ГУАП

КАФЕДРА №

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ _____

ПРЕПОДАВАТЕЛЬ

должность, уч. степень, звание		подпись, дата		инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №

Вариант

по курсу:

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. №					
			подпись, дата		инициалы, фамилия

Санкт-Петербург 2025

СОДЕРЖАНИЕ

0.1 Самопроверка

1. Актуальность защиты информации. Сущность и понятие информационной безопасности (ИБ). Основные характеристики ИБ
    1. Определение ИБ и безопасности ИС
    2. Базовые характеристики безопасности
        1. Конфиденциальность
        2. Целостность
        3. Доступность
    3. Дополнительные характеристики
        1. Аутентичность
        2. Безотказность
        3. Достоверность
        4. Подотчетность
2. Этапы развития защиты информации
    1. Начальный этап
        1. Три вида разграничения доступов
            1. Мандатное
            2. Ролевое
            3. Матрица полномочий
    2. Развитый этап
    3. Комплексный тап
        1. Три вида комплексности
            1. Целевая
            2. Инструментальная
            3. Всеобщая
    4. Идентификация/Авторизация/Аутентификация
3. Место ИБ в системе национальной безопасности. Доктрина ИБ. Законодательство в области ЗИ
    1. Определение доктрины ИБ в РФ
    2. Что рассматривает?
    3. Интересы

    4. Угрозы
    5. Меры
4. Теория защиты информации (ТЗИ). Ее составные части
    1. Определение ТЗИ
    2. Цель теории ЗИ
    3. Составные части
        1. Методологический базис
            1. Методы нечетких множеств
            2. Нестрогая математика
            3. Неформальное оценивание
            4. Неформальный поиск оптимальных решений
5. Методологический базис ТЗИ
    1. Нестрогая математика
    2. Неформальные методы оценивания
    3. Неформальные методы поиска оптимальных решений
    4. Методы непосредственного поиска
6. Нестрогая математика. Основные положения теории нечетких множеств
    1. Определение нестрогой математики
    2. Определение нечеткого множества
    3. Методы построения
    4. Определение лингвистических переменных
    5. Операции над нестрогими множествами
7. Неформальные методы оценивания
    1. Определение неформальных методов оценивания
    2. Метод экспертных оценок
    3. Способы и критерии привлечения экспертов
    4. Требования к числу экспертов
    5. Формы выражения оценок
    6. Методы оценок
8. Неформальные методы поиска оптимальных решений
    1. Что такое ПОР?
    2. Когда применяется и какие есть виды?
    3. Эвристика и эвристическое программирование

        1. Классификация
    4. Эволюционное моделирование
    5. Эргатические системы
9. Методы непосредственного поиска
    1. Экспертные оценки
    2. Неформально-эвристическое программирование
    3. Психоинтеллектуальная генерация
    4. Управление продуктивным мышлением
    5. Мозговой штурм
10. Защищаемая информация. Классификация информации по категориям доступа
    1. Определение защищаемой информации
    2. Классификация по категории доступа
    3. Критерии защищаемой информации
    4. Виды защищаемой информации.
        1. Гос-тайна
        2. Конфиденциальная
        3. Персональные данные
        4. Коммерческая тайна
        5. Служебная тайна
        6. Профессиональная тайна
11. Информация с ограниченным доступом и сведения, которые к ней не относятся
    1. Виды и определения
12. Понятие государственной тайны. Защита государственной тайны | определение, наказание, кто защищает
    1. Определение гос-тайны и критерии причастности.
    2. Кто осуществляет?
    3. Ответственность
13. Коммерческая тайна и её защита
    1. Определение
    2. Условия отнесения
    3. Меры
    4. Что не могут скрывать

14. Понятие конфиденциальной информации
    1. Определение
    2. Виды
15. Понятие компьютерных преступлений. Основные виды преступлений, связанных с ИБ
    1. Определение ИБ преступлений
    2. Классификация
        1. Экономические
        2. Против личных прав и частной сферы
        3. Против государственных и общественных интересов
    3. Основные виды
        1. НСД
        2. Разработка и распространение вредоносного ПО
        3. Невнимательность и небрежность
        4. Внедрение логических бомб
        5. Подделка информации в информационных системах
        6. Хищение
        7. Пиратство
16. Теория и классификация угроз защите информации
    1. Определение угроз
    2. Виды воздействия
    3. Классификация
        1. Виды
        2. Природа происхождения
        3. Предпосылки появления
        4. Источники
17. Предпосылки угроз ИБ: объективные и субъективные
    1. Определение предпосылок
    2. Обьективные
    3. Субьективные
18. Классификация угроз по происхождению
    1. Определение
    2. Случайные
    3. Преднамеренные

19. Классификация угроз по типам воздействия
    1. Определение
    2. Угрозы физической целостности
    3. Угрозы структуры информации
    4. Угрозы содержания информации
    5. Угрозы конфиденциальности
    6. Угрозы прав собственности
20. Вредоносные программы. Классификация, особенности и способы маскировки в среде
    1. Определение вредоносных программ
    2. Определение разрушающего программное воздействие
    3. Класификация
        1. Крекеры
        2. Компьютерные вирусы
        3. Логические бомбы
        4. Программы раскрытия паролей
        5. Репликаторы
        6. Сетевые программные анализаторы
        7. Суперзаппинговые утилиты
        8. Тайные ходы и лазейки
        9. Троянские кони
    4. Способы маскировки
21. Классификация вирусов по инфицируемым объектам
    1. Файловые
    2. Загрузочные
    3. Файлово-загрузочные
22. Классификация вирусов по способу инфицирования и способу размещения
    1. Резидентные
    2. Неризедентные
    3. Сопровождающие
    4. Включающие
    5. Перекрывающие
23. Классификация вирусов по разрушающему воздействию, по спо-

собности к изменению и по типу кода

1. Безвердные
2. Неопасные
3. Опасные
4. Особо опасные
5. Сигнатурные
6. Полиморфные
7. Микрокодируемые
8. Макрокодируемые

24. Методы защиты информации и соответствующие им средства защиты. Примеры
    1. Препятствия
    2. Управление доступом
    3. Маскировка
    4. Регламентация
    5. Принуждение
    6. Побуждение
25. Средства защиты информации и соответствующие им методы защиты. Примеры
    1. Стеганография
    2. Организационные
    3. !!!
26. Криптографическая защита информации. Понятие. Классификация методов
    1. Что такое криптографическая защита информации
    2. Понятие криптографии
    3. Отличие от шифрование
    4. Симметричные
    5. Асимметричные
27. Симметричные и асимметричные системы шифрования. Особенности. Примеры
28. Шифр Цезаря и шифр древней Спарты
29. Шифр: “одиночная перестановка по ключевому слову”. Алгоритм двойной перестановки

30. Перемешивание исходного текста с использованием магического квадрата. Шифр многоалфавитной замены
31. Определение и общие принципы построения систем защиты информации
    1. Принципы
    2. Признаки криптографической системы
    3. Обеспечение
32. Типизация систем защиты. Классификация СЗИ при типизации
    1. Определение типизации
    2. Определение стандартизации
    3. По уровне обеспечиваемой защиты.
    4. По активности реагирования
33. Стандартизация систем защиты. Уровни стандартизации
    1. Уровень системы
    2. Уровень компонентов
    3. Уровень проектных решений
34. Деление СЗИ по уровню обеспечиваемой безопасности
    1. Системы слабой защиты
    2. Системы сильной защиты
    3. Системы очень сильной защиты
    4. Системы особой защиты

1 Актуальность защиты информации. Сущность и понятие информационной безопасности (ИБ). Основные характеристики ИБ

1.1 Основной ответ

Информационная безопасность (ИБ) — это состояние защищённости обрабатываемых, хранимых и передаваемых в информационно-телекоммуникационных системах (ИТС) данных от незаконного ознакомления, преобразования и уничтожения, а также состояние защищённости информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Безопасность информационной системы (ИС) — это защищённость системы от случайного или преднамеренного вмешательства в нормальный процесс её функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения её компонентов. Иначе говоря, это способность противодействовать различным возмущающим воздействиям на ИС.

К *базовым характеристикам* безопасности информации относят:

- **Конфиденциальность (Confidentiality)** — свойство информации быть недоступной для неавторизованных лиц. Информация не может быть доступна неавторизованной стороне, то есть для неё она просто не существует. Авторизованная сторона может иметь полный доступ к информации.
- **Целостность (Integrity)** — свойство информации противостоять несанкционированному изменению. Информация не подвергается никакому воздействию от неавторизованной стороны.
- **Доступность (Accessibility)** — возможность использования соответствующих ресурсов в заданный момент времени согласно предъявленным полномочиям. Авторизованная сторона по первой потребности получает неограниченный доступ к нужной информации.

1.2 Дополнение

Помимо базовых характеристик, в информационной безопасности выделяются *дополнительные характеристики*, которые обеспечивают более глубокий уровень защиты:

- **Аутентичность (Authenticity)** — подтверждение подлинности источника информации. Гарантирует, что субъект или ресурс идентичны заявленному.
- **Невозможность отказа (Non-repudiation)** — невозможность отрицания факта совершения действия. Обеспечивает, что субъект не может отказаться от совершённых им действий.
- **Подотчётность (Accountability)** — возможность отслеживания действий субъектов. Обеспечивает фиксацию и идентификацию действий пользователей и систем.
- **Достоверность (Reliability)** — соответствие информации ожидаемому поведению и результатам. Гарантирует, что информация соответствует установленным требованиям.

Эти характеристики особенно важны в контексте современных угроз, таких как фишинг, атаки программ-вымогателей и утечки данных, и находят отражение в международных стандартах, таких как ISO/IEC 27000.

2 Этапы развития защиты информации

2.1 Основной ответ

Развитие защиты информации прошло три ключевых этапа:

2.1.1 Начальный этап

Характеризуется применением формальных средств защиты, направленных на предотвращение несанкционированного доступа (НСД). Основные методы:

- **Проверка по паролю**: доступ к системе разрешался при совпадении введённого пароля с эталонным, хранящимся в памяти.
- **Разграничение доступа** к данным с целью ограничения доступа зарегистрированных пользователей к информации за пределами их полномочий.

Методы разграничения доступа:

1. **Деление массивов на зоны по степени секретности**: пользователям предоставлялся доступ в соответствии с их уровнем допуска.
2. **Мандатный доступ**: выдача пользователям мандатов с указанием идентификаторов разрешённых областей данных.
3. **Матрица полномочий**: таблица, где строки — пользователи, столбцы — элементы данных, а на пересечении — права доступа (чтение, запись и т.п.).

2.1.2 Развитой этап

Основные характеристики:

- Появление понимания необходимости комплексного подхода к информационной безопасности, включая обеспечение целостности информации.
- Расширение средств защиты: технические, программные, организационные меры, включая криптозащиту.
- Формирование функциональных подсистем защиты в автоматизированных системах обработки данных (АСОД).

Развитие методов распознавания пользователей:

- **Усложнённые пароли**
- **Биометрические методы**: отпечатки пальцев, голос, подпись, гео-

метрия руки, рисунок сетчатки глаза.

- **Пластиковые карты** с информацией о пользователе.

2.1.3 Комплексный этап

Характеризуется переходом к научно-методологическому подходу в защите информации. Введено понятие **комплексности**:

- **Целевая комплексность**: решение нескольких разноплановых задач в рамках единой концепции.
- **Инструментальная комплексность**: использование различных инструментальных средств для решения одной задачи.
- **Всеобщая комплексность**: сочетание целевой и инструментальной комплексности.

2.2 Дополнение

2.2.1 Три вида комплексности

1. **Целевая комплексность**: интеграция различных задач (например, обеспечение конфиденциальности и целостности) в единую стратегию защиты.
2. **Инструментальная комплексность**: применение разнообразных средств (технических, программных, организационных) для решения одной задачи.
3. **Всеобщая комплексность**: объединение целевой и инструментальной комплексности, обеспечивая всестороннюю защиту информации.

2.2.2 Три метода разграничения доступа

1. **Мандатное разграничение**: доступ определяется на основе предписанных политик безопасности и уровней допуска.
2. **Ролевое разграничение**: права доступа предоставляются в соответствии с ролью пользователя в системе.
3. **Матрица полномочий**: детализированное определение прав доступа каждого пользователя к каждому ресурсу.

2.2.3 Различие между идентификацией и аутентификацией

- **Идентификация**: процесс предоставления пользователем идентификатора (например, логина) для обозначения своей личности в системе.
- **Аутентификация**: процесс проверки подлинности предоставленного

идентификатора, подтверждающий, что пользователь является тем, за кого себя выдаёт.

Пример: при входе в систему пользователь вводит логин (идентификация), затем пароль (аутентификация). Дополнительный ввод одноразового кода из SMS представляет собой **двухфакторную аутентификацию**, повышающую уровень безопасности.

3 Место информационной безопасности в системе национальной безопасности. Доктрина ИБ. Законодательство в области защиты информации

Информационная безопасность (ИБ) является неотъемлемой частью национальной безопасности Российской Федерации. Это обусловлено возрастающей зависимостью общества, государства и экономики от информационных технологий и информационной инфраструктуры.

3.0.1 Назначение Доктрины информационной безопасности РФ 2016 года

Доктрина ИБ РФ 2016 года представляет собой систему официальных взглядов на обеспечение национальной безопасности в информационной сфере. Она определяет:

- стратегические цели и задачи в области ИБ;
- национальные интересы в информационной сфере;
- основные угрозы информационной безопасности;
- меры по предотвращению и нейтрализации этих угроз;
- силы и средства обеспечения ИБ.

Доктрина служит основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения ИБ.

3.0.2 Чьи интересы прописаны в Доктрине и в чем они заключаются

Доктрина охватывает интересы:

- **Личности**: обеспечение и защита конституционных прав и свобод человека и гражданина в части получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий.
- **Общества**: сохранение духовно-нравственных ценностей, культурного и исторического наследия, обеспечение информационной поддержки демократических институтов и механизмов взаимодействия государства и гражданского общества.
- **Государства**: обеспечение суверенитета, территориальной целост-

ности, устойчивого социально-экономического развития, обороны и безопасности государства.

3.0.3 Угрозы информационной безопасности

Доктрина выделяет следующие основные угрозы информационной безопасности:

- **Наращивание рядом зарубежных стран возможностей информационно-технического воздействия** на информационную инфраструктуру РФ в военных целях.
- **Информационно-психологическое воздействие** спецслужб отдельных государств, направленное на дестабилизацию внутриполитической и социальной ситуации, подрыв суверенитета и нарушение территориальной целостности РФ.
- **Дискриминация российских СМИ за рубежом** и предвзятая оценка государственной политики России в зарубежных СМИ.
- **Наращивание информационного воздействия на население России**, особенно на молодежь, с целью размывания традиционных российских духовно-нравственных ценностей.
- **Возрастание масштабов компьютерной преступности**, прежде всего в кредитно-финансовой сфере.
- **Увеличение числа преступлений**, связанных с нарушением прав на неприкосновенность частной жизни при обработке персональных данных с использованием информационных технологий.

3.0.4 Меры предотвращения угроз

Для предотвращения и нейтрализации угроз информационной безопасности Доктрина предусматривает:

- **Развитие нормативно-правовой базы** в области ИБ.
- **Совершенствование системы обеспечения информационной безопасности**, включая правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры.
- **Развитие отечественной отрасли информационных технологий и электронной промышленности**, а также совершенствование де-

ятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения ИБ.

- **Содействие формированию системы международной информационной безопасности**, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности и на укрепление равноправного стратегического партнерства в области ИБ.

4 Теория защиты информации (ТЗИ). Ее составные части

Теория защиты информации (ТЗИ) — это совокупность основных идей, касающихся защиты информации, её становления и развития во взаимосвязи с другими отраслями знаний. Она базируется на многовековом опыте решения задач ЗИ, полученного как интуитивно, так и научными методами, и получила активное развитие с распространением вычислительной техники.

Цели теории ЗИ: - формулировка научной постановки задач ЗИ для конкретных информационных систем (ИС), объектов и организаций; - использование современных методов и методологий ЗИ; - разработка стратегических установок по организации ЗИ; - анализ и обоснование перспективных направлений развития ЗИ.

4.1 Составные части теории ЗИ

4.1.1 Методологический базис

Методологический базис теории ЗИ — совокупность методов и моделей, необходимых для изучения проблем ЗИ и решения практических задач.

Он включает как *традиционные методы системного анализа*, так и *современные методы*, позволяющие моделировать процессы с высоким уровнем неопределенности. К таким относятся:

- **Методы нечетких множеств**;
- **Нестрогая математика**;
- **Неформальное оценивание**;
- **Неформальный поиск оптимальных решений**.

Актуальность этих методов обусловлена *сложностью моделирования процессов*, подверженных воздействию непредсказуемых факторов — особенно связанных с действиями злоумышленников.

4.1.2 Нестрогая математика

Нестрогая математика (или **теория лингвистических переменных**) — это подход, опирающийся на неформальные суждения и умозаключения, основанные на здравом смысле и опыте человека. Применяется для построения моделей систем с высоким уровнем неопределённости.

Ключевые элементы: - **Лингвистическая переменная** — переменная, значения которой описываются словами естественного языка (например:

«низкий», «высокий»). - **Формализация лингвистической переменной**: - x — имя переменной; - $T(x)$ — базовое терм-множество (набор лингвистических значений); - X — универсальное множество; - G — правила синтаксического преобразования; - M — семантические процедуры (функции принадлежности).

Пример:
Переменная «Угроза информационной безопасности» может принимать значения:
{Низкая, Средняя, Высокая, Очень высокая}, и каждое значение моделируется через нечеткое множество.

Таким образом, **нестрогая математика** позволяет формализовать субъективные оценки, характерные для задач ЗИ, где точные численные данные недоступны или нецелесообразны.

4.2 Дополнение

Современная теория ЗИ охватывает не только технические аспекты, но и *организационные*, *психологические*, *юридические* и *социальные* компоненты, делая её междисциплинарной. Использование лингвистических переменных и нечеткой логики особенно актуально в задачах оценки рисков, выбора мер защиты и принятия управленческих решений в условиях неполной информации. Эти методы нашли применение в экспертных системах, системах поддержки принятия решений, а также в автоматизированном управлении безопасностью.

5 Методологический базис ТЗИ

ЛАН

6 Нестрогая математика. Основные положения теории нечетких множеств

Нестрогая математика — это направление, предназначенное для описания, анализа и моделирования систем с высокой степенью неопределённости, основанное на использовании **теории нечетких множеств (НМ)** и **лингвистических переменных**.

6.1 Основные положения теории нечетких множеств

6.1.1 Нечеткое множество

Нечетким множеством $\tilde{A}$ на универсальном множестве X называется множество пар:

$$\tilde{A} = \{(x, \mu_{\tilde{A}}(x)) \mid x \in X\}, \tag{1}$$

где $\mu_{\tilde{A}}(x) : X \to [0, 1]$ — *функция принадлежности*, определяющая степень принадлежности элемента x множеству $\tilde{A}$.

Если $\mu_{\tilde{A}}(x) \in \{0, 1\}$, то множество считается *четким* (обычным).

Пример:

Нечеткое множество, формализующее понятие «приблизительно 5»:

$$\tilde{A} = \{0/2;\ 0{,}4/4;\ 1/5;\ 0{,}8/6;\ 0{,}6/7;\ 0{,}1/10;\ 0/11\}. \tag{2}$$

6.1.2 Характеристики нечеткого множества

- **Носитель (support)**: $\text{supp}(\tilde{A}) = \{x \in X \mid \mu_{\tilde{A}}(x) > 0\}$
- **Высота (height)**: $\text{h}(\tilde{A}) = \sup_{x \in X} \mu_{\tilde{A}}(x)$

6.2 Методы построения функции принадлежности

Функция принадлежности может быть получена следующими методами:

1. **Статистические** (опрос экспертов, анализ термов и т.д.)
2. **Парных сравнений** (по шкалам предпочтений)
3. **Параметрические** (экспоненциальные, нормальные функции)
4. **Интервальные** (на основе экспертных диапазонов)
5. **Метод уровневых множеств**

6.2.1 Метод опроса (МО)

Если n_1 экспертов из m считают, что элемент x принадлежит нечеткому множеству:

$$\mu(x) = \frac{n_1}{m} \tag{3}$$

Пример:
Для элементов $X = \{15, 16, 17, 18, 19\}$ после опроса 7 экспертов получаем:

$$\tilde{A} = \{0/15;\ 0/16;\ 1/17;\ 0{,}86/18;\ 0{,}57/19\} \tag{4}$$

6.3 Лингвистические переменные

Лингвистическая переменная — переменная, значения которой выражаются в терминах естественного языка. Формально задается пятеркой:

$$x = \{x, T(x), X, G, M\}, \tag{5}$$

где: - x — имя переменной; - $T(x)$ — базовое терм-множество (набор лингвистических значений, например: “низкий”, “средний”, “высокий”); - X — универсальное множество; - G — синтаксические правила для образования новых значений (например: «очень»); - M — семантические процедуры, задающие функции принадлежности.

Пример:
Лингвистическая переменная: *“Угроза ИБ”*
Значения: {“Низкая”, “Средняя”, “Высокая”, “Очень высокая”}

6.4 Основные операции над НМ

- **Равенство**: $\mu_{\tilde{A}}(x) = \mu_{\tilde{B}}(x)$
- **Включение**: $\mu_{\tilde{A}}(x) \leq \mu_{\tilde{B}}(x)$
- **Объединение**: $\mu_{\tilde{C}}(x) = \max(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x))$
- **Пересечение**: $\mu_{\tilde{C}}(x) = \min(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x))$
- **Дополнение**: $\mu_{\tilde{A}'}(x) = 1 - \mu_{\tilde{A}}(x)$
- **Декартово произведение**: $\mu_{\tilde{C}}(x, y) = \min(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(y))$

6.5 Дополнение

Нечеткие множества и лингвистические переменные применяются: - в системах поддержки принятия решений; - при оценке рисков информационной безопасности; - в экспертных системах; - для моделирования человече-

ской логики в условиях неопределенности.

Они позволяют *учитывать субъективные, неформализуемые знания* экспертов, формализуя понятия типа «примерно», «больше, чем обычно», «высокий риск», что особенно важно в области **информационной безопасности**, где количественные оценки часто невозможны или неполны.

7 Неформальные методы оценивания

Неформальные методы оценивания применяются при моделировании сложных систем, в которых параметры либо не поддаются точному измерению, либо отсутствует достаточная предыстория их использования. В таких случаях применяются **экспертные оценки (ЭО)** — суждения специалистов, основанные на их знаниях и опыте.

7.0.1 Определение

Методы экспертных оценок — это методы поиска решений сложных, не поддающихся формализации задач, основанные на мнениях компетентных специалистов.

7.0.2 Этапы применения методов ЭО:

1. *Постановка задачи.*
2. *Определение параметров*, подлежащих экспертной оценке.
3. *Выбор способа проведения оценки.*
4. *Подготовка инструкций и бланков.*
5. *Подбор и подготовка экспертов.*
6. *Организация работы экспертов.*
7. *Контроль и начальная обработка оценок.*
8. *Окончательная обработка результатов.*

7.0.3 Способы привлечения экспертов:

- **Простые суждения** (устно/письменно).
- **Интервьюирование** (устное/письменное, диалоговое).
- **Анкетирование** (эксперт заполняет заранее составленные анкеты).

7.0.4 Требования к числу экспертов

Для получения *статистически устойчивых характеристик* параметров требуется репрезентативная выборка — обычно не менее 20 экспертов. Одним из критериев является **коэффициент компетентности (КК)**:

$$KK_i = \frac{KA_i + KO_i}{KA_{max} + KO_{max}}, \tag{6}$$

где: - KA_i — коэффициент аргументированности мнения эксперта, - KO_i — коэффициент осведомленности, - KA_{max}, KO_{max} — максимальные возможные значения.

Группа считается **репрезентативной**, если $0{,}67 \leq M \leq 1$.

7.0.5 Критерии отбора экспертов:

1. Компетентность.
2. Креативность.
3. Антиконформизм.
4. Коллективизм.
5. Конструктивность мышления.
6. Самокритичность.
7. Доступность по времени.
8. Заинтересованность.

7.0.6 Способы организации экспертной работы:

- **Интервьюирование** — позволяет уточнять оценки.
- **Анкетирование** — дает экспертам время на осмысление.
- Возможна *комбинированная схема*: интервью → анкета → итоговое интервью.

7.0.7 Формы выражения оценок:

- **Неявная**:
    - *Линейное ранжирование* — упорядочивание элементов.
    - *Групповое ранжирование* — деление на группы с возможным ранжированием внутри.
- **Явная**:
    - *Лингвистические оценки*.
    - *Количественные оценки*: баллы или значения на непрерывной шкале.

7.0.8 Методы формирования и обработки оценок:

1. *По форме оценки*:
    - Ранжирование.
    - Количественная оценка (баллы, шкала).
    - Парные сравнения.
    - Лингвистические выражения.

2. *По способу формирования*:

- Непосредственный (оценка каждого элемента).
- Сравнительный (оценка через сравнение пар).

7.1 Дополнение

Методы ЭО широко применяются в информационной безопасности, управлении рисками, анализе угроз и проектировании систем, где численные данные отсутствуют или неполны. Современные подходы включают:

- **Метод Делфи** — итеративный анонимный опрос экспертов с последующим уточнением.
- **Функции принадлежности** и **нечеткие множества** — при обработке лингвистических оценок.
- **Интеллектуальные системы** (на базе ИИ) всё чаще используют экспертные базы знаний, построенные с применением ЭО.

Таким образом, неформальные методы позволяют получать релевантные оценки в условиях неопределённости и недостатка данных, дополняя формальные аналитические подходы.

8 Неформальные методы поиска оптимальных решений

Поиск оптимальных решений (ПОР) — это сложные процедуры, которые осуществляются, когда необходимо обеспечить функционирование больших систем.

Неформальные методы ПОР направлены на нахождение эффективных решений при ограниченных ресурсах и неопределённости. Они применяются, когда:

- *формализация задачи затруднена*;
- *полнота или достоверность исходной информации ограничена*;
- *требуется использование человеческой интуиции и опыта*.

Существует два основных направления применения неформальных методов:

1. **Методы сведения задачи к формальной:**
   - **Теория нечетких множеств** — позволяет использовать экспертные оценки с неопределённостью, определять степени принадлежности и сводить задачу к формальной.
   - **Эвристическое программирование** — опирается на формализованные эвристики.
   - **Эволюционное моделирование** — процесс статистического совершенствования алгоритма моделирования.
2. **Методы непосредственного поиска решений:**
   - Включают в себя *экспертные оценки*, *неформально-эвристическое программирование*, *психоинтеллектуальную генерацию*, *управление продуктивным мышлением* и др.
   - Применяются без формального описания задачи, часто опираются на интуитивное или групповое мышление.

8.0.1 Эвристики и эвристическое программирование

Эвристика (эвристическое правило) — это стратегия или приём, найденный на основе опыта, знаний, интуиции или догадки, позволяющий эффективно решать творческие задачи.

Эвристическое программирование — методы, основанные на формализованных эвристиках. Решения не обязательно строго оптимальны, но лучшие среди тех, что были бы получены без эвристик.

Особенности: - поле поиска решений *не фиксировано*, может *сужаться* или *расширяться* в ходе поиска; - при этом достигается *повышение продуктивности поиска* при высокой неопределённости задачи.

8.0.2 Классификация эвристик:

- **Лабиринтные эвристики** — решения ищутся в пространстве возможных путей (лабиринте), человек отсеивает малоперспективные варианты на основе мышления.
- **Концептуальные эвристики** — поиск основан на построении *структурированной модели* проблемы, где выделяются ключевые элементы (концепты), на основе которых строятся связи и обобщения. Решение возникает как *мысленный эксперимент* в рамках построенной модели.

8.0.3 Эволюционное моделирование

Представляет собой развитие статистического моделирования, при котором *алгоритм моделирования сам эволюционирует*.

Стадии:

1. Построение исходной модели процесса.
2. Построение механизма её совершенствования.
3. Определение характеристик на исходной и усовершенствованной модели.
4. Сравнительный анализ и фиксация лучшей модели.

8.0.4 Эргатические системы

Эргатическая система — взаимодействие человека (или коллектива) и машины. Применяются при:

- нестандартных проблемах;
- недостоверности информации;
- необходимости учитывать социально-психологические аспекты.

Особенности:

- высокая гибкость;
- применение нечеткой логики;
- непрерывное совершенствование;
- риск ИБ из-за человеческого фактора.

9 Методы непосредственного поиска

Методы непосредственного поиска относятся ко второму направлению неформальных методов **поиска оптимальных решений (ПОР)** и используются в ситуациях, когда задача не может быть формализована, либо формализация затруднена. Эти методы предполагают применение *интуиции, опыта, продуктивного мышления* и коллективной генерации идей.

Методы непосредственного поиска решений включают:

9.0.1 Экспертные оценки

Заключаются в привлечении специалистов для анализа ситуации и принятия решений на основе их опыта и знаний. Используются при отсутствии объективных данных, при этом возможна формализация оценки в виде *нечетких множеств*.

9.0.2 Неформально-эвристическое программирование

Опирается на использование **эвристик** — стратегий или приёмов, найденных человеком на основе опыта, интуиции, догадок, позволяющих эффективно решать творческие задачи. Не предполагается обязательное формальное описание таких эвристик, как в классическом эвристическом программировании.

9.0.3 Психоинтеллектуальная генерация

Направлена на управление процессом мышления с целью генерации новых решений. Включает техники повышения креативности, усиления интуитивного восприятия и переработки информации. Является индивидуальным методом, опирающимся на особенности восприятия и когнитивные способности человека.

9.0.4 Управление продуктивным мышлением

Заключается в целенаправленном стимулировании процесса мышления, в том числе за счёт постановки провоцирующих вопросов, визуализации проблемной ситуации, декомпозиции задачи. Используется для повышения эффективности поиска решений и генерации идей.

9.0.5 Мозговой штурм

Метод коллективного поиска решений, в основе которого лежит *генерация максимального числа идей без критики на первом этапе*. Основные принципы:

- участие группы экспертов;
- строгое разделение этапов генерации и оценки идей;
- стимулирование любых, в том числе нестандартных, предложений;
- выбор наиболее перспективных решений на втором этапе.

Методы непосредственного поиска применяются в условиях высокой неопределённости, когда невозможно точно задать параметры задачи. Они являются основой многих креативных техник и коллективных форм работы, используемых в анализе угроз информационной безопасности, управлении рисками и проектировании адаптивных ИБ-систем.

9.1 Дополнение

Методы непосредственного поиска находят широкое применение в бизнес-аналитике, ИТ и управлении проектами. Например, **мозговой штурм** используется в разработке стратегий защиты информации, построении сценариев атак и выборе оптимальных архитектур безопасности. **Психоинтеллектуальная генерация** тесно связана с когнитивными науками и теориями принятия решений, включая подходы системного мышления, TRIZ и дизайн-мышление. Эти методы дополняют формальные подходы и обеспечивают необходимую гибкость в условиях неопределённости.

10 Защищаемая информация. Классификация информации по категориям доступа

В соответствии с Федеральным законом, **защищаемой** считается **документированная информация**, т.е. «зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель» (определение 5.1).

Информационные ресурсы классифицируются по категориям доступа на две группы: - **Открытые информационные ресурсы** - **Ресурсы с ограниченным доступом**

К **информации с ограниченным доступом** относят только ту информацию, которая: 1. **Документирована** 2. Имеет **нормативное ограничение доступа**

Информация с ограниченным доступом включает следующие категории:

- **Государственная тайна**
- **Конфиденциальная информация**, включающая:
    - **Персональные данные**
    - **Коммерческая тайна**
    - **Служебная тайна**
    - **Профессиональная тайна**

1. **Государственная тайна** — сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ (определение 5.2).
2. **Коммерческая тайна** — сведения любого характера, имеющие коммерческую ценность, неизвестные третьим лицам и охраняемые режимом конфиденциальности (определение 5.3).
3. **Служебная тайна** — информация, не связанная с извлечением прибыли, но необходимая для обеспечения интересов клиента или внутренней безопасности организации.
4. **Профессиональная тайна** — сведения, не подлежащие разглашению в силу выполнения профессиональных обязанностей (например,

адвокатская, врачебная, нотариальная и др.).

5. **Персональные данные** — любая информация, по которой можно определить конкретного человека (определение 5.4). Включают общие, специальные, биометрические и иные данные.

11 Информация с ограниченным доступом и сведения, которые к ней не относятся

Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года, **информация с ограниченным доступом** — это **документированная информация**, доступ к которой ограничен в соответствии с нормативным актом. Условия отнесения информации к категории ограниченного доступа: 1. Информация должна быть **документирована**. 2. Должен существовать **закон**, *ограничивающий доступ* к ней.

Классификация информации с ограниченным доступом:

1. **Государственная тайна**

2. **Конфиденциальная информация**, в которую входят:
    - **Персональные данные**
    - **Коммерческая тайна**
    - **Служебная тайна**
    - **Профессиональная тайна** (врачебная, адвокатская, нотариальная и др.)
    - Иные конфиденциальные сведения (тайна связи, тайна усыновления, банковская тайна и пр.)

Каждый вид информации с ограниченным доступом защищается соответствующим законодательством (ГК РФ, УК РФ, специализированные законы).

11.1 Сведения, которые не относятся к информации с ограниченным доступом

Некоторые категории информации, даже при наличии ограниченного распространения, **не могут** быть отнесены к информации с ограниченным доступом. Это исключения, установленные законодательством:

1. **Законодательные и нормативные акты**, устанавливающие правовой статус органов власти, организаций и граждан, а также права, свободы и обязанности граждан.
2. **Информация о чрезвычайных ситуациях**, экологическая, метеорологическая, демографическая, санитарно-эпидемиологическая и

иная информация, необходимая для обеспечения безопасности.

3. **Сведения о деятельности органов власти**, включая данные об использовании бюджетных и иных государственных ресурсов, за исключением информации, отнесенной к государственной тайне.
4. **Информация из открытых фондов библиотек, архивов и информационных систем органов власти**, представляющая общественный интерес и необходимая для реализации прав и свобод граждан.

Таким образом, даже при наличии чувствительности или значимости информации, она не может быть признана ограниченной, если прямо отнесена к перечню открытых сведений законом.

12 Понятие государственной тайны. Защита государственной тайны

Государственная тайна — это *защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации*.

12.1 Защита государственной тайны

Защита государственной тайны представляет собой совокупность правовых, организационных и технических мер, направленных на:

- *предотвращение утечки сведений*, составляющих государственную тайну;
- *ограничение круга лиц, имеющих доступ к такой информации*;
- *контроль за порядком ее обработки и хранения*.

Защиту государственной тайны осуществляют:

- Федеральные органы государственной власти,
- Органы государственной безопасности (включая ФСБ России),
- Другие специально уполномоченные государственные органы,
- Организации и учреждения, которым поручено выполнение работ с информацией, составляющей государственную тайну.

12.2 Ответственность за нарушение

Нарушение порядка обращения с государственной тайной влечёт за собой юридическую ответственность, в том числе: - **Уголовную** — за разглашение сведений, составляющих государственную тайну, предусмотрены наказания по Уголовному кодексу РФ (например, лишение свободы, штрафы, лишение права занимать определённые должности); - **Административную** — например, за нарушение правил допуска к сведениям, составляющим государственную тайну; - **Гражданско-правовую** — возмещение убытков при причинении вреда вследствие утечки информации.

13 Коммерческая тайна и её защита

Информация, составляющая коммерческую тайну (секрет производства) — это *сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введён режим коммерческой тайны*.

Коммерческая тайна — это *режим конфиденциальности информации*, позволяющий её обладателю:

- *увеличивать доходы*,
- *избегать неоправданных расходов*,
- *сохранять рыночные позиции*,
- *получать коммерческую выгоду*.

13.1 Условия отнесения информации к коммерческой тайне

1. Информация **документирована**.
2. Имеет **коммерческую ценность** (действительную или потенциальную).
3. Отсутствует **свободный доступ** к ней у третьих лиц на законных основаниях.
4. Введён **режим коммерческой тайны** обладателем информации.

13.2 Защита коммерческой тайны

Юридические меры:

- **Гражданско-правовая защита**: предусмотрена компенсация убытков при незаконном завладении или разглашении.
- **Трудовое законодательство**: работники несут ответственность за разглашение коммерческой тайны, в том числе по контракту.
- **Контроль доступа**: ограничение круга лиц, имеющих доступ, с подписанием обязательств о неразглашении.

Организационные меры:

- Введение внутреннего режима КТ (инструкции, списки защищаемой

информации).

- Назначение ответственных лиц.
- Обучение сотрудников.

Технические меры:

- Применение систем защиты от НСД (несанкционированного доступа).
- Защита каналов связи.
- Применение шифрования.

13.3 Информация, не подлежащая сокрытию

Даже при наличии режима коммерческой тайны, организации не вправе скрывать следующие сведения:

- Учредительные документы, лицензии, патенты.
- Финансово-хозяйственные данные, влияющие на налогообложение.
- Сведения о трудовых условиях, экологии, имуществе, задолженностях.
- Информация, обязательная к раскрытию по закону.

14 Понятие конфиденциальной информации

конфиденциальная информация — это *информация с ограниченным доступом, доступ к которой ограничен в соответствии с законодательством, при этом она не относится к сведениям, составляющим государственную тайну*.

Конфиденциальная информация охватывает широкий спектр сведений, подлежащих защите в силу их чувствительности, коммерческой, служебной или иной специфики. К видам конфиденциальной информации относятся:

- **Персональные данные**
- **Коммерческая тайна**
- **Служебная тайна**
- **Профессиональная тайна**
- **Иные конфиденциальные сведения**, установленные нормативными актами

14.1 Тайна изобретения (изобретателя)

Согласно методическим материалам и **Указу Президента РФ № 188 «Об утверждении перечня сведений конфиденциального характера»**, **сведения о сущности изобретения** до момента официальной публикации патентной информации относятся к **конфиденциальной информации**.

Эти сведения подлежат защите от несанкционированного доступа и могут составлять: - элемент **коммерческой тайны**, если изобретение имеет коммерческую ценность; - часть **служебной тайны**, если создано в рамках выполнения трудовых обязанностей; - охраняемые объекты интеллектуальной собственности до момента регистрации.

Конфиденциальность изобретения обеспечивает: - сохранение приоритета авторства; - возможность дальнейшей патентной охраны; - предотвращение промышленного шпионажа.

14.2 Дополнение

В современной практике до подачи заявки на патент изобретатели и организации заключают соглашения о конфиденциальности (NDA), что позволяет юридически закрепить запрет на разглашение сведений о сущности технического решения. При утечке информации до подачи заявки на патент может быть **утрачена новизна**, и изобретение **не получит правовой охраны**. Именно поэтому конфиденциальность на начальном этапе — критически важна как юридически, так и стратегически.

15 Понятие компьютерных преступлений. Основные виды преступлений, связанных с ИБ

Компьютерное преступление — это *регламентируемое законом общественно опасное деяние, которое совершается с использованием средств вычислительной техники (ВТ)*.

Классификация компьютерных преступлений, предложенная в 1983 году экспертами ОЭСР, включает три основные группы:

1. **Экономические преступления**:
   - кражи программ, услуг или машинного времени;
   - мошенничество с использованием ПК;
   - экономический шпионаж.

   Основной мотив – корысть.
2. **Преступления против личных прав и частной сферы**:
   - незаконный сбор или разглашение персональных данных;
   - получение информации о частных расходах;
   - нарушение банковской или врачебной тайны.
3. **Преступления против государственных и общественных интересов**:
   - действия, угрожающие госбезопасности и обороноспособности;
   - злоупотребление автоматизированными системами голосования.

К основным видам преступлений, непосредственно связанных с информационной безопасностью, относятся:

1. **Несанкционированный доступ (НСД)** к информации, хранящейся на ПК или в сети:
   - достигается с использованием специального ПО;
   - включает кражу носителей информации или подключение аппаратуры к каналам передачи данных.
2. **Разработка и распространение вредоносного ПО**, включая компьютерные вирусы.
3. **Невнимательность и небрежность** в процессе проектирования, разработки и эксплуатации систем защиты информации (ЗИ).
4. **Внедрение логических бомб** — программных закладок, активиру-

ющихся при наступлении определённых условий.

5. **Подделка информации в информационных системах**:
    - целенаправленное искажение выходных данных;
    - используется в том числе квалифицированными разработчиками с целью сокрытия дефектов.
6. **Хищение программного обеспечения**.
7. **Неправомерная модификация, копирование или удаление** программ и данных.
8. **Неправомерное ознакомление или кража информации** из баз и банков данных.

Знание указанных угроз и методов преступлений способствует формированию эффективных мер предотвращения и обеспечения информационной безопасности.

16 Теория и классификация угроз защите информации

Угроза для информации в автоматизированной системе (АС) — это *возможность возникновения на определённом этапе жизненного цикла АС такого события, результатом которого могут быть нежелательные воздействия на информацию*:

- *нарушение (или опасность нарушения) физической целостности или логической структуры*;
- *несанкционированная модификация (или опасность такой модификации)*;
- *несанкционированное получение (или опасность такого получения)*;
- *несанкционированное тиражирование информации*.

Для системного анализа угроз используется классификация по ряду параметров, отражённая в таблице 6.1.

Таблица. Системная классификация угроз информации

Параметры классификации	Значения параметров	Содержание значения критерия
Виды угроз		
	Физической целостности	Уничтожение, искажение информации
	Структуры	Искажение структуры информации
	Содержания	Несанкционированная модификация
	Конфиденциальности	Несанкционированное получение
	Права собственности	Присвоение чужого права
Природа происхождения		
	Случайная	Отказы, сбои, ошибки, стихийные бедствия, побочные влияния

Параметры классификации	Значения параметров	Содержание значения критерия
	Преднамеренная	Злоумышленные действия людей
Предпосылки появления		
	Объективные	Количественная или качественная недостаточность элементов системы
	Субъективные	Разведорганы, промышленный шпионаж, уголовные элементы, недобросовестные сотрудники
Источники угроз		
	Люди	Посторонние лица, пользователи, персонал
	Технические устройства	Устройства регистрации, передачи, хранения, переработки, выдачи информации
	Модели, алгоритмы, программы	Общего назначения, прикладные, вспомогательные
	Технологические схемы	Ручные, интерактивные, внутримашинные, сетевые
	Внешняя среда	Состояние атмосферы, побочные шумы, побочные сигналы

16.1 Дополнение

Современные подходы к анализу угроз включают построение **моделей угроз**, которые учитывают уязвимости, активы и потенциальных нарушите-

лей. Расширенные классификации могут включать *вектор атаки*, *мотив злоумышленника* и *потенциальные последствия*. Используются стандарты, такие как ISO/IEC 27005 и методологии STRIDE, DREAD, MITRE ATT&CK.

17 Предпосылки угроз ИБ: объективные и субъективные

Предпосылки появления угроз информационной безопасности (ИБ) — это *факторы, наличие которых способствует возникновению угроз на различных этапах функционирования автоматизированной системы (АС)*.

Предпосылки подразделяются на **объективные** и **субъективные**.

17.0.1 Объективные предпосылки — обусловлены техническими или организационными недостатками системы:

- **Количественная недостаточность элементов системы** — *физическая нехватка ресурсов*, приводящая к перегрузке или сбоям при обработке данных.
- **Качественная недостаточность элементов системы** — *несовершенство конструкции*, допускающее возможность воздействия на информацию (в том числе непреднамеренного).

17.0.2 Субъективные предпосылки — связаны с деятельностью людей, сознательно или по неосторожности создающих угрозы:

- **Разведорганы иностранных государств** — организованная деятельность по сбору защищаемой информации, включая агентурную, радио-, радиотехническую и космическую разведку.
- **Промышленный шпионаж** — скрытая деятельность коммерческих структур по получению конфиденциальной информации для извлечения выгоды.
- **Уголовные элементы** — действия, совершаемые в целях наживы или в интересах третьих лиц.
- **Недобросовестные сотрудники** — хищение, уничтожение или несанкционированное копирование информации изнутри организации по личным мотивам.

Фрагмент таблицы. Предпосылки появления угроз ИБ

Параметры классификации	Значения параметров	Содержание значения критерия
Предпосылки появления		

Параметры классификации	Значения параметров	Содержание значения критерия
	Объективные	Количественная недостаточность элементов системы, Качественная недостаточность элементов системы
	Субъективные	Разведорганы иностранных государств, Промышленный шпионаж, Уголовные элемен-ты,Недобросовестные сотрудники

17.1 Дополнение

В рамках анализа рисков ИБ, выявление и устранение **объективных предпосылок** часто реализуется путём повышения отказоустойчивости и надёжности архитектуры, в то время как **субъективные предпосылки** требуют применения организационных мер: проверки персонала, контроля доступа, мониторинга поведения и внедрения политики безопасности.

18 Классификация угроз по происхождению

Происхождение угроз — это *признак классификации, отражающий характер условий, при которых возникает угроза для информации в автоматизированной системе (АС)*. По этому признаку выделяют два основных класса угроз: **случайные** и **преднамеренные**.

18.0.1 Случайные угрозы — возникают *непреднамеренно, без участия воли человека*, вследствие спонтанных обстоятельств, сопровождающих функционирование АС. Включают:

- **Отказ** — *нарушение работоспособности элемента системы*, приводящее к невозможности выполнения его основных функций.
- **Сбой** — *временное нарушение работоспособности элемента*, вызывающее некорректное выполнение функций.
- **Ошибка** — *разовое или систематическое неправильное выполнение функций*, связанное с состоянием элемента.
- **Стихийные бедствия** — *природные катаклизмы*, оказывающие влияние на информационные ресурсы (пожары, наводнения, землетрясения и т.п.).
- **Побочные влияния** — *внутренние или внешние воздействия*, отрицательно влияющие на компоненты системы (например, электромагнитные помехи, перепады температуры).

18.0.2 Преднамеренные угрозы — это *злоумышленные действия людей*, направленные на нанесение вреда информационным ресурсам, часто с целью получения выгоды или нарушения функционирования системы. Примеры:

- вредоносные действия со стороны инсайдеров;
- внешние кибератаки;
- внедрение вредоносного программного обеспечения;
- подделка или уничтожение информации.

Фрагмент таблицы. Классификация угроз по происхождению

Параметры классификации	Значения параметров	Содержание значения критерия
Природа происхождения		
	Случайная	Отказы, сбои, ошибки, стихийные бедствия, побочные влияния
	Преднамеренная	Злоумышленные действия людей

18.1 Дополнение

В современных системах особую опасность представляют *гибридные угрозы*, сочетающие как случайные факторы (например, ошибки проектирования), так и преднамеренные действия (внедрение вредоносного кода). Это требует комплексного подхода к защите, включающего технические средства, обучение персонала и постоянный мониторинг поведения системы.

19 Классификация угроз по типам воздействия

Тип воздействия угрозы — это *характер нежелательного влияния на информацию или её носители*, оказываемого в результате реализации угрозы в автоматизированной системе (АС). Данный параметр определяет *целевая направленность* мер защиты информации.

В соответствии с системной классификацией, выделяют следующие **виды угроз по типу воздействия**:

19.0.1 Угрозы физической целостности

- *Воздействие*: уничтожение или искажение физического носителя информации.
- *Примеры*: разрушение дисков, повреждение оборудования.

19.0.2 Угрозы структуры информации

- *Воздействие*: искажение логической структуры данных, что приводит к их недоступности или искажению при обработке.
- *Примеры*: нарушение форматов хранения, нарушение связей в базах данных.

19.0.3 Угрозы содержания информации

- *Воздействие*: несанкционированная модификация содержимого данных.
- *Примеры*: изменение параметров в БД, подмена выходной информации.

19.0.4 Угрозы конфиденциальности

- *Воздействие*: несанкционированное получение защищённой информации.
- *Примеры*: утечка персональных данных, промышленная разведка.

19.0.5 Угрозы прав собственности

- *Воздействие*: присвоение или неправомерное использование авторских и имущественных прав на информацию.
- *Примеры*: кража программного обеспечения, незаконное копирование данных.

Фрагмент таблицы. Классификация угроз по типам воздействия

Параметры классификации	Значения параметров	Содержание значения критерия
Виды угроз		
	Физической целостности	Уничтожение, искажение
	Структуры	Искажение логической структуры информации
	Содержания	Несанкционированная модификация
	Конфиденциальности	Несанкционированное получение информации
	Права собственности	Присвоение чужого права

19.1 Дополнение

Анализ угроз по типу воздействия позволяет сформировать **направленные механизмы защиты**, например: - *контроль целостности* — с использованием хеш-функций и цифровых подписей; - *защита конфиденциальности* — посредством шифрования и контроля доступа; - *обеспечение авторского права* — через лицензирование и цифровую маркировку контента.

Такой подход лежит в основе современных стандартов ИБ, включая ISO/IEC 27001 и ГОСТ Р 57580.

20 Вредоносные программы. Классификация, особенности и способы маскировки в среде

Вредоносные программы — это совокупность программных средств, реализующих **разрушающее программное воздействие**, то есть такой программный код или его части, с помощью которых осуществляется угроза хотя бы одной из характеристик безопасности компонентов компьютерной системы (КС): *конфиденциальности*, *целостности* или *доступности*.

20.1 Классификация

К вредоносным программам относятся следующие группы:

- **крекеры** — программы для взлома защиты программного обеспечения;
- **компьютерные вирусы** — *самораспространяющиеся* программы, модифицирующие другие объекты;
- **логические бомбы** — код, активизирующийся при наступлении определённого события;
- **программы раскрытия паролей** — средства перехвата или подбора паролей;
- **репликаторы** — программы, создающие собственные копии;
- **сетевые программные анализаторы** — утилиты, перехватывающие сетевой трафик;
- **суперзаппинговые утилиты** — инструменты низкоуровневого доступа к данным;
- **тайные хода и лазейки** — механизмы обхода стандартной авторизации;
- **троянские кони** — программы, маскирующиеся под легитимные, но выполняющие вредоносные действия.

Некоторые из них могут быть реализованы как **программные закладки** (жучки), внедрённые в существующие легитимные программы, например — в командный процессор операционной системы. Эти закладки могут, например, сохранять вводимые с клавиатуры пароли в помеченные как сбойные секторы диска, нарушая *конфиденциальность* и *целостность* данных.

20.2 Отличие от вирусов

Вирус — это **программа**, способная к **многократному самопроизвольному созданию своего тела**, которая модифицирует (заражает) другие объекты, чтобы получить управление и выполнять разрушительные действия. Это делает вирусы *самораспространяющимися* вредоносными программами.

Ключевое отличие вирусов от других вредоносных программ заключается в их способности к *самораспространению* и заражению других объектов. Вредоносные программы в целом не обязательно обладают этим свойством.

20.3 Способы маскировки

По способу маскировки в среде вредоносные программы, в частности вирусы, делятся на:

- **видимые** — легко обнаруживаются с помощью стандартных средств (например, изменение размера файла, наличие сигнатуры);
- **невидимые** (стелс-вирусы) — используют специальные алгоритмы сокрытия, например, подмену модифицированных участков на оригинальные при обращении системы, что делает невозможным их обнаружение с помощью обычных системных команд или редакторов.

Невидимость и *маскировка* являются важной характеристикой вредоносных программ, особенно опасных в условиях отсутствия специализированных средств защиты.

20.4 Дополнение

Современные вредоносные программы нередко сочетают функции нескольких типов, например, **троянский вирус** может одновременно быть *полиморфным*, *резидентным* и использовать *стелс-технологии*. Маскировка осуществляется не только технически, но и *социальной инженерией* — через фишинг, поддельные обновления и т.д.

21 Классификация вирусов по инфицируемым объектам

Классификация вирусов по **инфицированным объектам** отражает, какие компоненты компьютерной системы подвергаются заражению вирусом. Этот признак важен для определения векторов заражения и построения эффективных защитных мер.

Согласно методике, вирусы делятся на следующие группы:

21.0.1 Файловые вирусы

Файловые вирусы размещаются в файлах различных форматов, таких как: - COM - EXE - SYS - DOC и др.

Особенности: - Инициализируются при обращении к заражённому файлу. - Часто внедряются в начало, конец или внутреннюю часть файла. - При заражении могут увеличивать размер файла или повреждать его структуру в зависимости от способа размещения (включающие или перекрывающие вирусы).

21.0.2 Загрузочные вирусы

Загрузочные вирусы располагаются в: - Boot-секторе дискет - Главной загрузочной записи (MBR) жёсткого диска

Особенности: - Активизируются при начальной загрузке операционной системы. - Могут быть особенно опасны, поскольку перехватывают управление до запуска ОС, затрудняя их обнаружение и удаление.

21.0.3 Файлово-загрузочные вирусы

Файлово-загрузочные вирусы объединяют свойства двух предыдущих категорий: - Инфицируют как исполняемые файлы, так и загрузочные сектора. - Отличаются сложной логикой и высокой устойчивостью.

Особенности: - Труднее обнаруживаются и удаляются. - Способны действовать на уровне системной загрузки и прикладного ПО.

21.1 Дополнение

Современные вирусы могут использовать *мультивекторные* подходы, заражая не только традиционные объекты (файлы и загрузчики), но и: - скрипты в веб-страницах, - документы с макросами (макровирусы), - модули автозагрузки в реестре, - сетевые компоненты и даже BIOS/UEFI.

Это требует от антивирусных решений комплексного подхода: скани-

рования всех возможных точек заражения и анализа поведения программ в системе.

22 Классификация вирусов по способу инфицирования и способу размещения

Для эффективной защиты от вредоносного кода важно учитывать *механизмы заражения* и *структурные особенности* взаимодействия вирусов с объектами. В связи с этим проводится классификация вирусов по **способу инфицирования объекта** и **способу размещения в инфицируемом объекте**.

22.1 По способу инфицирования объекта

Выделяются две основные категории:

22.1.1 Резидентные вирусы

Резидентные вирусы после запуска оставляют свою часть в оперативной памяти. Эта часть:

- перехватывает системные обращения к объектам (файлам, загрузочным секторам),
- осуществляет заражение других объектов,
- остаётся активной до выключения или перезагрузки компьютера.

Преимущество для вируса — возможность непрерывного заражения новых объектов без повторного запуска вируса.

22.1.2 Нерезидентные вирусы

Нерезидентные вирусы активны только в момент исполнения заражённого объекта:

- не заражают память,
- не способны самостоятельно распространяться после завершения текущей сессии.

Преимущество для антивирусов — меньшая устойчивость вируса и возможность локализации.

22.2 По способу размещения в инфицируемом объекте

Классификация по размещению определяет, каким образом вирус внедряется в объект:

22.2.1 Сопровождающие вирусы

Редкая разновидность, при которой заражение происходит *косвенно*:

- создаётся файл с расширением `.COM` с тем же именем, что и существующий `.EXE`-файл,
- при запуске по имени система сначала активирует `.COM`-файл (вирус),
- вирус затем запускает исходный `.EXE`-файл.

22.2.2 Включающие вирусы

Такие вирусы внедряются непосредственно в тело файла:

- в начало, конец или внутреннюю часть,
- при этом файл остаётся работоспособным, но увеличивается в размере,
- инфицируемый объект *не повреждается*.

Это наиболее распространённая форма файловых вирусов.

22.2.3 Перекрывающие вирусы

Наиболее разрушительные вирусы, которые:

- перезаписывают часть или весь код объекта,
- уничтожают оригинальное содержимое,
- делают объект *непригодным к восстановлению*.

Инфицированные таким способом файлы, как правило, подлежат удалению.

22.3 Дополнение

Современные вирусы могут динамически менять способ инфицирования и размещения, например: - устанавливать резидентные модули в системные службы, - внедряться в скрипты автозагрузки, - использовать методы DLL-инъекций.

Кроме того, перекрывающие вирусы всё чаще применяются в *вымогателях (ransomware)*, когда вместо перезаписи происходит шифрование содержимого, делающее объект недоступным без ключа дешифрации.

23 Классификация вирусов по разрушающему воздействию, по способности к изменению и по типу кода

Классификация вирусов по *разрушающему воздействию*, *способности к изменению* и *типу кода* позволяет определить уровень опасности, сложность обнаружения и способы функционирования вируса. Эти признаки особенно важны при проектировании средств антивирусной защиты.

23.1 По разрушающему воздействию

Критерий отражает степень угрозы, которую вирус представляет для компонентов компьютерной системы. Выделяются следующие категории:

23.1.1 Безвредные

- Не наносят прямого вреда.
- Занимают дисковое пространство и оперативную память (особенно резидентные).
- Могут быть потенциально опасными при изменении среды исполнения.

23.1.2 Неопасные

- Вызывают несущественные эффекты (звуковые/графические).
- Также потребляют ресурсы системы.
- Не разрушают данные или программы.

23.1.3 Опасные

- Могут вызывать сбои в работе системы.
- Модифицируют или повреждают данные.
- Значительно влияют на стабильность и безопасность работы.

23.1.4 Особо опасные

- Уничтожают программы, данные, записи на дисках.
- Приводят к невозвратимым утратам и серьёзным отказам работы системы.

23.2 По способности к изменению

Этот признак определяет устойчивость вируса к обнаружению и его способность маскироваться:

23.2.1 Сигнатурные

- Содержат **неизменяемую часть кода (сигнатуру)**.
- Легко обнаруживаются по этой сигнатуре с помощью антивирусных баз.

23.2.2 Полиморфные

- Не имеют постоянной сигнатуры.
- Каждая копия вируса отличается от предыдущей.
- Изменение достигается:
    - шифрованием тела (обычно с использованием XOR),
    - изменением шифрующей подпрограммы.
- Часто используют стелс-технологии, что делает их обнаружение особенно затруднительным.

23.3 По типу кода

Определяет уровень взаимодействия вируса с архитектурой и средствами исполнения:

23.3.1 Микрокодируемые

- Представлены в виде **бинарного исполняемого кода**.
- Создаются компиляторами.
- Подсоединяются к инфицируемым объектам напрямую.

23.3.2 Макрокодируемые

- Состоят из **последовательностей макрокоманд**.
- Обрабатываются интерпретаторами макрокода (например, в MS Word).
- Часто скрыты в документах (DOC и других), созданных приложениями с поддержкой макросов.

23.4 Дополнение

Полиморфизм и макрокод активно используются в современных кибератаках. Макровирусы особенно актуальны при атаке через электронную почту или документы. Полиморфные вирусы требуют от антивирусов применения эвристических и поведенческих методов анализа, поскольку классическое сигнатурное сканирование становится неэффективным.

24 Методы защиты информации и соответствующие им средства защиты. Примеры

Создание эффективной системы защиты информации требует применения *комплекса методов*, каждый из которых направлен на противодействие определённому классу угроз. Эти методы реализуются с помощью соответствующих **средств защиты информации (СрЗИ)**. Ниже приведены основные методы и средства защиты информации согласно теоретическим положениям.

24.0.1 Препятствие

Определение 8.1. Препятствие — метод создания преграды на пути злоумышленника к защищаемой информационной системе (ИС) и информации, хранящейся в ней.

Средства реализации:

- **Аппаратные и программно-аппаратные средства**, такие как:
- турникеты, шлагбаумы;
- замки, бронированные двери;
- системы охранной сигнализации;
- устройства видеонаблюдения.

24.0.2 Управление доступом

Определение 8.2. Управление доступом — метод регулирования использования всех ресурсов ИС, включая базы данных, программное и техническое обеспечение.

Основные функции:

- идентификация и аутентификация;
- проверка полномочий;
- протоколирование действий;
- реагирование на НСД.

Средства реализации:

- **Программные:** системы управления учетными записями, политики безопасности ОС;
- **Программно-аппаратные: СКУД** (системы контроля и управления доступом);
- **Аппаратные:** биометрические сканеры, электронные ключи.

24.0.3 Маскировка

Определение 8.3. Маскировка — метод сокрытия информации и самого факта её обработки, хранения или передачи.

Средства реализации:

- **Программные и программно-аппаратные средства**, например:
- системы криптографической защиты (шифровальщики, Криптон, Тессера);
- **стеганографические** средства (внедрение скрытой информации в изображения, звук, HTML-код).

24.0.4 Регламентация

Определение 8.4. Регламентация — метод защиты, при котором устанавливаются условия, минимизирующие риск НСД.

Средства реализации:

- **Организационные, законодательные, программные**, например:
- регламенты времени работы, доступ к устройствам хранения;
- настройка ограничений в программном обеспечении;
- введение режима коммерческой тайны.

24.0.5 Принуждение

Определение 8.5. Принуждение — метод защиты, включающий угрозу ответственности (административной, уголовной и др.) за нарушение норм обращения с конфиденциальной информацией.

Средства реализации:

- **Законодательные**, например:
- **УК РФ ст. 283** — ответственность за разглашение государственной тайны;
- **КоАП РФ ст. 13.12** — ответственность за нарушение условий лицензии в сфере ЗИ.

24.0.6 Побуждение

Определение 8.6. Побуждение — метод, регулирующий соблюдение пользователями моральных и этических норм при обращении с информацией.

Средства реализации:

- **Морально-этические**, например:
- корпоративные кодексы поведения;

- воспитание культуры информационной безопасности.

24.1 Примеры соответствия методов и средств защиты

Метод	Средства
Препятствие	Турникеты, шлагбаумы, замки, сигнализация
Управление доступом	СКУД, биометрические сканеры, Firewalls
Маскировка	Шифровальщики, системы стеганографии
Регламентация	Политики безопасности, приказы, ограничения в ИС
Принуждение	Уголовный и административный кодексы РФ
Побуждение	Корпоративные этические кодексы, внутренние стандарты поведения

25 Средства защиты информации и соответствующие им методы защиты. Примеры

Система защиты информации (СЗИ) — это организованная совокупность **средств, методов и мероприятий**, предусмотренных в автоматизированной системе (АС) для решения задач защиты информации. СЗИ является функционально самостоятельной подсистемой информационной системы (ИС), обеспечивающей её безопасность.

Построение СЗИ основывается на следующих *принципах*: - **Системный подход** — оптимальное сочетание организационных, программных, аппаратных и физических средств, обеспечивающих всестороннюю защиту информации. - **Непрерывное развитие системы** — постоянное совершенствование методов защиты в ответ на изменяющиеся угрозы. - **Минимизация полномочий** — предоставление пользователям только тех прав, которые необходимы для выполнения их обязанностей. - **Полнота контроля и регистрации** — точная идентификация пользователей и протоколирование их действий. - **Надёжность** — устойчивость системы к ошибкам, сбоям, атакам и другим отказам. - **Контроль функционирования** — наличие механизмов самопроверки и оценки работоспособности СЗИ. - **Борьба с вредоносными программами** — наличие встроенных или внешних антивирусных и антишпионских решений. - **Экономическая целесообразность** — соотношение между стоимостью защиты и потенциальным ущербом от реализации угроз.

25.1 Виды обеспечения и соответствующие методы защиты

25.1.1 Правовое обеспечение

Это совокупность **законодательных и нормативных документов**, обязательных для исполнения в рамках системы защиты информации.

- **Методы:** правовое регулирование доступа, ответственности, требований к защите информации.
- **Примеры:** законы о персональных данных, государственные стандарты (например, ГОСТ), внутренние регламенты ИС.

25.1.2 Организационное обеспечение

Реализуется через **структурные единицы**, ответственные за ИБ, такие как службы безопасности, режимные отделы, охрана.

- **Методы:** идентификация, аутентификация, разграничение прав доступа, управление паролями, учёт пользователей, регистрация событий.
- **Примеры:** организация многоуровневой системы допусков, введение режима “чистой комнаты”, ротация паролей, регламентация действий персонала.

25.1.3 Информационное обеспечение

Включает в себя **данные, параметры и показатели**, необходимые для функционирования СЗИ.

- **Методы:** ведение базы данных пользователей, журналов событий, учётных записей, оценка статистики угроз.
- **Примеры:** электронные базы доступа, журналы печати и входов в систему, отчёты о нарушениях.

25.1.4 Техническое (аппаратное) обеспечение

Использование **аппаратных средств защиты информации** и поддержания функционирования СЗИ.

- **Методы:** физическая защита помещений, экранирование, контроль электромагнитных излучений, ограничение физического доступа.
- **Примеры:** системы видеонаблюдения, сигнализация, металлические сейфы, биометрические системы доступа, экранирующие кабели.

25.1.5 Программное обеспечение

Представлено **ПО, направленным на предотвращение, обнаружение и реагирование на угрозы безопасности**.

- **Методы:** криптографическая защита, антивирусная защита, межсетевой экран, IDS/IPS-системы, контроль целостности данных.
- **Примеры:** антивирусы, системы шифрования, системы аудита, средства резервного копирования.

25.1.6 Математическое обеспечение

Использование **математических моделей и методов** для анализа защищённости.

- **Методы:** моделирование угроз, оценка рисков, вычисление зон безопасности.

- **Примеры:** вероятностные модели атак, построение матриц доступа, расчет коэффициентов защищённости.

25.1.7 Лингвистическое обеспечение

Это совокупность **языковых и терминологических средств**, обеспечивающих единообразие в описании СЗИ.

- **Методы:** формализация терминов, унификация инструкций и интерфейсов.
- **Примеры:** стандартизированные руководства пользователя, терминологические словари по ИБ.

25.1.8 Нормативно-методическое обеспечение

Охватывает **методики, инструкции и руководства**, регулирующие процессы защиты информации.

- **Методы:** разработка и внедрение методик оценки защищённости, аудита, реагирования на инциденты.
- **Примеры:** методика классификации информации по уровню конфиденциальности, рекомендации по проведению расследований.

25.2 Признаки защищённой информационной системы

Современная ИС должна обеспечивать: - наличие информации различной степени конфиденциальности; - криптографическую защиту данных при передаче; - иерархичную модель доступа; - управление информационными потоками; - регистрацию попыток НСД и действий пользователей; - обеспечение целостности данных; - восстановление после сбоев; - учёт и физическую защиту носителей; - наличие специализированной службы ИБ.

25.3 Пример: ОС Windows NT

ОС Windows NT активно использовалась как основа для защищённых ИС. В ответ на обнаружение уязвимостей компания Microsoft регулярно выпускала **обновления (hotfixes, service packs)**. Это соответствует принципу *непрерывного развития* СЗИ. ОС включала средства разграничения доступа, регистрацию событий, политики безопасности — всё это примеры программных и организационных методов защиты.

26 Криптографическая защита информации. Понятие. Классификация методов

Криптографическая защита информации (КЗИ) — это один из ключевых механизмов обеспечения конфиденциальности, целостности и подлинности информации. Она реализуется с помощью **криптографических средств**, основанных на преобразовании информации в форму, недоступную для восприятия без наличия специального ключа.

26.0.1 Понятие криптографии

Криптография — это наука и практика **защиты информации путём её преобразования** таким образом, чтобы сделать её содержание недоступным для неавторизованных лиц.

криптография — более широкое понятие, чем шифрование

- **Шифрование** — это **частный случай криптографического преобразования**, направленный на сокрытие содержания информации.
- **Криптография**, кроме шифрования, включает также:
    - **Цифровую подпись** (проверка подлинности);
    - **Хэш-функции** (контроль целостности);
    - **Генераторы случайных чисел** (ключевая основа);
    - **Протоколы аутентификации и распределения ключей**.

26.0.2 Классификация методов криптографической защиты

Криптографические методы делятся по признаку структуры ключей на два основных класса:

26.0.2.1 Симметричные криптографические системы

- Используют **один и тот же ключ** как для шифрования, так и для дешифрования.
- Обладают высокой скоростью работы.
- Требуют **безопасного канала** для обмена ключами.

Примеры:

- **DES (Data Encryption Standard)**

- **ГОСТ 28147-89**

26.0.2.2 Асимметричные криптографические системы

- Используют **пару ключей**: открытый (публичный) и закрытый (секретный).
- Позволяют передавать зашифрованную информацию без предварительного обмена секретными ключами.
- Обычно менее производительны, чем симметричные.

Примеры:

- **RSA**
- **Диффи — Хеллман**
- **Ель-Гамаль**

26.0.3 Практическая реализация

Криптографическая защита реализуется через **аппаратные, программные и программно-аппаратные средства**, построенные на основе криптографических алгоритмов.

Примеры средств:

- **Криптон**
- **Тессера**
- **Клиппер**

27 Симметричные и асимметричные системы шифрования. Особенности. Примеры

Шифрование — ключевой метод криптографической защиты информации, направленный на сокрытие её содержания от неавторизованных лиц. В зависимости от принципа использования ключей, все системы шифрования делятся на два основных класса: **симметричные** и **асимметричные** криптографические системы.

27.0.1 Симметричные криптографические системы

Определение: системы, в которых **один и тот же ключ** используется как для шифрования, так и для расшифровки информации.

Особенности: - Высокая **скорость обработки данных** — подходят для больших объёмов информации. - Основной недостаток — *необходимость безопасной передачи ключа* между участниками. - Уязвимы при компрометации ключа — при его утечке нарушается весь режим конфиденциальности.

Примеры: - **DES (Data Encryption Standard)** — классический блоковый шифр. - **ГОСТ 28147-89** — российский стандарт симметричного шифрования.

27.0.2 Асимметричные криптографические системы

Определение: системы, в которых используются **две ключевые пары**: открытый (public key) для шифрования и закрытый (private key) для дешифрования.

Особенности: - Решают задачу **безопасного обмена ключами**, поскольку открытый ключ может быть известен всем. - Позволяют реализовать **цифровую подпись** и механизмы аутентификации. - Основной недостаток — *низкая производительность* по сравнению с симметричными алгоритмами.

Примеры: - **RSA** — одна из наиболее широко применяемых систем. - **Диффи — Хеллман** — протокол для безопасного распределения ключей. - **Ель-Гамаль** — асимметричный алгоритм на основе дискретного логарифмирования.

27.0.3 Сравнительная таблица

Критерий	Симметричные системы	Асимметричные системы
Количество ключей	Один общий ключ	Пара: открытый и закрытый
Производительность	Высокая	Ниже
Безопасный обмен ключами	Требуется	Не требуется
Область применения	Массовое шифрование	Передача ключей, подпись
Тип алгоритма	Блочный или потоковый	На основе теории чисел

27.1 Дополнение

В современной практике **чаще всего используется гибридный подход**, при котором: - для установления защищённого канала используется **асимметричное шифрование** (например, RSA), - после чего для передачи данных используется **симметричный сеансовый ключ**, обеспечивающий высокую скорость.

Такой подход реализован в популярных криптографических протоколах (например, TLS/SSL), где сочетаются **надёжность асимметрии** и **эффективность симметрии**.

28 Шифр Цезаря и шифр древней Спарты

28.1 Шифр Цезаря

Шифр Цезаря — это метод символьной подстановки, при котором каждая буква исходного текста заменяется на букву, *отстоящую от неё в алфавите* на заданное число позиций (прогон).

Принцип работы: - Формируется таблица из двух строк: - **Первая строка** — символы кириллицы в алфавитном порядке. - **Вторая строка** — те же символы, но со *смещением вправо* на число позиций, равное прогону. - При шифровании каждый символ исходного текста заменяется символом из второй строки, расположенным под соответствующим символом из первой строки. - Для дешифрации используется обратная замена — из второй строки в первую.

Пример:

Исходный текст: **«ВПЕРЕД ТОЛЬКО ВПЕРЕД»**

Прогон: **4**

Таблица (фрагмент):

```
1  А Б В Г Д Е Ж З И ...
2  Д Е Ж З И К Л М Н ...
```

Шифрованный текст: **«ЖУКФКИЦУРЯПУЗФЛХЛК»**

28.2 Шифр древней Спарты

Шифр древней Спарты — это метод, основанный на *матричном преобразовании текста*. Суть заключается в записи текста по *столбцам*, а чтении его *построчно*, с фиксированным числом строк, равным **прогон + 1**.

Алгоритм шифрования: 1. Определяется прогон g. 2. Строится матрица с числом строк $g + 1$. 3. Исходный текст записывается *по столбцам* сверху вниз, затем слева направо. 4. Полученная матрица считывается *построчно* — это и есть шифртекст.

Особенность: при необходимости текст дополняется до кратного $(g+1)$ числу символов.

Пример:

Исходный текст: **«КРИПТОГРАММЫ ДРЕВНИХ ВРЕМЕН»**

Прогон: **3** (значит, 4 строки)

Подсчёт: $25 \to 28$ символов (дополнение до кратного 4), таблица:

1	2	3	4	5	6	7
К	Т	А	Д	Н	Р	Н
Р	О	М	Р	И	Е	-
И	Г	М	Е	Х	М	-
П	Р	Ы	В	В	Е	-

Шифртекст: **КТАДНРНРОМРИЕ-ИГМЕХМ-ПРЫВВЕ-**

28.3 Вывод

Оба метода относятся к *классическим шифрам*, однако: - **Шифр Цезаря** основан на *моноалфавитной подстановке* и отличается простотой. - **Шифр Спарты** использует *матричную перестановку*, устойчивее к простому анализу частот.

28.4 Дополнение

- Шифр Цезаря легко вскрывается *перебором* всех возможных прогонов, особенно на малом алфавите.
- Шифр Спарты — пример *транспозиционного* шифра. Принцип аналогичен современному шифрованию с использованием блочных перестановок.
- В современных условиях данные методы используются *в учебных целях*, для демонстрации базовых принципов криптографии.

29 Шифр: “одиночная перестановка по ключевому слову”. Алгоритм двойной перестановки

29.1 Одиночная перестановка по ключевому слову

Одиночная перестановка — это метод транспозиционного шифрования, при котором символы исходного текста *переставляются* на основе порядка букв в ключевом слове.

29.1.1 Алгоритм:

1. **Выбор параметров**:
    - Задаётся **ключевое слово**.
    - Определяется **число строк** в таблице (фиксированное).
2. **Формирование таблицы**:
    - Исходный текст записывается в таблицу **построчно по столбцам**, то есть символы записываются сверху вниз, переходя к следующему столбцу после заполнения предыдущего.
    - В **нулевую строку** таблицы записывается ключевое слово. Если его длина меньше числа столбцов, оно **повторяется циклически**.
3. **Упорядочивание столбцов**:
    - Столбцы сортируются **по алфавиту ключевого слова** (с учётом повторов — одинаковые буквы нумеруются слева направо).
    - Меняется порядок следования столбцов, содержимое остаётся прежним.
4. **Шифрование**:
    - Зашифрованный текст получается путём **построчного** считывания символов **из упорядоченной таблицы**.

29.2 Двойная перестановка

Двойная перестановка — усложнённая версия одиночной, в которой *перестановка производится дважды*: сначала по столбцам, затем по строкам.

29.2.1 Алгоритм:

1. **Выбор параметров**:
    - Определяется **ключевое слово**, а также **размерность таблицы** (число строк и столбцов).

    - Ключевое слово используется как для столбцов, так и для строк. При необходимости **повторяется** до нужной длины.
2. **Формирование таблицы**:
    - Исходный текст записывается **внутрь таблицы** построчно.
    - В **нулевую строку** и **нулевой столбец** таблицы вписывается ключевое слово.
3. **Сортировка**:
    - Сначала **столбцы сортируются** в алфавитном порядке по символам в нулевой строке.
    - Затем **строки сортируются** по символам в нулевом столбце.
4. **Шифрование**:
    - Шифртекст извлекается **построчно** из преобразованной таблицы.

29.3 Вывод

- *Одиночная перестановка* применяется только к **столбцам**, давая умеренную стойкость.
- *Двойная перестановка* работает и со **строками, и со столбцами**, что значительно усложняет анализ и повышает криптостойкость.

29.4 Дополнение

- Обе схемы относятся к классу **транспозиционных шифров** — шифров, не изменяющих символов, но меняющих их порядок.
- При достаточной длине ключа и добавлении случайности (например, в виде заполнителей), такие схемы могут быть устойчивы к простому частотному анализу.
- Двойная перестановка применялась в реальных военных шифрах до середины XX века (например, в шифре ADFGVX).

30 Перемешивание исходного текста с использованием магического квадрата. Шифр многоалфавитной замены

30.1 Перемешивание с использованием магического квадрата

Магический квадрат — это квадратная таблица, заполненная числами так, что *суммы чисел по всем строкам, столбцам и диагоналям одинаковы*. В криптографии он используется для *перестановки символов текста*.

30.1.1 Алгоритм:

1. **Подготовка**:
    - Выбирается магический квадрат фиксированного размера.
    - Определяется число ячеек в квадрате (например, $6 \times 6 = 36$).
2. **Запись текста**:
    - Исходный текст **посимвольно вписывается** в ячейки квадрата *в порядке возрастания номеров*, указанных в магическом квадрате.
    - Если текста недостаточно для полного заполнения — добавляются *пустые символы или заглушки*.
    - Если текста слишком много — используется несколько квадратов.
3. **Формирование шифртекста**:
    - После заполнения квадрат читается **построчно**, слева направо и сверху вниз.
    - Итоговая строка и есть шифртекст.

Ключевым элементом стойкости является использование нестандартной последовательности для записи символов — она задаётся структурой магического квадрата.

30.2 Шифр многоалфавитной замены

Шифр многоалфавитной замены — это метод, в котором для шифрования используется *несколько различных алфавитов подстановки*, выбор которых определяется **ключевым словом**.

30.2.1 Алгоритм:

1. **Формирование таблицы**:
    - Создаётся таблица, где:

        - первая строка — алфавит в прямом порядке;
        - каждая последующая — алфавит со *сдвигом вправо* на один символ по сравнению с предыдущей.
    - Такая таблица представляет собой *набор циклических подстановок*, аналогичных шифру Цезаря.
2. **Подготовка ключа**:
    - Ключевое слово записывается под текстом.
    - Если оно короче текста, оно **повторяется циклически**.
3. **Шифрование**:
    - Для каждого символа текста выбирается строка таблицы, соответствующая символу ключа.
    - Затем, по текущему символу текста определяется столбец.
    - Шифрованный символ — это символ на пересечении выбранной строки и столбца.

Таким образом, каждый символ шифруется *по своему алфавиту*, выбор которого определяется ключевым словом. Это обеспечивает стойкость к частотному анализу, поскольку **один и тот же символ** может быть зашифрован **по-разному** в зависимости от позиции в тексте.

30.3 Вывод

- Шифр с магическим квадратом — это метод *перестановки символов* по заранее заданной схеме.
- Шифр многоалфавитной замены — это метод *многократной подстановки*, в котором каждый символ текста шифруется по разному правилу, зависящему от ключа.

30.4 Дополнение

- Перемешивание по магическому квадрату применяется в системах, где важна устойчивость к реконструкции структуры текста.
- Многоалфавитная замена — основа таких исторически значимых шифров, как **шифр Виженера**, и она до сих пор используется как часть более сложных алгоритмов шифрования.

31 Определение и общие принципы построения систем защиты информации

Система защиты информации (СЗИ) — это **организованная совокупность средств, методов и мероприятий**, выделяемых в автоматизированной системе (АС) для решения в ней задач защиты информации. СЗИ представляет собой **функционально самостоятельную подсистему информационной системы (ИС)**.

31.1 Принципы построения систем защиты информации

Создание систем информационной безопасности (СИБ) в ИС основывается на следующих *ключевых принципах*:

1. **Системный подход** — заключается в оптимальном сочетании взаимосвязанных организационных, программных, аппаратных, физических и иных мер, охватывающих все этапы жизненного цикла обработки информации.
2. **Непрерывное развитие** — обусловлено постоянным изменением способов реализации угроз, что требует регулярного совершенствования методов защиты, мониторинга уязвимостей и адаптации системы к новым условиям.
3. **Разделение и минимизация полномочий** — каждому пользователю предоставляется минимум строго определённых прав доступа, необходимых для выполнения служебных обязанностей, что снижает вероятность несанкционированного доступа.
4. **Полнота контроля и регистрации** — все действия пользователей должны быть идентифицированы и протоколированы. Это обеспечивает возможность последующего анализа и расследования инцидентов.
5. **Надёжность системы** — предполагает устойчивость к сбоям, отказам, атакам и ошибкам как со стороны пользователей, так и злоумышленников, без потери уровня защищённости.
6. **Контроль функционирования** — включает внедрение инструментов и методов оценки работоспособности механизмов защиты.
7. **Противодействие вредоносному ПО** — наличие технических и программных средств для выявления и устранения вредоносных про-

грамм.

8. **Экономическая целесообразность** — затраты на СИБ должны быть обоснованы и не превышать потенциальный ущерб от угроз безопасности.

31.2 Основные характеристики современных СЗИ

Современные СЗИ, встроенные в ИС, должны обладать следующими признаками:

- наличие информации различной степени конфиденциальности;
- криптографическая защита передаваемых данных;
- иерархическая система полномочий субъектов доступа;
- управление информационными потоками;
- регистрация попыток несанкционированного доступа и действий пользователей;
- обеспечение целостности программ и данных;
- наличие механизмов восстановления СЗИ после сбоев;
- учёт и контроль использования магнитных носителей;
- физическая защита средств вычислительной техники;
- функционирование службы информационной безопасности.

31.3 Структура и элементы обеспечения СЗИ

Для эффективного функционирования СЗИ должна быть организована система обеспечения, включающая следующие подсистемы:

1. **Правовое обеспечение**

   Включает совокупность законодательных, нормативно-правовых документов, положений, инструкций и руководств, требования которых обязательны к выполнению.

2. **Организационное обеспечение**

   Представляет собой совокупность организационных структур (например, служба безопасности организации), ответственных за реализацию СИБ, включая режимные мероприятия, охрану и распределение ролей.

3. **Информационное обеспечение**

   Включает сведения, показатели и данные, необходимые для функционирования СИБ (например, параметры доступа, учёта, хранения ин-

формации).

4. **Техническое (аппаратное) обеспечение**

   Использование технических средств (СКУД, системы видеонаблюдения, сигнализации и др.) для защиты информации и поддержки работы СИБ.

5. **Программное обеспечение**

   Программы, обеспечивающие:

   - управление доступом;
   - аудит и мониторинг;
   - защиту от НСД и утечек информации;
   - оценку угроз.

6. **Математическое обеспечение**

   Математические методы оценки рисков, расчёта эффективности защиты, определения зон воздействия и моделей злоумышленников.

7. **Лингвистическое обеспечение**

   Совокупность специализированных терминов, классификаторов, командных языков и форм взаимодействия специалистов и пользователей в сфере ИБ.

8. **Нормативно-методическое обеспечение**

   Сюда входят методики, стандарты, регламенты и правила, направленные на реализацию и поддержку защиты информации. Может быть совмещено с правовым обеспечением.

Организационные меры считаются *ведущими*, поскольку определяют общее функционирование всей СЗИ и работу службы безопасности, в составе которой выделяются: - администраторы безопасности, - менеджеры по безопасности, - операторы и технический персонал.защитную деятельность.

32 Типизация систем защиты. Классификация СЗИ при типизации

Типизация — это разработка типовых конструкций или технологических процессов на основе общих для ряда изделий или процессов технических характеристик.

Стандартизация — это процесс установления и применения стандартов, которые определяются как образцы, эталоны, модели, принимаемые за исходные для сопоставления с ними других подобных объектов.

Целью типизации и стандартизации является *разработка, утверждение и повсеместное применение стандартов*. Первый шаг к достижению этой цели — *максимальная типизация основных решений* в области защиты информации.

32.1 Уровни типизации и стандартизации СЗИ

Выделяются три уровня типизации и стандартизации:

32.1.1 Высший уровень — уровень СЗИ в целом

На этом уровне требуется системная **классификация СЗИ** по двум критериям:

- **По уровню обеспечиваемой защиты:**
    - **Системы слабой защиты** — для АСОД с низкой конфиденциальностью информации.
    - **Системы сильной защиты** — для АСОД с умеренными объемами защищаемой информации.
    - **Системы очень сильной защиты** — для АСОД с регулярной обработкой больших объёмов конфиденциальной информации.
    - **Системы особой защиты** — для АСОД, обрабатывающих информацию повышенной секретности.
- **По активности реагирования на НСД:**
    - **Пассивные СЗИ** — не предусматривают ни сигнализации, ни противодействия.
    - **Полуактивные СЗИ** — предусматривают сигнализацию, но не противодействие.
    - **Активные СЗИ** — предусматривают как сигнализацию, так

и воздействие на нарушителя.

Также учитывается соответствие между уровнями защиты и типами активности: в классификационной структуре различают обязательные (О), целесообразные (Ц), допустимые (Д), нецелесообразные (НЦ), недопустимые (НД) сочетания.

Дополнительно при типизации следует учитывать **тип АСОД**: - Персональная ЭВМ - Локальная вычислительная сеть - Слабораспределённая сеть - Региональная вычислительная сеть - Глобальная вычислительная сеть

32.1.2 Средний уровень — уровень компонентов СЗИ

На этом уровне разрабатываются **типовые проекты компонентов СЗИ**, которые могут быть:

- **Структурно ориентированные компоненты**, соответствующие типовым структурным компонентам (ТСК) АСОД и различным уровням защиты.
- **Функционально ориентированные компоненты**, включая:
    - Регулирование доступа (к территории, помещениям, ТС, ПО и данным),
    - Подавление ПЭМИН,
    - Предупреждение наблюдения и подслушивания,
    - Управление СЗ.

Каждый компонент может быть представлен в различных модификациях, соответствующих конкретным ТСК АСОД.

32.1.3 Низший уровень — уровень проектных решений

На этом уровне создаются **типовые проектные решения** по практической реализации средств защиты: - Технические, - Программные, - Организационные, - Криптографические.

Эффективный подход — **семирубежная модель** СЗИ, включающая следующие рубежи: 1. Защита территории; 2. Защита зданий; 3. Защита помещений; 4. Защита информационных ресурсов; 5. Защита внутридомовых линий связи; 6. Защита межзданий на охраняемой территории; 7. Защита линий связи вне охраняемой территории.

Рубеж защиты — это организованная совокупность средств, методов и мероприятий, реализуемых на соответствующем участке для обеспечения

безопасности информации.

33 Стандартизация систем защиты. Уровни стандартизации

Стандартизация — это *процесс установления и применения стандартов*, которые определяются как **образцы, эталоны, модели, принимаемые за исходные для сопоставления с ними других подобных объектов**.
Стандарт как нормативно-технический документ устанавливает *комплекс норм, правил, требований к объекту стандартизации* и утверждается компетентным органом.

Цель стандартизации систем защиты информации (СЗИ) — *обеспечение сопоставимости, совместимости и повторного использования решений защиты*, а также *объективная оценка соответствия уровня защиты нормативным требованиям*. Стандартизация логически связана с типизацией и основывается на ней.

33.1 Уровни стандартизации СЗИ

Различают три уровня стандартизации, соответствующие уровням типизации:

33.1.1 Высший уровень — стандартизация СЗИ в целом

На этом уровне основой служит **системная классификация СЗИ**, включающая:

- **Классификацию по уровню обеспечиваемой защиты**:
    - Системы слабой, сильной, очень сильной и особой защиты.
- **Классификацию по активности реагирования на НСД**:
    - Пассивные, полуактивные и активные СЗИ.
- **Классификацию по типу АСОД**:
    - От персональных ЭВМ до глобальных вычислительных сетей.

Результатом стандартизации на этом уровне являются *обобщённые стандарты на архитектуры СЗИ и требования к их построению*, отражающие особенности категорий защищаемой информации и типов информационных систем.

33.1.2 Средний уровень — стандартизация компонентов СЗИ

На этом уровне стандартизации разрабатываются **типовые проекты компонентов СЗИ**, включающие:

- **Структурно ориентированные компоненты**, соответствующие ти-

повым элементам АСОД (например, сегменты сети, серверные помещения и т.п.).

- **Функционально ориентированные компоненты**, такие как:
    - Контроль доступа (физический и логический),
    - Подавление ПЭМИН,
    - Противодействие технической разведке,
    - Средства управления СЗИ.

Компоненты должны быть аттестованы в качестве стандартных решений и совместимы между собой. Это позволяет собирать СЗИ на основе библиотек сертифицированных компонентов.

33.1.3 Низший уровень — стандартизация проектных решений

Здесь создаются **типовые проектные решения** по реализации средств защиты, в том числе:

- Технических (средства охраны, блокировки, защиты каналов связи),
- Программных (средства контроля доступа, антивирусы, межсетевые экраны),
- Организационных (регламенты, инструкции),
- Криптографических (алгоритмы шифрования, ЭЦП).

Стандарты определяют *состав и параметры средств защиты* для каждого рубежа.

33.2 Дополнение

Современная стандартизация СЗИ развивается в контексте международных и национальных норм, включая ГОСТ Р, СТБ, ISO/IEC 27000 и др. Особое значение имеет стандартизация на среднем уровне, так как именно она обеспечивает *взаимозаменяемость и масштабируемость компонентов*. В условиях быстро меняющихся угроз стандарты позволяют *оперативно обновлять элементы СЗИ без перепроектирования всей системы*.

34 Деление СЗИ по уровню обеспечиваемой безопасности

В рамках типизации и стандартизации систем защиты информации (СЗИ) одним из ключевых критериев классификации является **уровень обеспечиваемой безопасности**. Этот критерий отражает степень защищённости информации в автоматизированных системах обработки данных (АСОД) и лежит в основе построения и выбора соответствующих СЗИ.

Согласно теоретической базе, **все СЗИ целесообразно разделить на четыре категории** по уровню защиты:

34.0.1 Системы слабой защиты

Предназначены для АСОД, в которых обрабатывается информация с **низким уровнем конфиденциальности**.
Такие системы ориентированы на защиту от случайных или неинтенсивных угроз. Они реализуют минимальный набор функций защиты и, как правило, характеризуются низкой стоимостью и простотой реализации.

34.0.2 Системы сильной защиты

Предназначены для АСОД, в которых обрабатывается информация, **подлежащая защите от несанкционированного получения**, однако: - объёмы защищаемой информации **невелики**, - обработка осуществляется **эпизодически**.

Данные системы включают более развитые механизмы защиты, включая контроль доступа, средства регистрации событий и другие базовые функции СЗИ.

34.0.3 Системы очень сильной защиты

Применяются в АСОД, в которых регулярно обрабатываются **большие объёмы конфиденциальной информации**, подлежащей защите.
Такие СЗИ предполагают наличие: - комплексных механизмов разграничения доступа, - средств мониторинга, - защиты каналов связи, - а также организационных и криптографических мер.

34.0.4 Системы особой защиты

Предназначены для АСОД, обрабатывающих **информацию повышенной секретности**.
Это системы максимального уровня защищенности, для которых характер-

ны: - избыточность и резервирование, - активные средства противодействия нарушителям, - многоуровневая система контроля и аудита, - специальные технические средства и криптографическая защита высокого класса.