«Информационная безопасность»

Лекции 2, 3, тема: Программные и аппаратные средства защиты информации

Преподаватель:
Поздняков Станислав Александрович,
кандидат технических наук
pozdnyakov_sta@mail.ru

2026

1994–2024

КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Филиал
в г. Славянске-на-Кубани

КУБГУ

План лекций (2):

- Методы обеспечения информационной безопасности
- Средства обеспечения информационной безопасности
- Формальные средства защиты информации
- Аппаратные или технические средства защиты информации
- Применение технических средств защиты информации
- Программные средства защиты информации
- Программно-аппаратные средства защиты информации
- Основные вопросы лекции
- Учебная литература
- Самостоятельная работа

План лекций (3):

- Средства уничтожения информации
- Защита от несанкционированного доступа
- Методы и средства технологий защиты от угроз информационной безопасности
- Криптографические методы защиты информации
- Неформальные средства защиты информации
- Безопасный интернет
- Основные вопросы лекции
- Учебная литература
- Самостоятельная работа

Терминология:

Программно-аппаратные средства защиты информации — это сервисы безопасности, встроенные в сетевые операционные системы.

Программно-аппаратные комплексы защиты информации – набор программных и технических средств, совместное действие которых направлено на эффективное выполнение задач по информационной безопасности. Состоят такие комплексы, как правило, из аппаратной (устройство сбора/обработки информации) и программной (специализированное программное обеспечение) части.

Идентификация - процедура распознавания субъекта по его идентификатору.

Аутентификация - процедура проверки подлинности.


Методы обеспечения информационной безопасности
Препятствия
Управление доступом
Маскировка
Регламентация
Принуждение
Побуждение
Средства обеспечения безопасности информации
Формальные
Неформальные
Технические
Программно-аппаратные
Программные
Организа-ционные
Законода-тельные
Морально-этические

Методы защиты информации:

- **Препятствие:**
  метод физического преграждения пути злоумышленнику к защищаемой информации (аппаратуре, носителям информации и т.д.).
  Это начальный уровень защиты, который включает меры физической защиты, такие как охрана, контроль доступа, замки и пропускная система.
  Также сюда входят правовые меры, такие как законодательство и правила внутреннего распорядка.

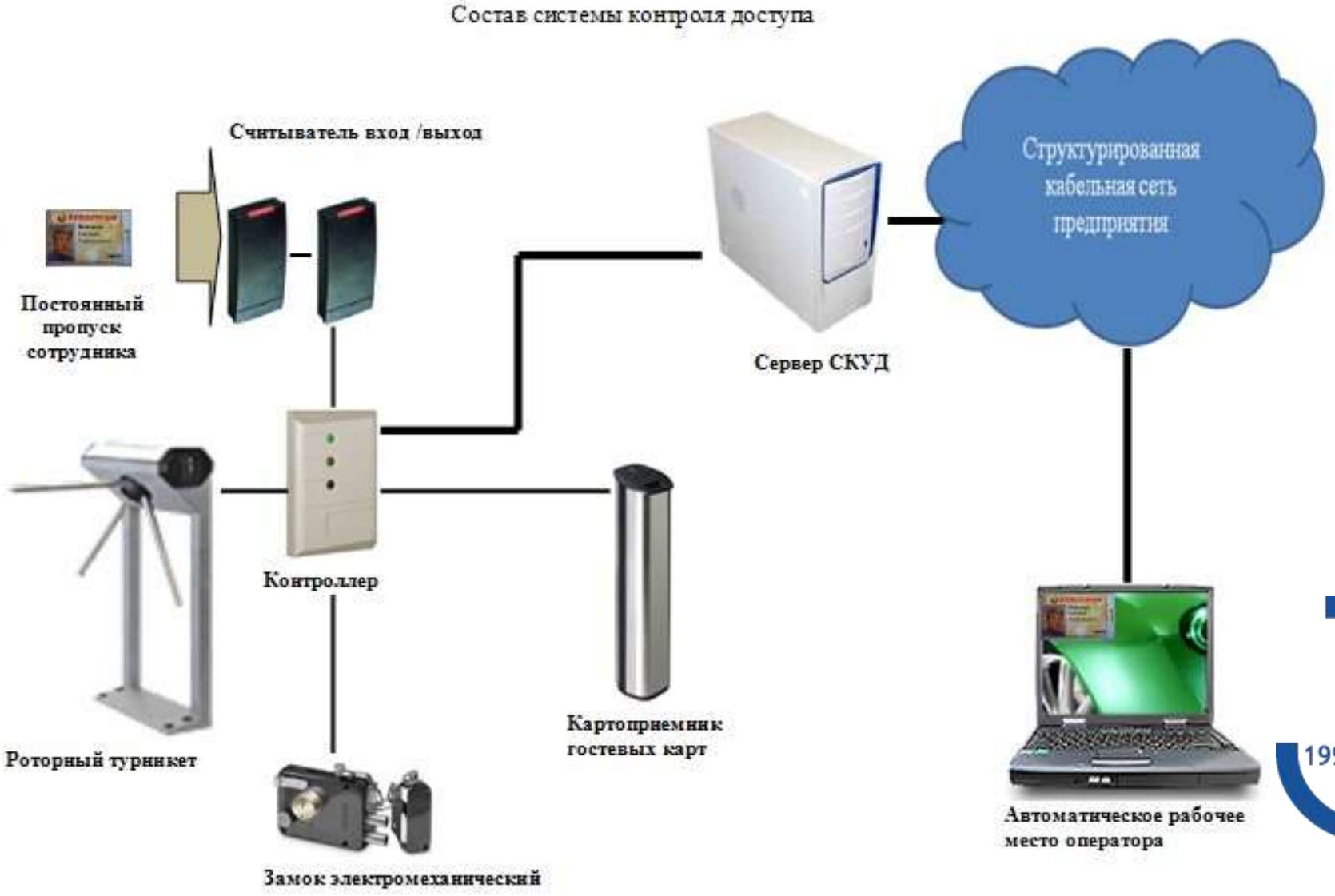
Методы защиты информации:

- **Управление доступом:**
  метод защиты информации регулированием использования всех ресурсов компьютерной информационной системы (элементов баз данных, программных и технических средств).
  Управление доступом включает следующие функции защиты:

➢ *идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);*
➢ *опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;*
➢ *проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);*
➢ *разрешение и создание условий работы в пределах установленного регламента;*
➢ *регистрацию (протоколирование) обращений к защищаемым ресурсам;*
➢ *регистрацию (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.*

Методы защиты информации:

- **Управление контролем доступа**



2026

1994–2024

КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Филиал
в г. Славянске-на-Кубани

КУБГУ

Методы защиты информации:

- **Маскировка:**
  метод защиты информации путем ее криптографического закрытия. Этот метод широко применяется за рубежом как при обработке, так и при хранении информации, в том числе на дискетах. При передаче информации по каналам связи большой протяженности данный метод является единственно надежным.

2026

1994–2024

КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Филиал
в г. Славянске-на-Кубани

КУБГУ

Методы защиты информации:

- **Регламентация:**
  метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму. Охватывает структурное построение системы, технологию обработки данных, организацию работы пользователей и обслуживающего персонала.
- **Принуждение:**
  метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности. Использование юридических мер и законодательства для принуждения соблюдения правил и стандартов безопасности.
- **Побуждение:**
  метод защиты, который побуждает пользователя и персонал системы не нарушать установленный порядок за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных).

Средства защиты информации:

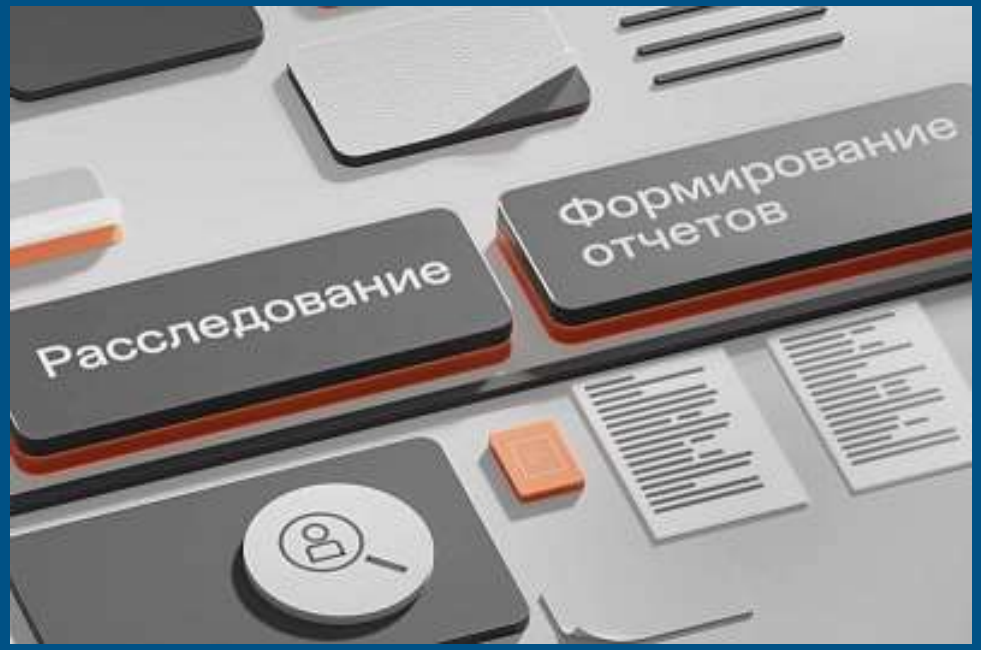
Рассмотренные методы обеспечения безопасности информации реализуются на практике за счет применения различных средств защиты. Средства обеспечения безопасности, используемые для создания механизмов защиты, подразделяются на формальные и неформальные:

- **Формальные:**
  средства защиты, которые выполняют свои функции по заранее установленным процедурам без непосредственного участия человека.

- **Неформальные:**
  средства защиты, которые определяются целенаправленной деятельностью человека, либо регламентируют эту деятельность.

Формальные средства защиты информации:

- Технические, реализуются в виде механических, электрических, электронных, оптических, акустических и других устройств, систем и сооружений, предназначенных для предотвращения доступа нарушителя к защищаемой информации и ее утечки по техническим каналам;



- Программные и программно-аппаратные, представляют собой программное и аппаратное обеспечение, специально предназначенное для выполнения функций защиты информации.

2026

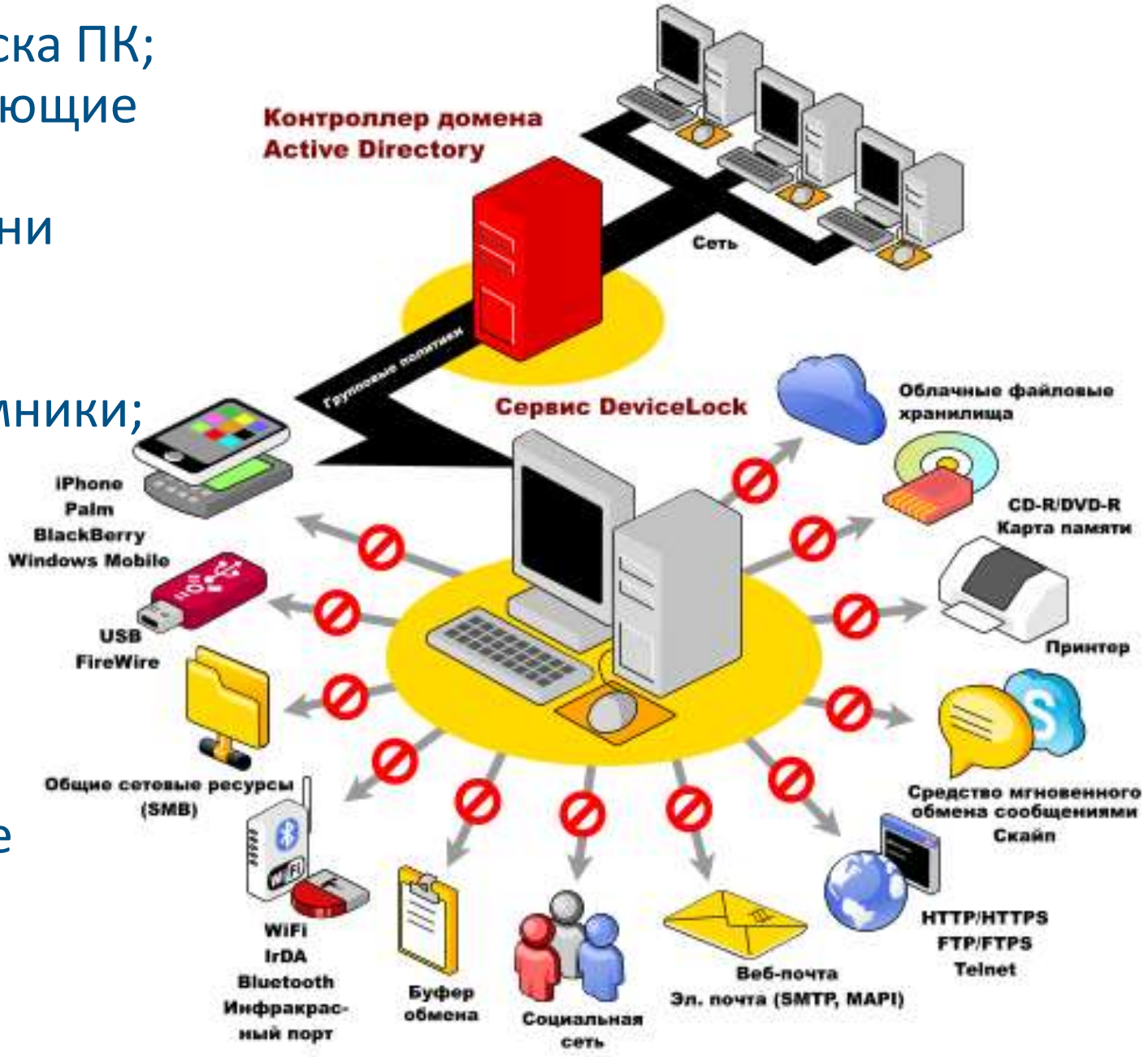
КУБГУ

Средства защиты информации:

- **Технические средства:**
  реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на **аппаратные** и **физические**. Под **аппаратными средствами** принято понимать технику или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Например, система опознания и разграничения доступа к информации (посредством паролей, записи кодов и другой информации на различные карточки). **Физические средства** реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, источники бесперебойного питания, электромеханическое оборудование охранной сигнализации.

Аппаратные или технические средства защиты информации:

- модули доверенного запуска ПК;
- особые регистры, позволяющие максимально обезопасить защитные реквизиты (уровни секретности, пин-коды, пароли и т. д.);
- сканирующие радиоприемники;
- источники шума;
- генераторы кодов, обеспечивающие автосоздание паролей и кодов;
- сетевые фильтры;
- устройства, распознающие биометрические данные пользователей



Технические средства защиты информации:

Техническими являются такие средства защиты, в которых основная защитная функция реализуется некоторым техническим устройством (комплексом, системой).

К **достоинствам** технических средств относятся:

- широкий круг решаемых задач; высокая надежность;
- возможность создания развитых комплексных систем защиты;
- гибкое реагирование на попытки НСД;
- традиционность используемых методов осуществления защитных
- функций.

Основные **недостатки**:

- высокая стоимость многих средств;
- необходимость регулярного проведения регламентных работ и контроля;
- возможность подачи ложных тревог.

Применение технических средств защиты информации:

Применение ТСЗ направлено на решение трех задач:

1. предотвращение проникновения нарушителя к источникам информации;
2. предотвращение повреждения носителя информации в результате воздействия стихийных сил и, прежде всего, пожаров, а также воды и пены при попадании;
3. предотвращение утечки информации по различным техническим каналам.

Функции технических средств защиты:

1. охрана территорий и зданий;
2. охрана внутренних помещений;
3. охрана оборудования и наблюдение за ним;
4. контроль доступа в защищаемые зоны;
5. нейтрализация излучений и наводок;
6. создание препятствий визуальному наблюдению и прослушиванию;
7. противопожарная защита;
8. блокировка действий нарушителя.

Программные средства защиты информации:

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации. В такую группу средств входят:

- механизм шифрования (криптографии — специальный алгоритм, который запускается уникальным числом или битовой последовательностью, обычно называемым шифрующим ключом; затем по каналам связи передается зашифрованный текст, а получатель имеет свой ключ для дешифрования информации).
- механизм цифровой подписи.
- механизмы контроля доступа.
- механизмы обеспечения целостности данных.
- механизмы постановки графика.
- механизмы управления маршрутизацией.
- механизмы арбитража.
- антивирусные программы.
- программы архивации (например, zip, rar, arj и др.).
- защита при вводе и выводе информации и т.д.

Программно-аппаратные средства защиты информации:

Это комплекс средств для защиты информации и информационных систем, реализация которых осуществляется на аппаратном уровне. Они представляют собой устройства различного типа (электронные, механические, электро-механические и т.д.), защищающие информацию аппаратными средствами.

- **Генераторы кодов:** используются для автоматического создания идентифицирующих кодов устройства.
- **Специальные регистры:** предназначены для сохранности защитных реквизитов (идентифицирующих кодов, паролей, грифов и уровней секретности).
- **Устройства для распознания персональных характеристик:** (биометрических данных) человека, которые необходимы для его идентификации – голос, отпечатки пальцев и т.д.
- **Модули доверенного запуска компьютера**
- **Биты секретности:** устанавливают уровень секретности информации.
- **Устройства для шифрования данных:** криптографические СЗИ.

Программно-аппаратные средства защиты информации:

Примеры аппаратных средств защиты информации:

Стоит понимать, что основные средства защиты информации аппаратного уровня могут применяться для выполнения различных задач. Поэтому приведем по несколько примеров в каждом конкретном случае.

Защита от несанкционированного доступа:

Для защиты от несанкционированного доступа используются следующие средства защиты:

- Смарт-карты – электронные устройства, предназначенные для надежной аутентификации пользователей внутри сети без пароля;
- USB-идентификатор – применяется для авторизации пользователя на локальном компьютере или в сети, организации безопасного удаленного доступа, защиты электронной почты, безопасного хранения личной информации;
- Электронный замок – программно-аппаратное средство защиты информации от неразрешенного доступа.

Программно-аппаратные средства защиты информации:

Защита от утечки данных по каналам ПЭМИН:

Побочное электромагнитное излучение и наводки (ПЭМИН) — утечки, возникающие в результате электромагнитного излучение и наводок на различные каналы связи (чаще всего проводные).

В качестве примера можно привести VGA кабель для подключения монитора. Он очень сильно фонит. С него можно считать информацию и получить картинку, идущую на монитор. Для защиты используют чаще всего генераторы белого (гауссовского) шума.

Генераторы белого и радио шума – защищают объекты от утечки информации.

Программно-аппаратные средства защиты информации:

Защита речевой информации:

- Пассивные средства защиты – без изменения внешней среды измеряют, выявляются и локализуют каналы утечки.
- Активные средства защиты – всячески препятствуют возможным средствам негласного получения информации.

Защита телефонных линий связи:

- Аппаратура первого класса: самые простые и дешевые преобразователи, которые искажают сигнал (кнопочные сигнализаторы, шумогенераторы).
- Аппаратура второго класса: скремблеры, работающие со сменным ключ-паролем.
- Аппаратура третьего класса: профессиональная аппаратура, которая изменяет речь в цифровой код. Без ключа практически невозможно восстановить зашифрованный разговор.

Программно-аппаратные средства защиты информации:

Средства уничтожения информации:

- Механические способы: гарантированное уничтожение информации путем измельчения носителя.
- Физические: рабочий слой носителя доводится до магнитного насыщения.
- Химические: нанесение на рабочий слой носителя агрессивные разрушающие средства.
- Термические: разрушение основы носителя путем нагревания.
- Радиационные: небольшое облучение магнитного носителя.

Методы и средства технологий защиты от угроз информационной безопасности:

- К группе технологий **предотвращения ИБ** относятся технологии, осуществляющие упреждение и предупреждение от планирования проникновения, организации и реализации нападений на начальном этапе.
- К группе технологий **парирования угроз ИБ** относятся методы и приемы, препятствующие или ограничивающие воздействие на защищаемый объект.
- К группе технологии **нейтрализации угроз ИБ** относятся средства устранения и ликвидации угроз, а также либо частичной, либо полной их нейтрализации в случае проникновения или диверсии с объектом.

Сокрытие информации подразделяется на информационное и энергетическое:

Энергетическое сокрытие *(ослабление сигнала, зашумление) предполагает уменьшение отношения энергии сигналов, т.е. носителей информации и помех.*

Энергетическое сокрытие информации предусматривает использование таких средств как:

1. электромагнитная экранировка помещений, в которых расположены элементы радиоэлектронной системы;
2. применение в линиях и каналах связи волоконно-оптических кабелей, которые обладают следующими преимуществами: отсутствие электромагнитного излучения во внешнюю среду, устойчивость к внешним электромагнитным излучениям, большая помехозащищенность, скрытность передачи, малые габариты, устойчивость к воздействиям агрессивной среды.
3. активная радиотехническая маскировка подразумевает формирование и излучение в непосредственной близости от элементов радиоэлектронных систем маскирующего сигнала.

Сокрытие информации подразделяется на информационное и энергетическое:

Информационное сокрытие *предполагает изменение или создание ложного информационного портрета семантического сообщения, физического объекта или сигнала.*

Средствами информационного сокрытия являются **маскировка** и **дезинформирование**.

- **Маскировка** предусматривает изменение сигнала с целью затруднения его обнаружения среди других.
- **Дезинформирование** заключается в трансформации исходного сигнала в новый, соответствующий ложной семантической информации и «навязывании» нового сигнала злоумышленнику.

Криптографические методы защиты информации:

Криптографические методы выделяют в отдельную группу инженерно-технических средств защиты информации, хотя они обычно выступают как часть программной или аппаратной защиты, например хранилища ключей шифрования.

Криптографическая защита выполняет две функции:

1. Шифрует данные. Даже если злоумышленник получит доступ к информации, он увидит только зашифрованное сообщение, для расшифровки которого нужен ключ.
2. Подтверждает подлинность передаваемой информации и личность отправителя с помощью механизмов аутентификации. Если файл кто-то изменит или попытается подделать, это сразу станет понятно.

Криптографические методы защиты информации:

Криптографические методы защиты информации (алгоритм):

1. У отправителя есть определенный **ключ**, который он держит в секрете — последовательность битов (нулей и единиц). Такой **ключ** может обеспечивать не только шифрование данных, но и аутентификацию отправителя для того, кто получит сообщение.
2. Отправитель превращает сообщение в последовательность битов и передает в криптографическое устройство (или приложение). Кроме сообщения, на вход дается **секретный ключ**.
3. Криптографическое устройство берет сообщение и производит с ним определенные математические преобразования. На выходе этих преобразований получается **две** последовательности битов — зашифрованное **сообщение** и его уникальная **электронная подпись**, подтверждающая подлинность.
4. Сообщение отправляется принимающей стороне **вместе** с подписью.
5. Принимающая сторона знает **ключ** для расшифровки сообщения и проверки подписи. Проводятся преобразования, чтобы расшифровать сообщение и проверить подпись.
6. Если **ключ неверный** или **данные были изменены**, обратное преобразование не сработает — данные получатся бессмысленными, а подпись не совпадет.

Криптографические методы защиты информации (взлом):

Единственный способ взломать криптозащиту чтобы расшифровать сообщение или подделать подпись — **узнать ключ**.

Есть два способа это сделать:

1. Получить доступ к устройствам, на которых хранятся секретные ключи. От этого предохраняют другие средства защиты информации: физические, программные, аппаратные и организационные.
2. Подобрать ключ — пытаться дешифровать сообщение, перебирая ключи по одному, пока не получится что-то осмысленное.

Формулы устаревших алгоритмов шифрования несовершенны — для подбора ключа нужно перебрать меньше комбинаций, проще взломать алгоритм.

2026

КУБГУ

1994–2024

КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Филиал
в г. Славянске-на-Кубани

Криптографические методы защиты информации (взлом):

Современные методы шифрования намного надежнее.
Чтобы защитить информацию, нужно держать в секрете только ключ.
Секретность самого алгоритма не важна — формулы криптографических преобразований широко известны.

Надежность криптозащиты также зависит от длины ключа.
Например, популярный алгоритм AES использует ключ длиной 128, 192 или 256 бит — современным компьютерам потребуется примерно **1018 лет**, чтобы перебрать все варианты такого ключа.
Для сравнения: **возраст Вселенной**, по оценкам ученых, примерно **$13*10^9$ лет**.

Чем длиннее ключ, тем сложнее его подобрать. Но шифровать сообщения слишком длинным ключом долго и энергозатратно — компьютеру может не хватить на это вычислительных мощностей. Поэтому в криптозащите важен баланс — нужно создать такую систему, чтобы ключ был не слишком длинным и не слишком коротким, оптимальным для шифрования сообщения.
Большинство криптоалгоритмов нельзя взломать, используя современные компьютеры.
Поэтому если шифровать сообщения, можно не бояться их перехвата.

Неформальные средства защиты информации:

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации.

Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла:

строительство помещений, проектирование компьютерной информационной системы банковской деятельности, монтаж и наладка оборудования, использование, эксплуатация.

Неформальные средства защиты информации:

Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в обществе. Эти нормы большей частью не являются обязательными как законно-дательные меры, однако несоблюдение их обычно ведет к потере авторитета и престижа человека.

Неформальные средства защиты информации:

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Об утверждении Доктрины информационной безопасности Российской Федерации

В целях обеспечения информационной безопасности Российской Федерации постановляю:

1. Утвердить прилагаемую Доктрину информационной безопасности Российской Федерации.

2. Признать утратившей силу Доктрину информационной безопасности Российской Федерации, утвержденную Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

3. Настоящий Указ вступает в силу со дня его подписания.

Президент Российской Федерации В.Путин

Москва, Кремль
5 декабря 2016 года
№ 646

2026

КУБГУ

Памятка

безопасного поведения и общения в сети Интернет

Придумай безопасные пароли, держи их в секрете, не сообщай свой телефон и электронный адрес!

Будь вежливым и дружелюбным, не груби, нельзя использовать сеть для хулиганства и угроз!

Используй псевдоним (логин), не сообщай своё имя и фамилию, не высылай фотографии!

Помни о личной безопасности, веди себя осторожно: никогда не сообщай информацию о себе!

Не загружай сомнительные файлы – это вирусы, черви, программы-шпионы, которые приносят вред!

Нельзя встречаться с виртуальными знакомыми – это могут быть злоумышленники!

Не ходи по незнакомым сайтам и ссылкам, можно попасть в «небезопасную зону»!

Прекрати общение и не возобновляй, если тебя оскорбили, сообщи об этом взрослым!

Игнорируй нежелательную почту и рассылки – это спам (ненужные сообщения программ-роботов)!

Уважай авторские права, указывай источник информации! (Часть 4 Гражданского кодекса Р.Ф.)

Не открывай сообщения без взрослого, если не знаешь кто их отправил!

Твои защитники – антивирусные программы, установи их и регулярно обновляй!

Безопасного путешествия в сети!

2026

КУБГУ

Start

Безопасный Интернет

С осторожностью добавляйте незнакомцев в «друзья» и отказывайтесь от личных встреч с людьми, с которыми вы познакомились в Интернете. Обязательно расскажите взрослым и своим друзьям о запросе на такую встречу. Виртуальные друзья могут на самом деле быть не теми, за кого они себя выдают.

Клевета, оскорбление, незаконное копирование продуктов труда других людей и другие противоправные действия, совершенные в виртуальном мире, влекут за собой реальное привлечение к административной, гражданской правовой или даже уголовной ответственности.

Заведите отдельный почтовый адрес для регистрации в социальных сетях, форумах и прочих сервисах - придумайте к нему сложный пароль.

Относитесь с подозрением к сайтам, где запрашивают пароль, адрес, данные паспорта и т.д., просят прислать sms, фотографию, ввести номер телефона.

Если у вас есть вопросы по безопасности в сети Интернет, позвоните на телефон «горячей линии» 8 800 25 000 15

Незнакомые сайты и письма от неизвестных адресатов могут содержать вредоносные программы.

Всё, что вы сообщите о себе в социальных сетях, чатах или форумах, может быть использовано с мошенническими намерениями.

Подумайте прежде, чем разместить фотографии или рассказать о чем-нибудь в онлайн-среде. Фотография, размещенная несколько лет назад, может стать причиной отказа принять вас на работу в будущем.

Оставляйте в сети минимум информации о себе и своих близких, используйте логины и сложные пароли – новые для каждого сайта - чаще их меняйте!

Помните, что в безопасных играх и квестах никогда не предлагается выполнять задания в реальной жизни или в ночное время. Избегайте таких игр.

Если у вас есть вопросы по безопасности в сети Интернет, зайдите на сайт «Дети России онлайн» www.detionline.com

2026

КУБГУ

Учебная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. – 4-е изд. – Москва : РИОР : ИНФРА-М, 2024. – 336 с. – (Высшее образование). – URL: https://znanium.ru/catalog/product/2082642. – ISBN 978-5-369-01761-6.
2. Городнова, А. А. Развитие информационного общества : учебник и практикум для вузов / А. А. Городнова. – 2-е изд. – Москва : Юрайт, 2024. – 294 с. – (Высшее образование). – URL: https://urait.ru/bcode/545422. – ISBN 978-5-534-18716-8.
3. Информатика для гуманитариев : учебник и практикум для вузов / Г. Е. Кедрова [и др.] ; под редакцией Г. Е. Кедровой. – 3-е изд. – Москва : Юрайт, 2024. – 662 с. – (Высшее образование). – URL: https://urait.ru/bcode/536415. – ISBN 978-5-534-16197-7.
4. Киселев, Г. М. Информационные технологии в педагогическом образовании : учебник / Г. М. Киселев, Р. В. Бочкова. – 6-е изд. – Москва : Дашков и К°, 2024. – 300 с. – (Учебные издания для бакалавров). – URL: https://biblioclub.ru/index.php?page=book&id=711130. – ISBN 978-5-394-05582-9.
5. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. – Москва : Юрайт, 2024. – 170 с. – (Высшее образование). – URL: https://urait.ru/bcode/544965. – ISBN 978-5-534-17153-2.

Учебная литература

6. Мансуров, Г. З. Право цифровой безопасности : учебник / Г. З. Мансуров. – Москва : Директ-Медиа, 2022. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=687364. – ISBN 978-5-4499-3061-3.
7. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. – 3-е изд. – Санкт-Петербург : Лань, 2024. – 324 с. – URL: https://e.lanbook.com/book/370967. – ISBN 978-5-507-49077-6.
8. Преступления в сфере высоких технологий и информационной безопасности : учебное пособие / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина ; Московский государственный институт международных отношений (Университет). – Москва : Прометей, 2023. – 1086 с. – URL: https://biblioclub.ru/index.php?page=book&id=701090. – ISBN 978-5-00172-447-6.
9. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=694670. – ISBN 978-5-4499-3327-0.
10. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. – 3-е изд. – Москва : Юрайт, 2024. – 327 с. – (Высшее образование). – URL: https://urait.ru/bcode/542739. – ISBN 978-5-534-16772-6.

Тестовые задания по материалам лекций

1. Разработка законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением – это…
2. Защита информации с помощью ее криптографического преобразования – это…
3. Обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств – это…
4. Применение организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты – это…

Тестовые задания по материалам лекций

5. К правовым методам, обеспечивающим информационную безопасность, относятся:
6. Выберите определение термина «программно-аппаратные средства защиты информации»
7. Для автоматического создания идентифицирующих кодов устройства используются – …
8. Для сохранности защитных реквизитов (идентифицирующих кодов, паролей, грифов и уровней секретности предназначены – …
9. Для установки уровня секретности информации применяются – …
10. Криптографические средства защиты информации – это …
11. Для чего не применяются аппаратные средства защиты информации?
12. Что не относится к средствам функционального назначения аппаратных средств защиты информации?

Тестовые задания по материалам лекций

13. Программно-аппаратное средство защиты информации от неразрешенного доступа – это…
14. С него можно считать информацию и получить картинку, идущую на монитор (очень сильно «фонит») – это…
15. Что защищает объекты от утечки информации?
16. Какие средства измеряют, выявляются и локализуют каналы утечки без изменения внешней среды?
17. Какие средства всячески препятствуют возможным средствам негласного получения информации?
18. Утечки, возникающие в результате электромагнитного излучение и наводок на различные каналы связи (чаще всего проводные) – это…
19. В классификации защиты телефонных линий связи самые простые и дешевые преобразователи, которые искажают сигнал (кнопочные сигнализаторы, шумогенераторы) – это…

Тестовые задания по материалам лекций

20. В классификации защиты телефонных линий связи скремблеры, работающие со сменным ключ-паролем – это…
21. В классификации защиты телефонных линий связи профессиональная аппаратура, которая изменяет речь в цифровой код – это…
22. К аппаратуре первого класса защиты телефонных линий связи относятся…
23. К аппаратуре второго класса защиты телефонных линий связи относятся…
24. К аппаратуре третьего класса защиты телефонных линий связи относятся…
25. Что не относится к способам для уничтожения информации?
26. Рабочий слой носителя доводится до магнитного насыщения – это…
27. Небольшое облучение магнитного носителя – это…
28. Разрушение основы носителя путем нагревания – это…
29. Нанесение на рабочий слой носителя агрессивных разрушающих средств – это…

Тестовые задания по материалам лекций

30. Гарантированное уничтожение информации путем измельчения носителя – это…
31. К методам обеспечения информационной безопасности не относится…
32. Метод обеспечения информационной безопасности «управление» –
33. Метод обеспечения информационной безопасности «маскировка» –
34. Метод обеспечения информационной безопасности «препятствие» –
35. Метод обеспечения информационной безопасности «побуждение» –
36. Метод обеспечения информационной безопасности «принуждение» –
37. Механические, электрические, электронные, оптические, акустические и другие устройства, системы и сооружения, предназначенные для предотвращения доступа нарушителя к защищаемой информации и ее утечки по техническим каналам, относятся к…
38. Программное и аппаратное обеспечение, специально предназначенное для выполнения функций защиты информации, относится к…

Тестовые задания по материалам лекций

39. Организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации компьютерных средств, вычислительной техники, аппаратуры для обеспечения защиты информации относятся к…
40. Законодательными актами страны, регламентирующими правила использования, обработки и передачи информации ограниченного доступа и устанавливающими меры ответственности за нарушение этих правил определяются…
41. Какие средства защиты информации реализуются в виде норм, большей частью не являющихся обязательными, но влияющих на авторитет и престиж человека?
42. Что не относится к группам методов и средств технологий защиты от угроз информационной безопасности?
43. Технологии, осуществляющие упреждение и предупреждение от планирования проникновения, организации и реализации нападений на начальном этапе относятся к…

Тестовые задания по материалам лекций

44. Методы и приемы, препятствующие или ограничивающие воздействие на защищаемый объект, относятся к…
45. Средства устранения и ликвидации угроз, а также либо частичной, либо полной их нейтрализации в случае проникновения или диверсии с объектом, относятся к…
46. Что не относится к функциям технических средств защиты?
47. Для какой подсистемы защиты верно описание: «Основой данной подсистемы являются механические или строительные элементы, создающие для нарушителя реальное физическое препятствие»?
48. Для какой подсистемы защиты верно описание: «При построении данной подсистемы рекомендуется: оценить требуемую степень безопасности организации, которую можно повысить, к примеру, путем дополнения устройств считывания карточек средствами ввода персонального кода»?
49. Для какой подсистемы защиты верно описание: «Основные характеристики подобных подсистем определяются, главным образом, характеристиками используемых датчиков»?

Тестовые задания по материалам лекций

50. Для какой подсистемы защиты верно описание: «При срабатывании датчиков подсистемы изображение, передаваемое соответствующей телекамерой, автоматически выводится на экран монитора на центральном посту охраны»?
51. Для какой подсистемы защиты верно описание: «Каналами передачи сигнала могут быть специально проложенные проводные линии, телефонные линии объекта, телеграфные линии и радиосвязь»?
52. Для какой подсистемы защиты верно описание: «Для предотвращения вторжения на охраняемую территорию используется оборонительная система, в которой находят применение осветительные и звуковые установки»?
53. Для какой подсистемы защиты верно описание: «Центральный пост должен обеспечивать автоматическую регистрацию и отображение всех поступающих на центральный пост сообщений и сигналов тревоги, выполнение всех необходимых процедур»?

Тестовые задания по материалам лекций

54. Изменение сигнала с целью затруднения его обнаружения среди других предполагает…
55. Трансформация исходного сигнала в новый, соответствующий ложной семантической информации и «навязывание» нового сигнала злоумышленнику предполагает…
56. Формирование и излучение в непосредственной близости от элементов радиоэлектронных систем маскирующего сигнала предполагает…

Основные вопросы лекций:

1. Охарактеризуйте основные методы информационной безопасности.
2. Какие средства обеспечения безопасности относятся к формальным?
3. Какие средства обеспечения безопасности относятся к неформальным?
4. На какие группы подразделяются методы и средства обеспечения безопасности?
5. На решение каких задач направлено применение технических средств?
6. На какие группы подразделяются технические средства защиты информации?
7. Что такое информационное и энергетическое сокрытие информации?
8. Что такое криптозащита информации?

Спасибо за внимание!

2026

1994–2024

КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Филиал
в г. Славянске-на-Кубани

КУБГУ