

МДК 02.01 ПРОГРАММНЫЕ И ПРОГРАММНО- АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

**Бояркин Дмитрий
Владимирович**



Предмет и задачи программно-аппаратной защиты информации. Основные понятия ПАЗИ

Тема 1.1. Предмет и задачи программно-аппаратной защиты информации



План занятия

1. Введение
2. Краткая характеристика дисциплины «Программно-аппаратная защита информации»
3. Место ПАЗИ в системе ИБ
4. Предмет и задачи ПАЗИ
5. Объект ПАЗИ
6. Многоуровневая защита информации



Введение

- Для чего нужны программные и программно-аппаратные средства защиты информации?



1. Краткая характеристика дисциплины «Программно-аппаратная защита информации»

Целями дисциплины «Программно-аппаратная защита информации» являются:

- ❑ формирование у обучающихся знаний об основных программно-аппаратных средствах защиты информации;
- ❑ формирование у обучающихся умений и первоначальных навыков применения программно-аппаратных средств защиты информации.



1. Краткая характеристика дисциплины «Программно-аппаратная защита информации»

Основные задачи дисциплины:

- ❑ подготовить специалистов по программно-аппаратной защите информации в условиях широкого применения современных информационных технологий, четко представляющих ее возможности и ограничения;
- ❑ углубить знания обучающихся по наиболее важным вопросам обеспечения информационной безопасности различных автоматизированных систем.



2. Место ПАЗИ в системе ИБ

В Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г № 149-ФЗ говорится о трех направлениях защиты информации: правовом, организационном и техническом.

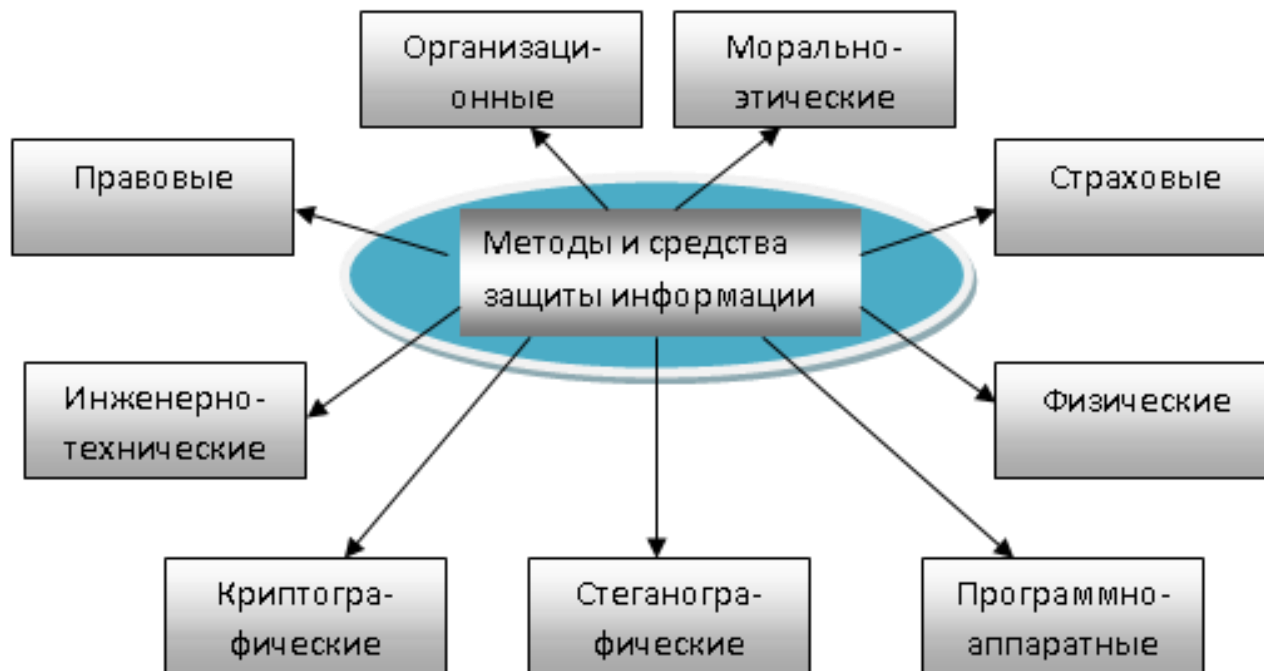


Рис. 1. Методы и средства обеспечения информационной безопасности



- Опрос на определение уровня осведомлённости о ПАЗИ (нужно сделать в сервисе типа menti, который не работает в РФ)



3. Предмет и задачи ПАЗИ

Программно-аппаратная защита информации относится к комплексу мер, которые применяются для обеспечения безопасности информации, используя как программное, так и аппаратное обеспечение.

Основной целью ПАЗИ является предотвращение несанкционированного доступа (НСД), изменения, утечки или уничтожения конфиденциальных данных.



3. Предмет и задачи ПАЗИ

Задачи ПАЗИ могут включать в себя:

- ❑ Аутентификацию и управление доступом:
Обеспечение идентификации и аутентификации пользователей, контроль доступа на основе ролей и разрешений, а также управление привилегиями доступа к информации.
- ❑ Шифрование данных: Применение криптографических алгоритмов для защиты конфиденциальности информации при её передаче или хранении.



3. Предмет и задачи ПАЗИ

Задачи ПАЗИ могут включать в себя:

- ❑ Защиту от вредоносного программного обеспечения: Установка антивирусных программ, брандмауэров и других средств защиты от вредоносных программ, таких как вирусы, троянские программы и шпионское ПО.
- ❑ Мониторинг и обнаружение инцидентов: Реализацию систем мониторинга и обнаружения инцидентов для раннего выявления атак, вторжений или других нарушений безопасности информации.



3. Предмет и задачи ПАЗИ

Задачи ПАЗИ могут включать в себя:

- ❑ Резервное копирование и восстановление данных:
Регулярное создание резервных копий информации и разработка планов восстановления после чрезвычайных ситуаций или инцидентов безопасности.
- ❑ Обучение пользователей: Проведение обучающих программ и информирование пользователей о методах защиты информации, осведомление о возможных угрозах безопасности и правильных методах работы с конфиденциальными данными.



3. Предмет и задачи ПАЗИ

Задачи ПАЗИ могут включать в себя:

- ❑ Тестирование на проникновение: Проведение тестирования на проникновение для оценки уязвимостей системы и выявления слабых мест в механизмах защиты информации.
- ❑ Защита от сетевых атак: Разработка и применение мер безопасности для предотвращения сетевых атак, таких как отказ в обслуживании (DDOS) или фишинг.
- ❑ Межсетевой экран (firewall): Установка и настройка межсетевого экрана для контроля трафика между внутренними и внешними сетями, блокировки нежелательных или потенциально опасных соединений.



3. Предмет и задачи ПАЗИ

Задачи ПАЗИ могут включать в себя:

- Защиту от утечки информации: Реализация мер по предотвращению утечки конфиденциальной информации, таких как контроль использования портативных устройств, систем предупреждения об утечке данных и мониторинг действий пользователей.
- Физическую защиту серверных помещений: Обеспечение безопасности серверных помещений путем контроля доступа, видеонаблюдения, датчиков тревоги и других физических мер защиты.



3. Предмет и задачи ПАЗИ

Задачи ПАЗИ могут включать в себя:

- ❑ Разработку безопасных приложений: Внедрение методов разработки безопасного программного обеспечения, таких как проверка входных данных, предотвращение уязвимостей, аутентификация и шифрование данных.
- ❑ Обеспечение целостности данных: Разработка и применение механизмов обнаружения и защиты от изменения данных без разрешения, например, с использованием хэш-функций и цифровых подписей.



3. Предмет и задачи ПАЗИ

Задачи ПАЗИ могут включать в себя:

Важно отметить, что эти задачи являются лишь общими примерами и могут различаться в зависимости от конкретных требований и контекста организации или системы, которую необходимо защитить.



4. Объект ПАЗИ

Программно-аппаратная защита информации, как и каждая научная дисциплина, имеет свой объект.

В руководящих документах по информационной безопасности Федеральной службы по техническому и экспортному контролю (ФСТЭК) указаны два различающихся между собой класса объектов ПАЗИ:

- средства вычислительной техники (СВТ) и
- автоматизированные системы (АС).



4. Объект ПАЗИ

Под СВТ понимают совокупность программных и аппаратных элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем. К СВТ относят автономные компьютеры, устройства ввода/вывода данных, встроенные и автономные устройства хранения данных, операционные системы ЭВМ, системы управления базами данных (СУБД), прикладное программное обеспечение и пр.

Под автоматизированными системами понимают полнофункциональные системы, предназначенные для обработки данных или для управления. При этом различают два вида автоматизированных систем управления: АСУ организационного типа (предприятием, организацией, министерством и пр.) и АСУ технологическими процессами (производственной линией, станком и пр.).



4. Объект ПАЗИ

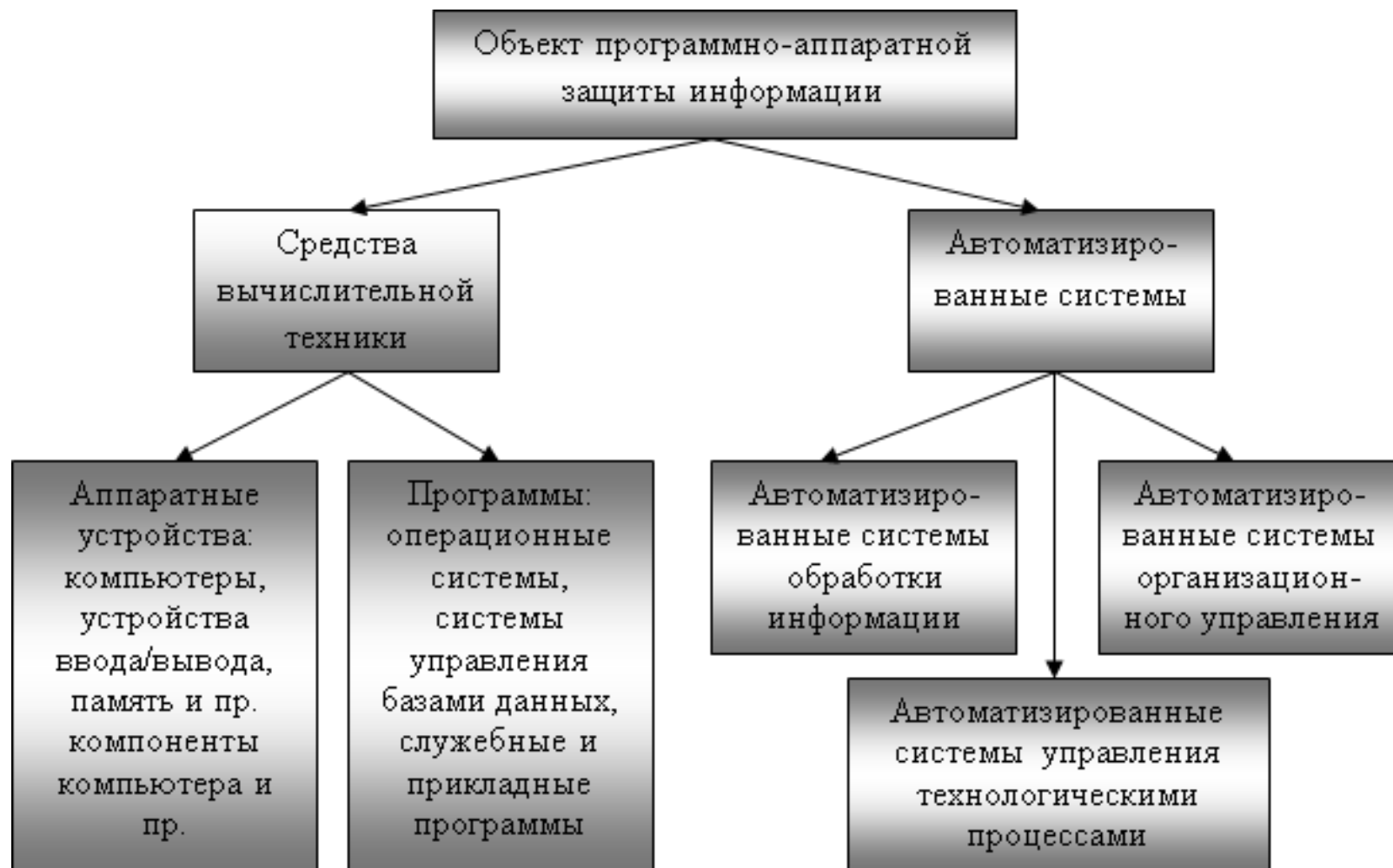


Рис. 2. Структура объекта программно-аппаратной защиты информации



4. Объект ПАЗИ



4. Объект ПАЗИ

Аппаратные средства – это любые электрические, электронные, оптические, лазерные и другие устройства, которые встраиваются в системы для защиты информации (генераторы шума, сетевые фильтры, сканирующие радиоприемники, сканеры отпечатков пальцев).

Программные средства – программное обеспечение для защиты информации (антивирусы, системы обнаружения вторжений, межсетевые экраны и др.)

Программно-аппаратные средства – программно-аппаратные комплексы для защиты информации (средство доверенной загрузки, СОВ, МЭ и тд)



5. Многоуровневая защита информации

Многоуровневая защита или эшелонированная оборона представляет собой иерархически организованный набор уровней защиты информационной системы. Правильный выбор компонент и их правильная настройка на каждом уровне позволяет создать «хорошую» систему защиты информации.

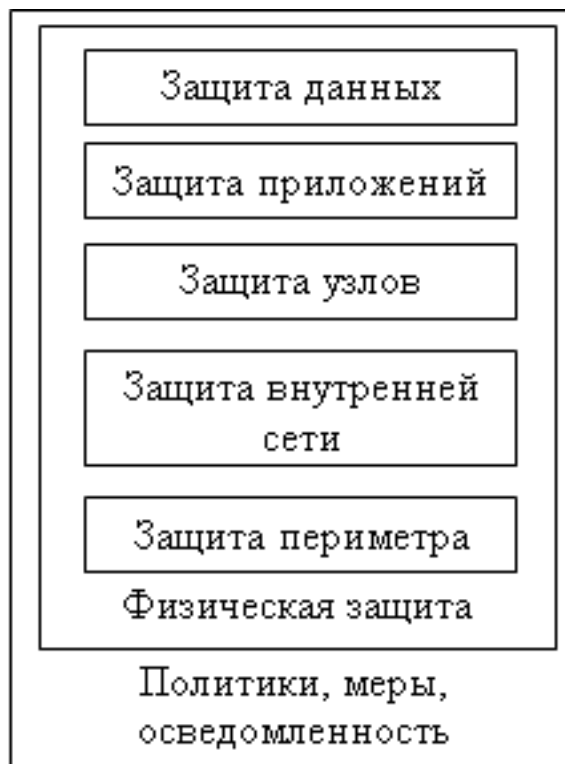


Рис. 3. Модель многоуровневой защиты



5. Многоуровневая защита информации

Политика безопасности описывает все аспекты работы системы с точки зрения информационной безопасности. Уровень политики безопасности является базовым. Он подразумевает наличие документированных организационных мер защиты и порядка информирования о происшествиях, обучение пользователей в области информационной безопасности и т.п. (см. например стандарт ISO/IEC 17799).

Уровень физической защиты включает меры по ограничению физического доступа к ресурсам системы: защита помещений, видеонаблюдение, контроль доступа.



5. Многоуровневая защита информации

Уровень защиты периметра включает меры безопасности в точках входа в защищаемую сеть. Классические средства защиты периметра это межсетевой экран, система обнаружения вторжений средства антивирусной защиты для шлюзов безопасности.

Уровень защиты внутренней сети ведает обеспечением безопасности внутреннего трафика и сетевой инфраструктуры. Это виртуальные локальные сети, протоколы IPSec и т.д. На этом уровне могут быть использованы те же средства, что и средства защиты периметра, например, межсетевые экраны.



5. Многоуровневая защита информации

Уровень защиты узлов защищает от атак на отдельные узлы сети. На этом уровне первоочередное внимание уделяется защите операционной системы: настройкам повышающим безопасность конфигурации (отключению неиспользуемых потенциально опасных служб), организации установки исправлений и обновлений, идентификации и аутентификации пользователей. Важную роль на этом уровне играет антивирусная защита.



5. Многоуровневая защита информации

Уровень защиты приложений отвечает за защиту от атак, направленных на конкретные приложения: почтовые и web серверы, серверы баз данных и пр. Сюда же можно отнести модификацию приложений компьютерными вирусами. Для защиты на этом уровне используются настройки безопасности самих приложений, установка обновлений, антивирусная защита.

Уровень защиты данных определяет порядок защиты обрабатываемых и хранящихся данных от НСД и других угроз. Это может быть шифрование данных при хранении передаче, разграничение доступа к данным средствами файловой системы.



Дополнительно

Вспомните основные понятия ИБ:

- Информационная безопасность
- Защита информации
- Уязвимость и угроза
- Риск ИБ
- Политика ИБ
- Информационная система
- И т.д.

