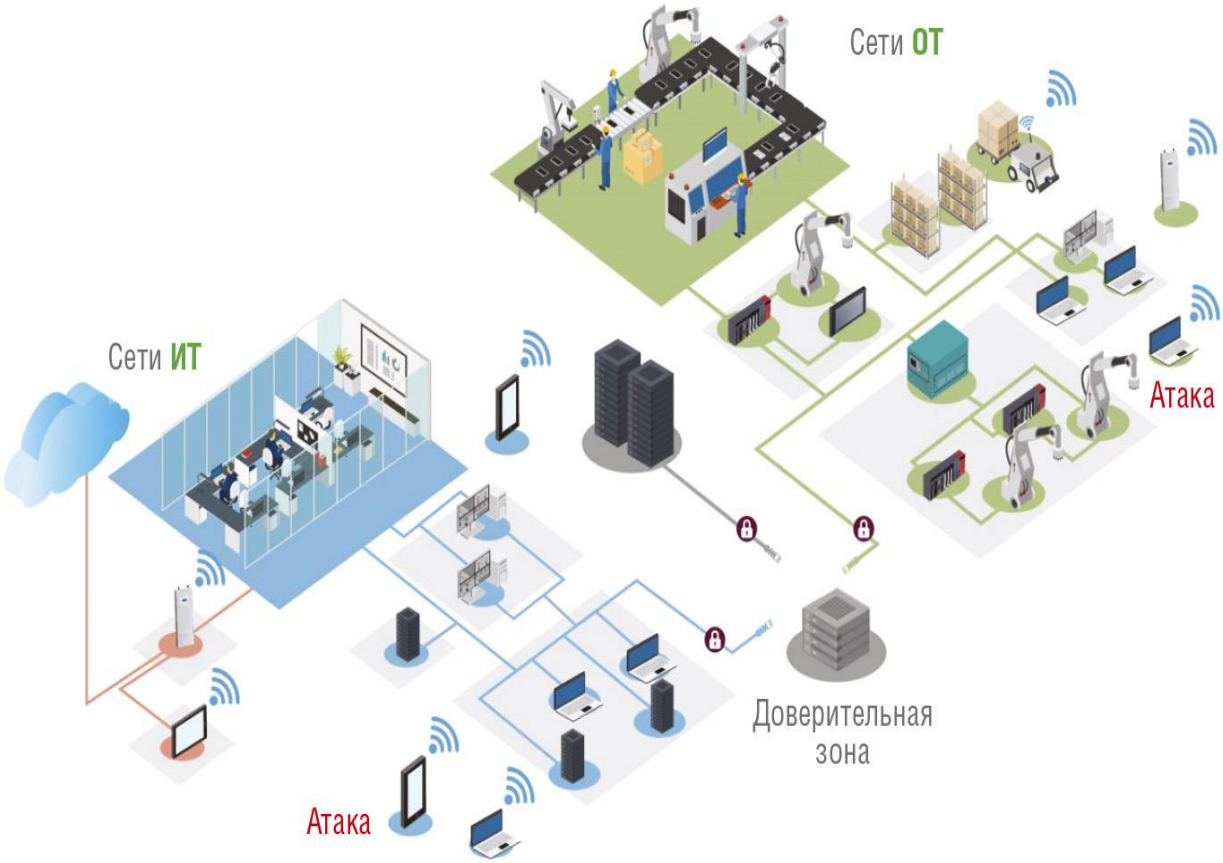

Рисунок 7.4. Инфраструктурная сетевая безопасность

Взаимодействие устройств, протоколов, механизмов аутентификации с интерфейсом и другими компонентами, а также с технологиями.

В современном мире, где цифровые технологии развиваются стремительными темпами, важно понимать, как различные устройства взаимодействуют друг с другом, какие протоколы используются для обмена данными, как обеспечивается безопасность через механизмы аутентификации и как все это интегрируется с пользовательским интерфейсом и другими компонентами системы. Эта лекция поможет вам разобраться в этих ключевых аспектах.

1. Взаимодействие устройств

Устройства — это физические или виртуальные объекты, которые могут обмениваться данными. Примеры устройств включают компьютеры, смартфоны, серверы, IoT-устройства (интернет вещей).

Основные аспекты взаимодействия устройств.

1) Аппаратные интерфейсы — это физические соединения, такие как USB, HDMI, Ethernet, через которые устройства могут передавать данные.
2) Сетевые соединения — используют сети, такие как Wi-Fi, Bluetooth, мобильные сети и др., для обмена данными между устройствами.
3) Программные интерфейсы (API) — программные точки взаимодействия, через которые приложения могут обмениваться данными и командами.

2. Протоколы

Протоколы — это наборы правил, определяющие формат и порядок обмена данными между устройствами.

Основные типы протоколов.

1) Протоколы передачи данных.
    a. HTTP/HTTPS — основа для передачи данных в интернете.
    b. FTP/SFTP — используется для передачи файлов.
    c. SMTP/IMAP/POP3 — для передачи электронной почты.
2) Сетевые протоколы.
    a. IP (Интернет-протокол) — определяет, как данные должны передаваться по сети.
    b. TCP/UDP — транспортные протоколы, управляющие передачей данных между устройствами.
3) Протоколы аутентификации и шифрования.
    a. SSL/TLS — обеспечивают безопасное соединение путем шифрования данных.
    b. OAuth — протокол для безопасной аутентификации и авторизации.

3. Механизмы аутентификации

Аутентификация — процесс проверки подлинности пользователя или устройства.

Основные методы аутентификации.

1) По паролю — самый распространенный метод, при котором пользователь вводит пароль для подтверждения своей личности.
2) Двухфакторная аутентификация (2FA) — добавление второго уровня безопасности, например, через SMS-код или приложение-аутентификатор.
3) Биометрическая аутентификация — использование отпечатков пальцев, распознавания лиц, сканирования радужки глаза.
4) Токены и смарт-карты — физические устройства, которые генерируют одноразовые пароли или хранят зашифрованные данные для аутентификации.

4. Интерфейсы и взаимодействие с пользователем

Интерфейс пользователя (UI) — это то, как пользователь взаимодействует с системой.

Основные аспекты UI.

1) Графический интерфейс пользователя (GUI) — визуальные элементы, такие как окна, иконки, кнопки.
2) Интерфейс командной строки (CLI) — взаимодействие через текстовые команды.
3) Жестовые интерфейсы — используют сенсорные экраны и жесты для управления устройством.
4) Голосовые интерфейсы — позволяют взаимодействовать с системой через голосовые команды (например, голосовые помощники).

5. Интеграция с другими компонентами и технологиями

Интеграция — процесс объединения различных систем и компонентов для работы в единой экосистеме.

Основные аспекты интеграции.

1) Средства интеграции.

a. API — интерфейсы для программирования приложений, позволяющие различным программным компонентам взаимодействовать друг с другом.
b. SDK (Software Development Kit) — наборы инструментов для разработки программного обеспечения, включающие API, документацию и примеры кода.

2) Платформы интеграции.
a. Middleware — промежуточное ПО, которое обеспечивает связь между различными приложениями и службами.
b. Enterprise Service Bus (ESB) — архитектурный стиль для интеграции разнородных систем и сервисов.

3) Технологии виртуализации и контейнеризации.
a. Виртуальные машины (VMs) — эмулируют аппаратное обеспечение для запуска различных операционных систем и приложений на одном физическом сервере.
b. Контейнеры (Docker, Kubernetes) — позволяют упаковывать приложения и их зависимости в стандартизированные блоки для легкого развертывания и масштабирования.

Понимание взаимодействия устройств, протоколов, механизмов аутентификации и интеграции с другими компонентами и технологиями является основой для разработки современных информационных систем. Эти знания помогают создавать надежные, масштабируемые и безопасные решения, которые удовлетворяют потребности пользователей и бизнеса.

Политика глобального управления безопасностью в рамках сети организации.

В современном мире организации всё больше зависят от информационных технологий и сети. Сети компаний становятся глобальными, соединяя офисы и филиалы по всему миру. Это повышает эффективность работы, но также увеличивает риски кибератак и утечек данных. Для защиты информации и обеспечения устойчивости сетевой инфраструктуры

необходимо внедрять политику глобального управления безопасностью.

Что такое политика глобального управления безопасностью?

Политика глобального управления безопасностью – это набор правил и процедур, направленных на защиту информационных ресурсов организации, управление рисками и обеспечение непрерывности бизнес-процессов. Эта политика охватывает все аспекты информационной безопасности, включая физическую безопасность, защиту данных, управление доступом и реагирование на инциденты.

Основные элементы политики глобального управления безопасностью

1. Оценка рисков.

Оценка уязвимостей. Анализ слабых мест в системе безопасности.

Оценка угроз. Идентификация потенциальных угроз, таких как кибератаки, вирусы, инсайдерские угрозы и природные катастрофы.

Оценка последствий. Анализ возможных последствий реализации угроз.

Пример. Международная компания проводит регулярный аудит своей сети, выявляя уязвимости и разрабатывая план по их устранению. Компания определяет, что одна из основных угроз – это фишинговые атаки на сотрудников. В результате принимаются меры по обучению персонала и установке антифишингового ПО.

2. Разработка политики безопасности.

Правила доступа. Определение, кто и к каким ресурсам может получить доступ.

Шифрование данных. Использование методов шифрования для защиты данных.

Мониторинг и аудит. Постоянное отслеживание сетевой активности и проведение аудитов для выявления нарушений.

Пример. Компания внедряет политику доступа, согласно которой сотрудники могут получить доступ к критическим данным только после аутентификации через двухфакторную систему (пароль + код с мобильного устройства). Также проводится регулярный аудит логов доступа для выявления подозрительной активности.

3. Обучение сотрудников.

Повышение осведомленности. Регулярное обучение сотрудников по вопросам информационной безопасности.

Тренировки и тесты. Проведение тренировок по реагированию на инциденты и тестов на знание политики безопасности.

Пример. В компании проводят ежеквартальные тренинги для сотрудников, где обучают их распознавать фишинговые письма, правилам создания сложных паролей и основам безопасного использования сети.

4. Инцидент-менеджмент.

План реагирования на инциденты. Разработка и тестирование планов реагирования на различные типы инцидентов.

Команда реагирования на инциденты. Создание специализированной команды, ответственной за управление инцидентами.

Пример. Компания создает команду быстрого реагирования на инциденты, которая проводит регулярные учения по сценариям кибератак. При возникновении реальной угрозы команда немедленно предпринимает меры для ее нейтрализации, минимизируя ущерб.

5. Контроль и аудит.

Постоянный мониторинг. Использование систем мониторинга для отслеживания сетевой активности в реальном времени.

Регулярные аудиты. Проведение независимых аудитов для оценки эффективности политики безопасности.

Пример. Компания использует системы SIEM (Security Information and Event Management) для сбора и анализа логов в реальном времени. В случае обнаружения аномалий система автоматически уведомляет специалистов по безопасности для принятия мер.

Примеры внедрения политики глобального управления безопасностью

1. Международная корпорация в области финансов.

Оценка рисков показала, что основная угроза – кибератаки на финансовые транзакции.

Введены строгие правила доступа, многослойное шифрование данных и двухфакторная аутентификация.

Регулярное обучение сотрудников по противодействию фишинговым атакам и социальной инженерии.

Создана команда реагирования на инциденты, проводящая ежемесячные тренировки.

Постоянный мониторинг транзакций с использованием систем машинного обучения для выявления подозрительных операций.

2. Глобальная производственная компания.

Оценка рисков выявила угрозы промышленного шпионажа и саботажа.

- Введены меры по защите физических объектов. контроль доступа на производство, видеонаблюдение и охрана.
- Использование VPN для защиты данных при удаленном доступе сотрудников.
- Обучение персонала по вопросам физической безопасности и кибербезопасности.
- Проведение регулярных аудитов и проверок безопасности производственных систем.

Политика глобального управления безопасностью – это неотъемлемая часть успешного функционирования современной организации. Она включает в себя комплекс

мероприятий по оценке рисков, разработке и внедрению мер защиты, обучению персонала и постоянному мониторингу состояния безопасности. Эффективная политика позволяет минимизировать риски, обеспечить защиту данных и непрерывность бизнес-процессов, что особенно важно в условиях глобальной взаимосвязанности и растущих киберугроз.

Формирование локальной политики безопасности.

Локальная политика безопасности (ЛПБ) — это набор правил и процедур, которые регулируют вопросы безопасности в конкретной организации или учреждении. Цель ЛПБ — защитить информационные ресурсы, минимизировать риски и обеспечить устойчивое функционирование организации.

Основные термины

1. Безопасность информации. меры, направленные на защиту данных от несанкционированного доступа, изменения или уничтожения.

2. Угроза. потенциальное событие или действие, которое может причинить вред информационным ресурсам.

3. Уязвимость. слабое место в системе, которое может быть использовано для осуществления угрозы.

4. Риск. вероятность наступления события, которое нанесет ущерб информационным ресурсам.

5. Контроль безопасности. меры, которые принимаются для уменьшения рисков и защиты информации.

Шаги формирования ЛПБ

1. Оценка рисков

Первый шаг — анализ рисков. Необходимо выявить возможные угрозы, оценить их вероятность и потенциальный ущерб.

Пример. В офисе компании могут быть следующие угрозы.

Утечка данных через несанкционированный доступ к компьютерам сотрудников.

Потеря данных из-за сбоя системы или атаки вирусов.

Кража оборудования.

Для каждой угрозы оценивается вероятность её возникновения и возможные последствия.

2. Определение политики безопасности

На основе оценки рисков формулируются правила и процедуры, которые будут регулировать вопросы безопасности.

Пример. Для защиты от утечек данных могут быть введены следующие правила.

- Установка антивирусного ПО на все компьютеры.
- Ограничение доступа к конфиденциальной информации.
- Обучение сотрудников основам кибербезопасности.

3. Внедрение технических и организационных мер

После определения политики необходимо внедрить соответствующие меры безопасности.

Технические меры.

- Установка фаерволов для защиты сети.
- Шифрование данных на компьютерах и серверах.
- Регулярное обновление программного обеспечения.

Организационные меры.

- Создание группы по безопасности информации.
- Разработка планов реагирования на инциденты.
- Проведение регулярных аудитов безопасности.

4. Обучение персонала

Все сотрудники должны понимать и соблюдать ЛПБ. Обучение включает.

- Ознакомление с правилами безопасности.
- Проведение тренингов по реагированию на инциденты.
- Обучение методам защиты от фишинга и других кибератак.

5. Мониторинг и анализ

Постоянный мониторинг системы безопасности позволяет своевременно выявлять и устранять новые угрозы и уязвимости.

Пример. Регулярные проверки журналов событий помогут обнаружить подозрительную активность и предотвратить возможные атаки.

6. Аудит и пересмотр политики

ЛПБ должна быть динамичной и адаптироваться к новым угрозам и изменениям в организации. Регулярные аудиты позволяют выявлять слабые места и вносить необходимые изменения.

Пример. Раз в год проводить аудит политики безопасности и обновлять её с учётом новых технологий и методов атак.

Примеры ЛПБ в различных организациях

1. Банк

Политика контроля доступа. использование биометрических данных для доступа к системе.

- Регулярные проверки безопасности банкоматов.
- Обязательное шифрование всех транзакций.

2. Медицинское учреждение

- Защита персональных данных пациентов с помощью шифрования.
- Ограничение доступа к медицинским данным только для авторизованных сотрудников.
- Внедрение систем мониторинга для обнаружения утечек данных.

3. ИТ-компания

- Использование двухфакторной аутентификации для всех сотрудников.
- Регулярные обновления и патчи для всех систем и приложений.
- Создание резервных копий данных и проверка их целостности.

Формирование локальной политики безопасности — это многоэтапный процесс, требующий тщательного анализа,

планирования и внедрения различных мер защиты. Важно не только создать ЛПБ, но и постоянно её поддерживать и совершенствовать. Только таким образом можно обеспечить надежную защиту информационных ресурсов организации и её устойчивое функционирование.

Внедрение локальных политик безопасности во все устройства защиты информации.

Внедрение локальных политик безопасности во все устройства защиты информации означает внедрение набора правил и мер безопасности на уровне отдельных устройств, чтобы защитить информацию от угроз и несанкционированного доступа.

Представьте, что у вас в офисе есть несколько компьютеров, серверов, мобильных устройств и другой техники, которая используется для обработки и хранения важной информации. Локальные политики безопасности представляют собой набор правил и настроек, которые применяются непосредственно на каждом из этих устройств.

Давайте рассмотрим пример. Предположим, у вас есть компания, которая работает с конфиденциальными клиентскими данными. Вы хотите обеспечить безопасность этой информации на каждом компьютере в офисе. Для этого вы можете внедрить локальные политики безопасности.

Пример 1. Установка паролей и ограничений доступа.

На каждом компьютере вы можете настроить политику, требующую ввода пароля для входа в систему. Это предотвратит несанкционированный доступ к данным даже в случае утери или кражи устройства. Вы также можете настроить доступ к определенным файлам или программам только для авторизованных пользователей.

Пример 3. Шифрование дисков.

Вы можете настроить локальные политики так, чтобы данные на жестких дисках были зашифрованы. Это означает,

что даже если кто-то получит физический доступ к компьютеру, ему будет сложно прочитать информацию без специального ключа.

Пример 3. Обновление программного обеспечения.

Часто обновления программного обеспечения включают исправления уязвимостей безопасности. Вы можете настроить политику, чтобы устройства автоматически загружали и устанавливали эти обновления, что поможет защитить их от известных угроз.

Это всего лишь несколько примеров того, как можно применить локальные политики безопасности. Главное в их внедрении — это настройка их таким образом, чтобы они соответствовали потребностям вашей компании и обеспечивали максимальную защиту конфиденциальности и целостности информации.

Контрольные вопросы.

1. Объясните, каким образом устройства в сети взаимодействуют друг с другом с помощью различных протоколов передачи данных. Укажите основные протоколы и их функции в этом процессе.

2. Что такое механизмы аутентификации и как они взаимодействуют с интерфейсом устройств? Приведите примеры таких механизмов и объясните их роль в обеспечении безопасности сети.

3. Какова роль политики глобального управления безопасностью в сети организации? Объясните, как она определяется и реализуется, и какие могут быть её основные принципы.

4. Что такое локальная политика безопасности, и как она формируется в контексте конкретной организации? Какие факторы и принципы могут влиять на её разработку?

5. Как происходит внедрение локальных политик безопасности во все устройства защиты информации?

Объясните этапы этого процесса и рассмотрите возможные препятствия или сложности при его реализации.

6. Каким образом технологии, такие как шифрование данных и межсетевые экраны, взаимодействуют с локальными политиками безопасности? Как они могут быть интегрированы в сетевую инфраструктуру организации с учётом этих политик?

Тесты для закрепления темы.

1. **Что означает понятие "политика безопасности сети?**

а) Обеспечение доступа к сети без ограничений.

б) Определение правил и мер безопасности для защиты сетевых ресурсов.

в) Установка новых сетевых устройств.

г) Отключение всех сетевых соединений.

Правильный ответ. б) Определение правил и мер безопасности для защиты сетевых ресурсов.

2**. Какие аспекты включают в себя политики безопасности сети?**

а) Только ограничение доступа к сети.

б) Отслеживание активности пользователей в сети.

в) Взаимодействие устройств, протоколов, механизмов аутентификации с интерфейсом и другими компонентами.

г) Проведение технического обслуживания сетевых устройств.

Правильный ответ. в) Взаимодействие устройств, протоколов, механизмов аутентификации с интерфейсом и другими компонентами.

3. **Для чего необходимо формирование локальной политики безопасности?**

а) Для увеличения скорости интернет-соединения.

б) Для предотвращения несанкционированного доступа к сети.

в) Для установки новых программ на компьютеры в сети.

г) Для удаленного управления всеми компьютерами в сети.

Правильный ответ. б) Для предотвращения несанкционированного доступа к сети.

4. **Что включает в себя внедрение локальных политик безопасности в устройства защиты информации?**

а) Использование слабых паролей для доступа к устройствам.

б) Установка антивирусного программного обеспечения на все компьютеры.

в) Передача информации о пользователях третьим лицам.

г) Настройка правил безопасности на маршрутизаторах и брандмауэрах.

Правильный ответ. г) Настройка правил безопасности на маршрутизаторах и брандмауэрах.

5. **Какие факторы влияют на успешное внедрение локальных политик безопасности?**

а) Только количество компьютеров в сети.

б) Обучение персонала по соблюдению политики безопасности.

в) Установка новых программ без предварительного тестирования.

г) Использование одного универсального пароля для всех устройств в сети.

Правильный ответ. б) Обучение персонала по соблюдению политики безопасности.

6. **Какие могут быть последствия от отсутствия эффективной политики безопасности сети?**

а) Только медленная работа компьютеров.

б) Утечка конфиденциальных данных.

в) Увеличение производительности сети.

г) Уменьшение количества атак на сеть.

Правильный ответ. б) Утечка конфиденциальных данных.

7. **Какие действия могут включать в себя локальные политики безопасности?**

а) Разрешение доступа к сети всем пользователям без аутентификации.

б) Ограничение доступа к определенным сетевым ресурсам.

в) Отключение всех механизмов аутентификации.

г) Публикация конфиденциальной информации на внешних ресурсах.

Правильный ответ. б) Ограничение доступа к определенным сетевым ресурсам.

8. **Какое значение имеет глобальное управление безопасностью в сети организации?**

а) Только контроль за использованием электронной почты.

б) Обеспечение целостности, конфиденциальности и доступности информации в сети.

в) Только ограничение доступа к сети с внешних устройств.

г) Регулярное проведение технического обслуживания компьютеров.

Правильный ответ. б) Обеспечение целостности, конфиденциальности и доступности информации в сети.

§3.9. Правовая законодательная база для определения информационного преступления

Правовая законодательная база по выявлению информационных преступлений, совершаемых в информационных процессах в нашей республике и за рубежом. Роль и место информационной

безопасности в системе национальной безопасности страны. Взаимосвязь государственной информационной политики с политикой обеспечения национальной безопасности страны осуществляется через информационную безопасность.

Правовая законодательная база по выявлению информационных преступлений, совершаемых в информационных процессах в нашей республике и за рубежом.

Информационные преступления становятся все более актуальной проблемой в современном мире, так как цифровизация охватывает все аспекты нашей жизни. В Узбекистане и других странах мира принимаются меры по защите от этих угроз и преследованию виновных. В данной лекции мы рассмотрим законодательные меры, направленные на выявление и пресечение информационных преступлений, как в Узбекистане, так и за рубежом.

1. Понятие информационных преступлений

Информационные преступления (киберпреступления) включают широкий спектр незаконных действий, совершаемых с использованием информационных технологий. К таким преступлениям относятся.

- Взлом компьютерных систем и сетей.
- Кража личных данных.
- Распространение вредоносного программного обеспечения (вирусов, троянов).
- Кибермошенничество и фишинг.
- Нарушение авторских прав в интернете.

2. Законодательная база Узбекистана

В Узбекистане разработаны и внедрены законы и нормативные акты, направленные на борьбу с киберпреступлениями.

2.1. Основные законы.

- Закон Республики Узбекистан "Об информации" регулирует отношения в области информации и информационных технологий,

устанавливает права и обязанности участников информационных процессов.

- Закон "О защите персональных данных" направлен на защиту прав граждан в области обработки и использования их личной информации.
- Уголовный кодекс Республики Узбекистан содержит статьи, касающиеся преступлений в сфере информационных технологий. Например, статья 278-1 предусматривает ответственность за несанкционированный доступ к компьютерной информации.

2.2. Органы, занимающиеся борьбой с киберпреступлениями.

- Министерство внутренних дел (МВД), которое включает подразделения, занимающиеся расследованием киберпреступлений.
- Государственный комитет по коммуникациям, информатизации и телекоммуникационным технологиям, занимающийся регулированием и контролем в сфере информационных технологий.

3. Международная правовая база

Для эффективной борьбы с киберпреступлениями необходимо международное сотрудничество. Существуют несколько ключевых международных документов и организаций, которые играют важную роль в этой сфере.

3.1. Будапештская конвенция по киберпреступности (2001). Этот международный договор, разработанный Советом Европы, направлен на гармонизацию национальных законов, улучшение сотрудничества между странами и разработку общих политик противодействия киберпреступности. Узбекистан также рассматривает возможность присоединения к этой конвенции.

3.2. Организация Объединенных Наций (ООН). ООН разработала ряд рекомендаций и модельных законов для борьбы с киберпреступлениями, которые помогают странам развивать свои национальные законодательства в этом направлении.

3.3. Интерпол. Международная организация уголовной полиции активно участвует в расследовании киберпреступлений,

предоставляя поддержку национальным полицейским силам, организуя международные операции и обмен информацией.

4. Примеры и статистика

Для иллюстрации масштаба проблемы можно привести несколько примеров и статистических данных.

4.1. Узбекистан. В 2023 году в Узбекистане зарегистрировано более 1000 случаев киберпреступлений, включая взломы аккаунтов, кражу личных данных и онлайн-мошенничество. МВД активно борется с такими преступлениями, проводя расследования и предотвращая дальнейшие атаки.

4.2. Мировая практика. По данным Интерпола, ежегодно фиксируются миллионы кибератак по всему миру. Например, в 2020 году мировая экономика потеряла около 1 триллиона долларов США из-за киберпреступлений.

5. Противодействие и профилактика

5.1. Национальные меры. Узбекистан активно работает над совершенствованием своей правовой базы и укреплением кибербезопасности. Важные шаги включают внедрение систем защиты информации в государственных и частных структурах, а также повышение уровня киберграмотности населения.

5.2. Международное сотрудничество. Узбекистан участвует в международных форумах и конференциях по кибербезопасности, сотрудничает с другими странами и международными организациями для обмена опытом и передовыми практиками.

Информационные преступления представляют серьезную угрозу как для отдельных граждан, так и для государства в целом. Эффективная правовая база и международное сотрудничество являются ключевыми элементами в борьбе с этими преступлениями. Узбекистан предпринимает значительные усилия для защиты своих граждан и обеспечения безопасности в киберпространстве, активно развивая национальное законодательство и участвуя в международных инициативах.

Роль и место информационной безопасности в системе национальной безопасности страны.

Информационная безопасность (ИБ) становится всё более значимой составляющей национальной безопасности в современном мире. Узбекистан, как развивающаяся страна, активно интегрируется в глобальное информационное пространство, что открывает новые возможности, но также и новые угрозы. В данной лекции мы рассмотрим роль и место информационной безопасности в системе национальной безопасности Узбекистана, приведем реальные примеры и факты.

Рисунок 8.5. Значимость профессии в области информационной безопасности

1. Значение информационной безопасности для Узбекистана

Информационная безопасность — это защита информации и информационной инфраструктуры от несанкционированного

доступа, использования, раскрытия, разрушения, модификации или нарушения. В условиях цифровизации и глобализации информационная безопасность становится критически важной по следующим причинам.

Защита критической инфраструктуры. В Узбекистане активно развиваются государственные и частные информационные системы. Защита этих систем от кибератак необходима для стабильного функционирования экономики, энергетики, транспорта и других ключевых отраслей.

Защита государственных тайн и персональных данных. Информация, касающаяся национальной безопасности, а также персональные данные граждан, должны быть защищены от несанкционированного доступа.

Экономическая безопасность. Утечка конфиденциальной информации и кибератаки могут привести к значительным экономическим потерям и снижению доверия к цифровой экономике страны.

2. Государственная политика в области информационной безопасности

Узбекистан предпринимает значительные шаги для укрепления информационной безопасности на национальном уровне.

Законодательные меры. В 2019 году был принят Закон Республики Узбекистан "О защите персональных данных", который регламентирует порядок обработки и защиты персональных данных граждан.

Создание специализированных органов. Для координации усилий в области информационной безопасности создана Государственная инспекция по контролю за информатизацией и телекоммуникациями (Uzkomnazorat).

Международное сотрудничество. Узбекистан активно сотрудничает с международными организациями и странами СНГ в области кибербезопасности, что позволяет обмениваться опытом и лучшими практиками.

3. Реальные угрозы и инциденты

В последние годы Узбекистан столкнулся с рядом киберинцидентов, которые подчеркивают важность информационной безопасности.

Кибератаки на государственные системы. В 2020 году были зафиксированы попытки несанкционированного доступа к информационным системам ряда государственных органов, что потребовало оперативного реагирования и усиления мер безопасности.

Фишинговые атаки и мошенничество. С ростом использования онлайн-услуг участились случаи фишинговых атак, направленных на кражу личных данных граждан и финансовые мошенничества.

Международные киберугрозы. Узбекистан, как часть глобального информационного пространства, также сталкивается с угрозами международного характера, включая распространение вредоносного ПО и хакерские атаки, исходящие из-за рубежа.

4. Программы и стратегии по усилению информационной безопасности

Для повышения уровня информационной безопасности в Узбекистане реализуются следующие инициативы.

Образовательные программы. В вузах страны вводятся курсы и программы по кибербезопасности, что способствует подготовке квалифицированных специалистов в этой области.

Публичные кампании по повышению осведомленности. Проводятся информационные кампании, направленные на повышение уровня цифровой грамотности населения и информирование о методах защиты от киберугроз.

Техническое оснащение. Внедрение современных технологий и решений для защиты информационных систем, включая системы обнаружения вторжений, шифрование данных и другие средства киберзащиты.

Информационная безопасность играет ключевую роль в обеспечении национальной безопасности Узбекистана. В условиях быстро меняющегося цифрового ландшафта, важность защиты информации и информационной инфраструктуры только возрастает. Скоординированные усилия государства, бизнеса и общества направлены на создание безопасного и устойчивого информационного пространства, что является залогом стабильного и процветающего будущего страны.

Вопросы для обсуждения

1. Какие основные угрозы информационной безопасности вы видите в ближайшие годы для Узбекистана?
2. Как государство и частный сектор могут сотрудничать для повышения уровня информационной безопасности?
3. Какие меры, по вашему мнению, необходимо предпринять для улучшения осведомленности населения о киберугрозах?

Эта тема охватывает ключевые аспекты и примеры, связанные с ролью и значением информационной безопасности в Узбекистане, и направлена на понимание важности данной области в контексте национальной безопасности.

Взаимосвязь государственной информационной политики с политикой обеспечения национальной безопасности страны осуществляется через информационную безопасность.

Рассмотрим, как информационная безопасность играет ключевую роль в этом взаимодействии.

В современном мире информация стала стратегическим ресурсом, от которого зависят не только экономическое развитие и социальная стабильность, но и национальная безопасность. В Узбекистане, как и в любой другой стране, защита информации и управление информационными потоками являются важными составляющими государственной политики.

Государственная информационная политика

Государственная информационная политика Узбекистана направлена на.

1. Обеспечение свободного доступа к информации для граждан и организаций.
2. Развитие информационно-коммуникационных технологий (ИКТ).
3. Создание и поддержание инфраструктуры для безопасного обмена данными.

Эти задачи выполняются через различные государственные программы и инициативы, направленные на цифровизацию и модернизацию всех сфер жизни.

Национальная безопасность

Политика обеспечения национальной безопасности Узбекистана включает.

1. Защиту суверенитета и территориальной целостности.
2. Охрану общественного порядка и правопорядка.
3. Экономическую и информационную безопасность.

Информационная безопасность, в свою очередь, является неотъемлемой частью национальной безопасности, поскольку она обеспечивает защиту от киберугроз, пропаганды и других форм информационной войны.

Информационная безопасность

Информационная безопасность подразумевает защиту информационных ресурсов страны от.

1. Кибератак.
2. Несанкционированного доступа к данным.
3. Информационных диверсий и манипуляций.

Для обеспечения информационной безопасности Узбекистана предпринимаются следующие меры.

1. Разработка и внедрение законодательства, регулирующего информационную сферу.

2. Создание специализированных государственных органов и подразделений, ответственных за кибербезопасность.
3. Обучение и подготовка кадров в области информационной безопасности.

Реальные примеры

1. Законодательство. В 2019 году в Узбекистане был принят Закон "О кибербезопасности", который устанавливает основные принципы и меры по защите информационных систем и сетей.
2. Центр по кибербезопасности. В 2020 году был создан Национальный центр по кибербезопасности, который координирует действия различных государственных органов и частных компаний в области защиты информационных ресурсов.
3. Образовательные программы. Вузами и учебными центрами страны внедряются программы подготовки специалистов в области информационной безопасности, что способствует повышению квалификации кадров и улучшению защиты данных.

Взаимосвязь информационной политики и национальной безопасности

Информационная политика Узбекистана тесно связана с политикой национальной безопасности через.

1. Правовое регулирование. Законодательные акты в сфере информационной безопасности обеспечивают правовую основу для защиты информации и противодействия киберугрозам.
2. Техническую инфраструктуру. Создание и поддержание современных информационных систем и сетей повышает уровень защиты национальных интересов.
3. Международное сотрудничество. Узбекистан активно сотрудничает с международными организациями и соседними странами в области кибербезопасности, что способствует обмену опытом и координации усилий в борьбе с глобальными угрозами.

Взаимосвязь государственной информационной политики и политики обеспечения национальной безопасности Узбекистана через призму информационной безопасности очевидна. Информационная безопасность играет ключевую роль в защите

национальных интересов и стабильности государства. Эффективная защита информационных ресурсов требует комплексного подхода, включающего правовое регулирование, технические меры и подготовку квалифицированных специалистов.

Контрольные вопросы.

1. Какие основные законодательные акты регулируют борьбу с информационными преступлениями в Республике Узбекистан?
2. Какова роль Уголовного кодекса Республики Узбекистан в противодействии информационным преступлениям?
3. Какие международные соглашения и конвенции, направленные на борьбу с киберпреступностью, ратифицированы Узбекистаном?
4. Как осуществляется взаимодействие между правоохранительными органами Узбекистана и международными организациями в области информационной безопасности?
5. Какие меры предусмотрены законодательством Узбекистана для защиты персональных данных и предотвращения их незаконного использования?
6. Какова роль Агентства по защите персональных данных в Республике Узбекистан в контексте информационной безопасности?
7. Какие виды информационных преступлений наиболее распространены в Узбекистане?
8. Какие методы и технологии используются для выявления и расследования информационных преступлений в Узбекистане?
9. Какие меры наказания предусмотрены законодательством Узбекистана за совершение информационных преступлений?
10. Как изменилось законодательство Узбекистана в области информационной безопасности за последние пять лет?
11. Как определяется понятие "информационная безопасность" в законодательстве Узбекистана?1
12. В чем заключается значимость информационной безопасности для национальной безопасности Узбекистана?

13. Какие основные угрозы информационной безопасности существуют в Узбекистане?
14. Какова роль государственных органов в обеспечении информационной безопасности в Узбекистане?
15. Какие стратегии и программы по обеспечению информационной безопасности реализуются в Узбекистане?
16. Какие меры принимаются для защиты критической информационной инфраструктуры в Узбекистане?
17. Каковы основные направления развития политики информационной безопасности в Узбекистане?
18. Какие государственные и частные структуры участвуют в обеспечении информационной безопасности в Узбекистане?
19. Как осуществляется мониторинг и анализ угроз информационной безопасности в Узбекистане?
20. Какова роль образовательных и научных учреждений в обеспечении информационной безопасности Узбекистана?
21. Какова роль государственной информационной политики в контексте обеспечения национальной безопасности Узбекистана?
22. Какие законодательные акты регулируют информационную политику Узбекистана?
23. Как государственная информационная политика способствует защите национальных интересов Узбекистана?
24. В чем состоит взаимодействие между органами государственной власти и частным сектором в области информационной безопасности?
25. Как осуществляется координация между различными государственными структурами в вопросах информационной безопасности?
26. Какие меры принимаются для повышения осведомленности населения о вопросах информационной безопасности?
27. Как международное сотрудничество влияет на информационную политику Узбекистана?
28. Какие информационные ресурсы считаются критически важными для национальной безопасности Узбекистана?

29. Как информационная политика Узбекистана адаптируется к новым вызовам и угрозам в информационной сфере?
30. Какие примеры успешной реализации государственной информационной политики в области обеспечения национальной безопасности можно привести?

Тесты для закрепления темы.

1**. Какой закон регулирует вопросы информационной безопасности в Республике Узбекистан?**

- A) Закон "О борьбе с коррупцией"
- B) Закон "Об информатизации"
- C) Закон "О защите персональных данных"
- D) Закон "О кибербезопасности"

Ответ.B) Закон "Об информатизации"

2. **В каком году был принят Закон Республики Узбекистан "Об информатизации"?**

- A) 1993
- B) 2003
- C) 2013
- D) 2018

Ответ.B) 2003

3. **Какой орган в Узбекистане отвечает за реализацию государственной политики в сфере информационной безопасности?**

- A) Министерство внутренних дел
- B) Министерство по развитию информационных технологий и коммуникаций
- C) Служба государственной безопасности
- D) Генеральная прокуратура

Ответ.B) Министерство по развитию информационных технологий и коммуникаций

4. **Какое наказание предусмотрено за киберпреступления в Узбекистане?**

- A) Только штраф

- B) Лишение свободы до 5 лет
- C) Лишение свободы до 10 лет
- D) Административное взыскание

Ответ.B) Лишение свободы до 5 лет

Роль и место информационной безопасности в системе национальной безопасности Узбекистана

1. **Какую роль играет информационная безопасность в системе национальной безопасности Узбекистана?**
- A) Второстепенную
- B) Приоритетную
- C) Не играет никакой роли
- D) Незначительную

Ответ.B) Приоритетную

2. **Что включает в себя концепция информационной безопасности Узбекистана?**
- A) Защиту национальных сетей
- B) Пропаганду культуры безопасности среди населения
- C) Обеспечение конфиденциальности, целостности и доступности информации
- D) Только борьбу с киберпреступностью

Ответ.C) Обеспечение конфиденциальности, целостности и доступности информации

3. **Какую функцию выполняет информационная безопасность в национальной стратегии безопасности?**
- A) Экономическую
- B) Политическую
- C) Образовательную
- D) Защитную

Ответ.D) Защитную

4. **Какое ведомство курирует реализацию политики информационной безопасности в Узбекистане?**
- A) Министерство обороны
- B) Министерство образования
- C) Министерство внутренних дел

- D) Министерство по развитию информационных технологий и коммуникаций

Ответ.D) Министерство по развитию информационных технологий и коммуникаций

Взаимосвязь государственной информационной политики с политикой обеспечения национальной безопасности через информационную безопасность

1. Как государственная информационная политика влияет на национальную безопасность Узбекистана?

- A) Укрепляет национальную безопасность
- B) Ослабляет национальную безопасность
- C) Не влияет на национальную безопасность
- D) Препятствует национальной безопасности

Ответ.A) Укрепляет национальную безопасность

2. **Какое место занимает информационная безопасность в стратегии национальной безопасности Узбекистана?**

- A) Важное, но не ключевое
- B) Ключевое
- C) Незначительное
- D) Не имеет значения

Ответ.B) Ключевое

3. **Какое из ниже перечисленных утверждений верно относительно государственной информационной политики и национальной безопасности Узбекистана?**

- A) Государственная информационная политика никак не связана с национальной безопасностью
- B) Государственная информационная политика напрямую влияет на обеспечение национальной безопасности
- C) Информационная безопасность важна только для частных компаний
- D) Государственная информационная политика направлена только на образовательные программы

Ответ.B) Государственная информационная политика напрямую влияет на обеспечение национальной безопасности

4. **Какой аспект является ключевым в государственной информационной политике Узбекистана для обеспечения национальной безопасности?**

- A) Образовательные инициативы
- B) Экономическое развитие
- C) Политическая стабильность
- D) Защита информационных ресурсов

Ответ.D) Защита информационных ресурсов

Источники и подтверждения

1. Закон Республики Узбекистан "Об информатизации" принят в 2003 году, регулирует отношения в сфере информатизации.
2. Министерство по развитию информационных технологий и коммуникаций Узбекистана курирует реализацию государственной политики в сфере информационной безопасности.
3. Информационная безопасность является приоритетной частью национальной безопасности Узбекистана, как указано в стратегических документах.

§3.10. Критическое использование СМИ.

Критическое использование СМИ. Право на получение и представление информации / знаний. Сделать информацию / знания прозрачными и понятными для всех.

Критическое использование СМИ.

В современном мире информация окружает нас повсюду, и умение грамотно пользоваться СМИ становится всё более важным навыком. Давайте разберёмся, что это такое, зачем это нужно и как правильно подходить к получению и анализу информации.

1. Что такое СМИ и почему важно их критическое использование? СМИ – это различные платформы и каналы, через которые распространяется информация. телевидение, радио, газеты, журналы, интернет-сайты, социальные сети и т.д. Критическое использование СМИ означает умение анализировать,

интерпретировать и оценивать информацию, которую мы получаем через эти каналы.

Рисунок 9.6. Виды СМИ.

Почему это важно?

- Информация влияет на наше мнение и поведение. СМИ могут формировать общественное мнение, влиять на наши решения и действия.
- Защита от дезинформации. В эпоху интернета количество ложной или искажённой информации сильно возросло. Критическое мышление помогает распознавать фейковые новости.
- Образование и саморазвитие. Правильная интерпретация информации способствует нашему интеллектуальному и культурному развитию.

2. Основные принципы критического использования СМИ

Чтобы эффективно и безопасно использовать СМИ, необходимо придерживаться нескольких принципов.

Проверка источников информации.

- Надёжность источника. оцените, насколько доверителен источник информации. Обратите внимание на репутацию издания, его историю и авторитет.
- Авторы и эксперты. Узнайте, кто является автором статьи или сообщения. Есть ли у него необходимые компетенции и опыт?
- Цель и мотивация. Понимание целей источника информации (образовательные, развлекательные, политические, коммерческие) помогает лучше понять контекст.

Анализ содержания.

- Факты против мнений. Отличайте факты (объективные данные) от мнений (субъективные суждения). Факты можно проверить, мнения – это личная точка зрения.
- Контекст и детали. Обращайте внимание на контекст информации и уточняющие детали. Не принимайте заголовки и краткие сообщения за полную картину.

Сравнение и кросс-проверка.

- Многообразие источников. Сравнивайте информацию из разных источников. Это помогает выявить искажения и противоречия.
- Перекрёстная проверка. Ищите подтверждение информации в других источниках. Это повышает вероятность её достоверности.

Скептическое мышление.

- Вопросы и сомнения. всегда задавайте вопросы. «Кто сказал?», «Почему сказано именно так?», «Какие доказательства есть?».
- Осторожность к сенсациям. Сенсационные новости часто искажают факты ради привлечения внимания.

3. Практические шаги для критического использования СМИ

1. Установите собственные стандарты доверия.
   - Создайте список надёжных источников, которым вы доверяете.
   - Оценивайте новые источники по тем же критериям.
2. Используйте инструменты фактчекинга.
   - В интернете существует множество платформ и сервисов, которые проверяют информацию на достоверность (например, Snopes, FactCheck.org, Media Bias/Fact Check).
3. Обучайтесь и делитесь знаниями.
   - Изучайте методы критического мышления и медиаграмотности.
   - Делитесь своими знаниями с друзьями и близкими, чтобы все могли эффективно использовать СМИ.
4. Придерживайтесь этических норм.
   - Будьте ответственны за распространение информации. Не делитесь непроверенными новостями и слухами.

Критическое использование СМИ – это навык, который требует постоянной практики и внимательности.

Рисунок 10.7 Средства массовой информации.

В условиях информационного потока важно сохранять здравый смысл и аналитическое мышление. Это поможет нам не только защищаться от дезинформации, но и более глубоко понимать мир вокруг нас. Будьте внимательны, анализируйте и делитесь только достоверной информацией!

Право на получение и представление информации / знаний.

Поговорим о праве на получение и представление информации, особенно в контексте информационной безопасности в интернете. Это довольно актуальная и важная тема в нашем современном мире, где доступ к информации играет ключевую роль в нашей повседневной жизни.

Итак, что такое право на получение информации? Это базовое право человека знать, что происходит в мире вокруг нас, иметь доступ к знаниям и источникам информации. В цифровую эпоху интернет стал основным источником информации для миллиардов

людей по всему миру. Но с этим доступом приходят и риски, особенно в сфере информационной безопасности.

Чтобы понять, почему это важно, вспомним, как много личной информации мы храним в интернете. Это могут быть наши фотографии, контактные данные, банковские детали, даже медицинская информация. Именно поэтому защита этой информации так важна.

Давайте рассмотрим несколько реальных фактов.

1. Кибератаки. ежедневно происходят тысячи кибератак, в результате которых могут быть скомпрометированы личные данные пользователей. Нападающие могут использовать различные методы, такие как вредоносные программы, фишинговые атаки и DDoS-атаки, чтобы получить доступ к конфиденциальной информации.

2. Утечки данных. Крупные компании, хранящие большие объемы личных данных пользователей, иногда подвергаются утечкам данных из-за недостаточной защиты или внутренних нарушений безопасности. Это может привести к утечке личной информации миллионов людей.

3. Шпионаж и наблюдение. В ряде стран правительства могут осуществлять массовый надзор за интернет-активностью своих граждан, что может привести к нарушению их права на конфиденциальность.

Теперь, что мы можем сделать для защиты себя и своей информации в интернете?

1. Сильные пароли и двухфакторная аутентификация. Используйте сложные пароли и активируйте двухфакторную аутентификацию для защиты учетной записи.

2. Бережное обращение с личной информацией. Будьте осторожны при предоставлении личной информации в интернете. Проверяйте, какая информация требуется, прежде чем делиться ею.

3. Обновляйте программное обеспечение и используйте антивирусное ПО. регулярно обновляйте программное

обеспечение на своих устройствах и устанавливайте антивирусное программное обеспечение для защиты от вредоносных программ.
4. Обучение о кибербезопасности. Обучайтесь основам кибербезопасности, чтобы понимать потенциальные угрозы и уметь защищаться от них.
Нужно всегда помнить, что защита нашей информации — это не только наше право, но и наша ответственность.

Сделать информацию / знания прозрачными и понятными для всех.

Давайте представим себе, что информация - это как вода. Она может быть чистой и прозрачной, или мутной и неясной. Точно так же и знания могут быть доступны для всех или оставаться непонятными и недоступными.
Когда речь заходит об информационной безопасности в интернете, мы сталкиваемся с огромным объемом данных, которые поступают к нам каждый день. Это могут быть новости, сообщения от друзей, информация о продуктах или услугах, и многое другое. Но как мы можем быть уверены, что эта информация надежна и безопасна?
Вот где вступает понятие прозрачности и понятности информации. Для того чтобы сделать информацию понятной и прозрачной для всех, мы должны следовать нескольким принципам.
1. Проверяйте источник информации. Перед тем как поверить или распространить какую-либо информацию, убедитесь, что она пришла из надежного источника. Это могут быть известные новостные агентства, официальные сайты компаний или организаций.
2. Анализируйте контент. Внимательно оценивайте содержание информации. Проверьте, есть ли у нее подтверждающие факты, логические аргументы и обоснования. Будьте особенно осторожны с информацией, которая вызывает эмоциональные реакции, так как она может быть искаженной или недостоверной.
3. Обратите внимание на контекст. Иногда информация может быть истинной, но выдернутой из контекста, что делает ее неполной или

вводящей в заблуждение. Важно понимать полную картину, чтобы сделать правильные выводы.

Теперь давайте посмотрим на несколько реальных примеров, связанных с информационной безопасностью в интернете.

- Фишинговые атаки. Киберпреступники могут отправлять поддельные электронные письма или создавать фальшивые веб-сайты, чтобы получить доступ к вашим личным данным, таким как пароли или номера кредитных карт. Разбираясь, как выглядят эти мошеннические попытки, вы сможете защитить себя и свою информацию.
- Фейковые новости. В интернете часто появляется ложная информация, которая может быть создана для манипуляции общественным мнением или распространения страха и паники. Проверяйте факты перед тем, как делиться новостями или принимать решения на их основе.
- Утечки данных. Крупные компании могут столкнуться с утечками данных, когда злоумышленники получают доступ к личной информации и могут использовать ее во вред. Будьте внимательны к мерам безопасности, предпринимаемым компаниями, с которыми вы взаимодействуете, и следуйте рекомендациям по защите данных.

Понимание этих реальных угроз поможет нам лучше защищать себя и свою информацию в онлайн-мире. Когда мы делаем информацию прозрачной и понятной для всех, мы создаем безопасное и надежное окружение для обмена знаниями и опытом. И помните, что обучение — это наилучший инструмент для защиты себя и других в цифровой эпохе.

Контрольные вопросы.

1. Какие механизмы использования СМИ могут стать угрозой для информационной безопасности в интернете? Приведите примеры реальных инцидентов.

2. Каким образом право на получение информации может быть нарушено через СМИ в онлайн-пространстве? Приведите примеры случаев цензуры или манипуляции информацией.
3. Какие методы критического мышления могут помочь определить достоверность информации, полученной через СМИ в интернете? Приведите примеры таких методов.
4. Каковы последствия распространения ложной информации через СМИ в интернете для общества и индивидуальных пользователей? Приведите конкретные примеры случаев массовой дезинформации.
5. Какие меры можно предпринять, чтобы сделать информацию в интернете более прозрачной и понятной для всех пользователей? Приведите примеры успешных инициатив в этом направлении.
6. Каким образом технологии, такие как блокчейн или цифровые подписи, могут быть использованы для обеспечения безопасности и подлинности информации в интернете? Приведите конкретные примеры их применения.
7. Как влияет повышенная осведомленность о методах манипуляции информацией через СМИ на общественную защиту от кибератак и кибермошенничества? Приведите примеры обучающих программ или кампаний по информационной грамотности.
8. Какие риски сопряжены с использованием социальных сетей в контексте информационной безопасности? Приведите примеры случаев утечки персональной информации или распространения вредоносных контентов.
9. Как можно определить, что информационный источник в интернете является недостоверным или подвержен манипуляции? Укажите на признаки, на которые следует обращать внимание.
10. Какую роль играют алгоритмы и фильтры в формировании информационного пространства в интернете? В чем состоит опасность их неявной модерации контента? Приведите примеры случаев алгоритмической дискриминации или формирования информационных пузырей.

11. Как можно защитить себя от фишинговых атак в интернете? Объясните, какие приемы используются злоумышленниками для обмана пользователей, и каким образом можно обнаружить и предотвратить подобные атаки.
12. Каким образом информационная грамотность и обучение цифровой безопасности могут помочь в предотвращении распространения непроверенной или ложной информации в интернете? Приведите примеры образовательных программ или инициатив в этой области.
13. Какие роли могут играть государственные органы и международные организации в защите информационной безопасности в интернете? Приведите примеры сотрудничества государственных и частных структур для борьбы с кибер угрозами.
14. Какие последствия могут возникнуть при недостаточной защите личных данных в интернете? Приведите примеры случаев утечки данных и их влияния на жизнь и безопасность пользователей.

Тесты для закрепления темы.

1**. Какое из нижеперечисленных прав гарантирует критическое использование СМИ и право на получение и представление информации/знаний?**

a) Право на безопасность в интернете
b) Свобода слова и информации
c) Право на анонимность в сети
d) Право на шифрование данных

Ответ. b) Свобода слова и информации

2. **Какая из следующих практик способствует деланию информации/знаний прозрачными и понятными для всех?**

a) Использование сложных терминов и языка
b) Ограничение доступа к информации для определенных групп пользователей
c) Обеспечение доступности информации для всех социальных слоев
d) Сокрытие источников информации

Ответ. c) Обеспечение доступности информации для всех социальных слоев

3. **Какая из нижеприведенных ситуаций является примером критического использования СМИ?**

a) Публикация ложной информации без проверки фактов

b) Регулярное анонимное публикование компроматов на политических оппонентов

c) Проведение исследований и анализа различных источников для выявления истины

d) Игнорирование новостей и событий, не относящихся к личным интересам

Ответ. c) Проведение исследований и анализа различных источников для выявления истины

4. **Какая из перечисленных практик способствует укреплению информационной безопасности в интернете?**

a) Использование общедоступных паролей для всех онлайн-аккаунтов

b) Регулярное обновление антивирусного программного обеспечения

c) Распространение личной информации в социальных сетях

d) Использование общедоступных Wi-Fi сетей без защиты

Ответ. b) Регулярное обновление антивирусного программного обеспечения

5. **Какая из перечисленных мер помогает сделать информацию/знания прозрачными и понятными для всех?**

a) Использование сложных технических терминов

b) Объективное и критическое освещение событий и фактов

c) Ограничение доступа к информации для определенных групп пользователей

d) Сокрытие методов сбора и анализа информации

Ответ. b) Объективное и критическое освещение событий и фактов

6. **Какой из нижеперечисленных факторов является ключевым для обеспечения информационной безопасности в интернете?**

a) Опубликование личных данных на всех доступных платформах

b) Регулярное обновление программного обеспечения и использование сильных паролей

c) Публикация информации о своих путешествиях и местах пребывания

d) Отправка конфиденциальной информации через незащищенные сети Wi-Fi

Ответ. b)

7. **Какое из следующих поведений может представлять угрозу для информационной безопасности в интернете?**

a) Использование двухфакторной аутентификации для входа в онлайн-аккаунты

b) Регулярное резервное копирование важных данных на внешние носители

c) Неизменное использование одного и того же пароля для всех сервисов

d) Чтение источников информации различных мнений и точек зрения

Ответ. c) Неизменное использование одного и того же пароля для всех сервисов

8. **Какой из нижеприведенных шагов может помочь вам оценить достоверность информации в интернете?**

a) Повторение информации, которую вы слышите, без проверки ее фактической правдивости

b) Проверка авторитетности источника информации

c) Игнорирование новостей, которые не соответствуют вашему мнению

d) Поддержка только тех новостей, которые подтверждают ваши существующие убеждения

Ответ. b) Проверка авторитетности источника информации

9**. Какой из следующих методов является безопасным способом обмена конфиденциальной информацией в интернете?**

a) Отправка конфиденциальных данных через незащищенные электронные письма

b) Использование сервисов облачного хранения с дополнительной шифровкой

c) Публикация конфиденциальных данных на общедоступных форумах

d) Предоставление доступа к конфиденциальной информации любому, кто запрашивает ее

Ответ. b) Использование сервисов облачного хранения с дополнительной шифровкой

10**. Какое из нижеперечисленных правил является важным для безопасного поведения в интернете?**

a) Публикация личной информации в открытых профилях социальных сетей

b) Избегание обновлений программного обеспечения и антивирусных баз данных

c) Нажатие на ссылки в электронных письмах от незнакомых отправителей

d) Проверка URL-адресов перед вводом личной информации на веб-сайтах

Ответ. d) Проверка URL-адресов перед вводом личной информации на веб-сайтах

ГЛОССАРИЙ

Авторизация- Предоставление доступа к определенным ресурсам или функциям после успешной аутентификации.

Аутентификация- Процесс проверки подлинности личности или сущности.

Безопасность в информационных системах- Обеспечение защиты информации и информационных систем от угроз и рисков.

Бэкап- Копирование данных для их последующего восстановления в случае их утраты или повреждения.

Виртуальная частная сеть (VPN)- Технология, обеспечивающая безопасное и приватное соединение между удаленными узлами через общую сеть, такую как интернет.

Глоссарий- Список слов или терминов с их определениями, используемый для упорядоченного описания специфической области знаний.

Информация- Данные, обработанные и представленные таким образом, чтобы они приобрели смысл или стали полезными для получателя.

Информационная безопасность- Состояние, при котором информация и информационные системы защищены от угроз и рисков.

Информационная система- Система, состоящая из оборудования, программного обеспечения, людей, процессов и процедур, предназначенная для сбора, хранения, обработки, передачи и использования информации.

Инцидент безопасности- Нарушение безопасности информационной системы или сети.

Киберпреступность- Преступные действия, совершаемые с использованием компьютерных технологий и сетей.

Ключ шифрования- Параметр, используемый в криптографических алгоритмах для шифрования и дешифрования данных.

Конфиденциальность- Защита информации от несанкционированного доступа.

Критическое мышление- Способность анализировать информацию критически, осознавать возможные искажения и манипуляции.

Криптография- Наука об обеспечении конфиденциальности, целостности и аутентичности информации с использованием математических методов.

Критическое использование СМИ- Аналитический подход к интерпретации информации, осознание возможных манипуляций и искажений в СМИ.

Математические алгоритмы- Методы обработки данных, основанные на математических принципах, применяемые в криптографии и других областях.

Меры сетевой безопасности- Технические, организационные и правовые меры, предпринимаемые для защиты сети от угроз.

Нормативные акты- Законы, постановления, правила и другие нормативные документы, регулирующие вопросы информационной безопасности и киберзащиты.

Организация защиты сети Интернет- Принципы и методы, направленные на обеспечение безопасности взаимодействия в сети Интернет.

Правовая база- Совокупность законов, правил и норм, определяющих правовой статус и обязанности в сфере информационной безопасности и защиты информации.

Программное обеспечение- Совокупность программных компонентов, предназначенных для выполнения определенных функций или задач.

Сетевая безопасность- Обеспечение защиты сети от угроз и рисков.

Социальные сети- Интернет-платформы и приложения, позволяющие пользователям обмениваться информацией, контактировать друг с другом и создавать сообщества.

Средства массовой информации (СМИ)- Средства распространения информации, такие как газеты, телевидение, радио, интернет и социальные сети.

Технические меры- Меры безопасности, основанные на использовании технических средств, таких как программное обеспечение и оборудование, для защиты информации.

Угроза информационной безопасности- Потенциальная возможность нарушения конфиденциальности, целостности или доступности информации.

Уязвимость- Слабое место в информационной системе, через которое может быть осуществлено нарушение ее безопасности.

Файервол- Сетевое устройство или программное обеспечение, контролирующее и фильтрующее трафик между сетями.

Физическая безопасность- Защита информации, основанная на ограничении физического доступа к оборудованию, хранилищам данных и другим ресурсам.

Шифрование- Преобразование информации с использованием математических алгоритмов для предотвращения несанкционированного доступа.

Целостность- Одно из основных свойств информации, означающее, что данные не подвергались несанкционированным изменениям или повреждениям.

Эксплуатация уязвимости- Использование найденной уязвимости в информационной системе или программном обеспечении для нанесения ущерба или получения несанкционированного доступа.

Электронные угрозы- Угрозы безопасности, связанные с использованием электронных средств и технологий, таких как вредоносные программы, хакерские атаки и кибершпионаж.

Этические стандарты- Набор правил и принципов, определяющих этические нормы поведения и деятельности в области информационной безопасности и кибер защиты.

Список использованной литературы

1. M. Aripov, B.Begalov va boshqalar. Axborot texnologiyalari. O‘quv qo‘llanma. Toshkent 2009.
2. M.Aripov, M.Fayziyeva, S.Dottayev. Web texnologiyalar. O‘quv qo‘llanma. T.. “Faylasuflar jamiyati”, 2013 y.
3. B.Mo‘minov. Informatika. O‘quv qo‘llanma. T.. “Tafakkur-bo‘stoni”, 2014 y.
4. G‘aniyev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. Oliy ta’lim muassasalari uchun mo‘ljallangan darslik. -T.. «Fan va texnologiya» 2010. 407 bet.
5. G‘aniyev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Oliy ta’lim muassasalari uchun mo‘ljallangan darslik. -T.. «Fan va texnologiya» 2017, 372 bet.

Дополнительная Литература

1. Mirziyoev Shavkat Miromonovich. Tanqidiy tahlil, qat’iy tartib-intizom va shaxsiy javobgarlik – har bir rahbar faoliyatining kundalik qoidasi bo‘lishi kerak. Mamlakatimizni 2016 yilda ijtimoiy-iqtisodiy rivojlantirishning asosiy yakunlari va 2017 yilga mo‘ljallangan iqtisodiy dasturning eng muhim ustuvor yo‘nalishlariga bag‘ishlangan Vazirlar Mahkamasining kengaytirilgan majlisidagi ma’ruza, 2017 yil 14 yanvar / Sh.M. Mirziyoev. – Toshkent. O‘zbekiston, 2017. – 104 b.
2. Mirziyoev Shavkat Miromonovich. Qonun ustuvorligi va inson manfaatlarini ta’minlash – yurt taraqqiyoti va xalq farovonligining garovi. O‘zbekiston Respublikasi Konstitutsiyasi qabul qilinganining 24 yilligiga bag‘ishlangan tantanali marosimdagi ma’ruza. 2016 yil 7 dekabr /Sh.M.Mirziyoev. – Toshkent. “O‘zbekiston”, 2017. – 48 b.
3. Mirziyoev Shavkat Miromonovich. Buyuk kelajagimizni mard va olijanob xalqimiz bilan birga quramiz. Mazkur kitobdan O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoevning 2016 yil 1 noyabrdan 24 noyabrga qadar Qoraqalpog‘iston Respublikasi, viloyatlar va Toshkent shahri saylovchilari vakillari bilan o‘tkazilgan saylovoldi

uchrashuvlarida so‘zlagan nutqlari o‘rin olgan. /Sh.M.Mirziyoev. – Toshkent. “O‘zbekiston”, 2017. – 488 b.
4. Mirziyoev Shavkat Miromonovich. Yangi O‘zbekiston strategiyasi.-Toshkent, 2021. -458 b.
5. Kamilov Sh.M., Masharipov A.K., Zakirova T.A., Ermatov Sh.T., Musayeva M.A. Kompyuter tizimlarida axborotni himoyalash. O‘quv qo‘llanma – T.. TDIU, 2005.
6. Галатенко В.А. Основы информатсионной безопасности. Учебное пособие. - М..ИНТУИТ РУ «Интернет» - Университет Информатсионных Технологий» 2009.
7. Щеглов А.Ю. Защита компютерной информации от несанксионированного доступа. – СПб.. Наука и техника, 2004.
8. Richard E.Smith. Elementary Information Security. Jones &Barlett Learning. USA, 2015.
9. Виталий Леонтев. Безопасност в сети Интернет. - М.. ОЛМА Медиа Групп, 2008. – 256 с.

УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ УЗБЕКИСТАН

1. O‘zbekiston respublikasini yanada rivojlantirish bo‘yicha harakatlar strategiyasi to‘g‘risida. (O‘zbekiston Respublikasi qonun hujjatlari to‘plami, 2017 y., 6-son, 70-modda)
2. O‘zbekiston Respublikasi Prezidentining 2020 - yil 6 – noyabrdagi "O‘zbekistonning yangi taraqqiyot davrida ta’lim - tarbiya va ilm - fan sohalarini rivojlantirish chora tadbirlari to‘g‘risida " gi PF - 6108 - son farmoni.

Источники информации

3. http.//www.edu.uz–O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi sayti.
4. http.www.uzedu.uz – O‘zbekiston Respublikasi Xalq ta’limi vazirligi sayti.

http.//www.gov.uz– O‘zbekiston Respublikasi xukumati portali.

O‘QUV ADABIYOTINING NASHR RUXSATNOMASI

Nizomiy nomidagi Toshkent davlat pedagogika universiteti Kengashining 2024 “ 27 ” dekabr dagi “ 5/4.1 ”-sonli qaroriga asosan

Mamarajabov Mirsalim Elmirzayevich

(muallifning familiyasi, ismi-sharifi)

Yusupova Gulchixra Yuldashovna

60112000-Chaqiriqqacha harbiy ta’lim yo‘nalishining

(ta’lim yo’nalishi (mutaxassisligi))

talabalari (o‘quvchilari) uchun tavsiya etilgan

Информационная безопасность и интернет

o‘quv qo‘llanma ga

(o‘quv adabiyotining nomi va turi: darslik, o‘quv qo‘llanma)

O‘zbekiston Respublikasi Vazirlar Mahkamasi tomonidan litsenziya berilgan nashriyotlarda nashr qilishga ruxsat beriladi.

Rektor _____ **A.K.QIRG‘IZBOYEV**

(imzo)

Ro‘yxatga olish raqami **2024-645U-536**

“ 28 ” 12 2024

МАМАРАЖАБОВ МИРСАЛИМ ЭЛЬМИРЗАЕВИЧ
ЮСУПОВА ГУЛЬЧЕХРА ЮЛДАШОВНА

Учебное пособие по дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИНТЕРНЕТ

7513

Muharrir:	Sh.Muhammedov
Texnik muharrir:	G. Ne’matova
Dizayner:	S.Jiyanov
Sahifalovchi:	SH. Muhiddinov

Nashr. lits. № 220812 08.02.2024.
Bosmaxonaga berildi: 27.12.2024. Bosishga ruxsat etildi: 26.02.2025.
Bichimi 60x84 1/16 Offset qog‘ozi. Times New Roman garniturasi.
Shartli bosma tabog‘i 11,25. Nashr hisob tabog‘i 6,1.
Adadi 50 nusxada. Buyurtma № 05-03.
“ZUXRO BARAKA BIZNES” nashriyoti.
Toshkent shahar, Yakkasaroy tumani
Yusuf Xos Xojib ko‘chasi 103 uy.

Bosmaxona. lits. № 220812 08.02.2024.
«ZUXRO BARAKA BIZNES» bosmaxonasida chop
etildi. Toshkent shahri Bunyodkor shoh ko‘chasi 27 A–uy.