

Классификация методов и средств ПАЗИ

Тема 1.1. Предмет и задачи программно-аппаратной защиты информации



План занятия

1. Введение
2. Классификация программно-аппаратных средств защиты информации
3. Программно-аппаратные средства защиты информации
4. Программно-аппаратные средства защиты информации (дополнительные)



1. Введение

Известно, что система защиты информации представляет собой взаимоувязанный комплекс правовых, организационных, технических, криптографических, программно-аппаратных, стеганографических, страховых, морально-этических и психологических средств и методов защиты информации.

Причем граница между этими средствами и методами подчас размыта. Поэтому при изучении ПАЗИ необходимо учитывать взаимосвязь различных подсистем с программно-аппаратными средствами.



2. Классификация программно-аппаратных средств защиты информации (ПАСЗИ)

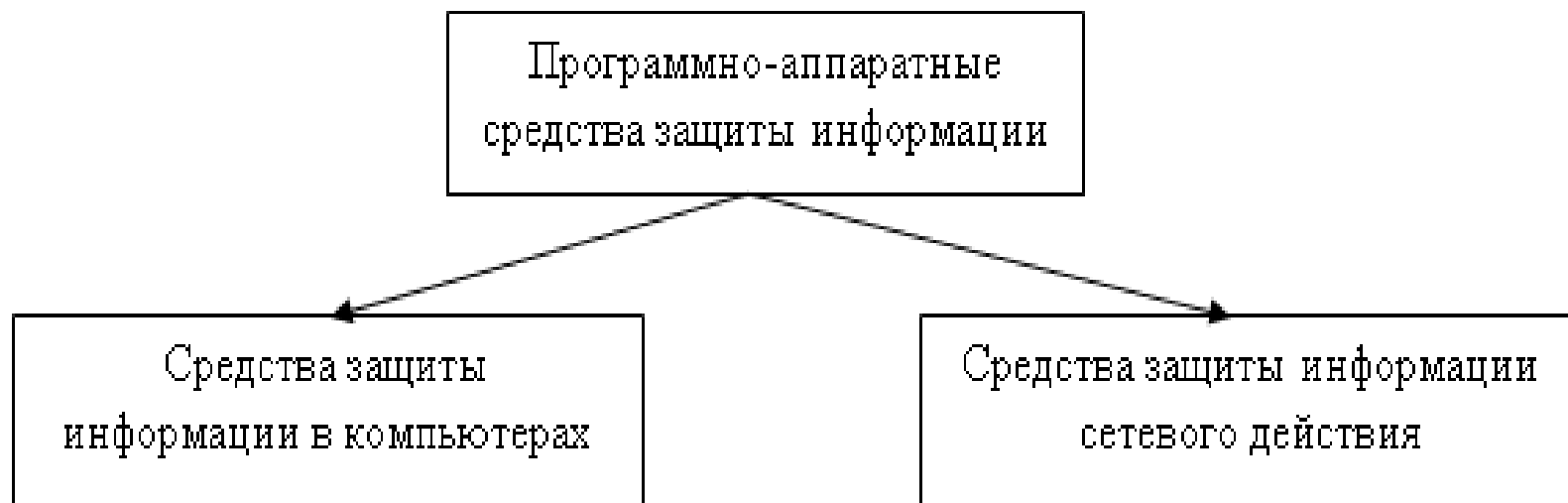


Рис. 1. Классификация программно-аппаратных средств по защищаемым объектам



2. Классификация программно-аппаратных средств защиты информации (ПАСЗИ)

СЗИ, которые чаще всего применяются для защиты информации:

1. средства защиты информации от несанкционированного доступа (СЗИ от НСД);
2. межсетевые экраны;
3. системы обнаружения и предотвращения вторжений;
4. операционные системы для обеспечения защиты информации;
5. СКЗИ (средства криптографической защиты информации);
6. средства защиты электронной подписи;
7. антивирусные средства.



2. Классификация программно-аппаратных средств защиты информации (ПАСЗИ)

СЗИ, которые дополнительно применяются при создании систем обеспечения ИБ:

- 1) межсетевые экраны уровня веб-приложений (Web Application Firewall, WAF);
- 2) универсальные шлюзы безопасности (Unified threat management, UTM);
- 3) межсетевые экраны нового поколения (Next generation firewall, NGFW);
- 4) электронные подписи и инфраструктуру открытых ключей (PKI);
- 5) системы сбора, корреляции и анализа событий ИБ (SIEM);
- 6) системы предотвращения утечек информации (DLP);
- 7) системы защиты среды виртуализации;
- 8) песочницы и honeypots.



3. Программно-аппаратные средства защиты информации

1 - Средства защиты информации от несанкционированного доступа (СЗИ от НСД)

СЗИ от НСД служат для доверенной загрузки операционной системы (ОС), внедрения систем идентификации и аутентификации, а также для разграничения доступа. СЗИ от НСД бывают в программном и программно-аппаратном исполнении.



3. Программно-аппаратные средства защиты информации

1 - Средства защиты информации от несанкционированного доступа (СЗИ от НСД)

СЗИ от НСД включают в себя набор механизмов по защите информации, которые можно разделить на следующие подклассы [30]:

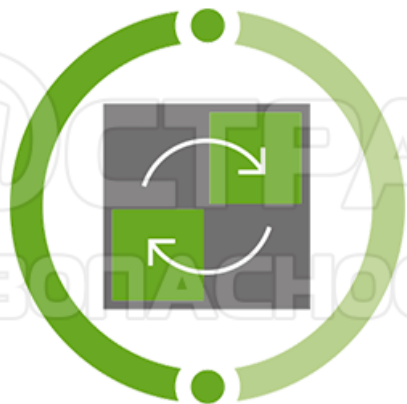
- системы идентификации и аутентификации;
- системы разграничения доступа;
- средства доверенной загрузки;
- аппаратные средства аутентификации и хранения ключевой информации;
- замкнутая программная среда;
- подсистемы регистрации и учета;
- средства контроля съемных машинных носителей информации.



3. Программно-аппаратные средства защиты информации

1 - Средства защиты информации от несанкционированного доступа (СЗИ от НСД)

Примеры:



СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

SECRET NET STUDIO 8.

Максимальная защита



СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

DALLAS LOCK

8.0 - К



3. Программно-аппаратные средства защиты информации

2 - Межсетевые экраны

Межсетевой экран – это СЗИ, с помощью которого организуется процесс контроля и фильтрации проходящего через него трафика в соответствии с определенными правилами. Межсетевые экраны также известны под названиями «брандмауэр» и «файрвол»



3. Программно-аппаратные средства защиты информации

2 - Межсетевые экраны

Основной задачей межсетевого экранирования является фильтрация трафика (на сетевом и транспортном уровне модели OSI) в соответствии с заданными правилами с целью предотвращения несанкционированного доступа путем использования уязвимостей как протоколов модели OSI, так и хостового программного обеспечения.

Межсетевые экраны предоставляют следующий функционал:

- 1) остановка подмены трафика – анализ данных соединений и обнаружение постороннего IP-адреса в процессе обмена;
- 2) защита сети от DoS- и DDoS-атак – определение атакующих IP-адресов и блокирование трафика от них;
- 3) блокирование передачи данных на неизвестный IP-адрес – определение нелегитимных соединений и их блокирование.



3. Программно-аппаратные средства защиты информации

2 - Межсетевые экраны

Примеры:



3. Программно-аппаратные средства защиты информации

3 - Системы обнаружения (предотвращения) вторжений

Система обнаружения вторжений (СОВ, англ. Intrusion Detection System, IDS) – это система, предназначенная для выявления фактов несанкционированного доступа к ИС или СВТ, а также несанкционированного управления ими через сеть.

IDS могут быть программного и программно-аппаратного исполнения.



3. Программно-аппаратные средства защиты информации

3 - Системы обнаружения (предотвращения) вторжений

IDS используются для выявления следующих типов вредоносной активности:

- сетевых атак на уязвимые сервисы;
- атак на повышение привилегий;
- действий вредоносного программного обеспечения и др.

Аналогично межсетевым экранам IDS могут устанавливаться непосредственно на хосте в виде программного обеспечения или на границе сети в программно-аппаратном или виртуальном исполнении (рис. 4).



3. Программно-аппаратные средства защиты информации

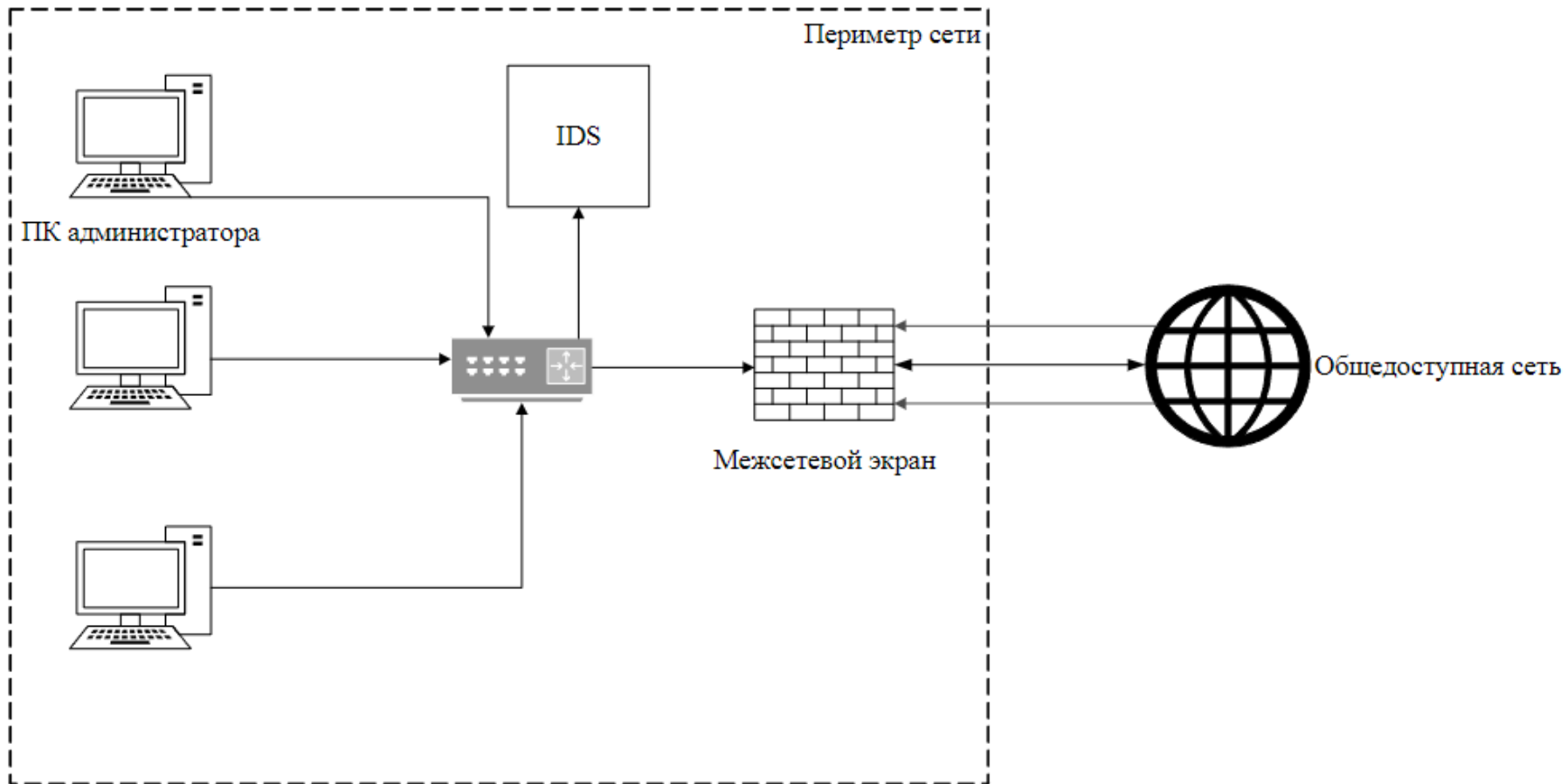


Рис. 4. Установка системы обнаружения вторжений



3. Программно-аппаратные средства защиты информации

3 - Системы обнаружения (предотвращения) вторжений

Примеры



3. Программно-аппаратные средства защиты информации

4 – Операционные системы для обеспечения безопасности

Операционная система специального назначения – ОС, которая имеет встроенные механизмы защиты информации (управление доступом, ограничение программной среды, контроль устройств и др.)

Данные системы широко применяются для защиты гос. тайны, персональных данных, значимых объектов КИИ.



3. Программно-аппаратные средства защиты информации

4 – Операционные системы для обеспечения безопасности

Типы операционных систем

Различают следующие виды операционных систем:

- ОС общего назначения (ОС типа «А») устанавливаются на СВТ общего назначения (ПК, серверы, смартфоны);
- встраиваемые ОС (ОС типа «Б») устанавливаются на специальные технические средства, проектируемые для решения заранее определенных задач;
- ОС реального времени (ОС типа «В») обеспечивают реагирование на события в рамках заранее заданных временных интервалов при заранее заданном уровне функциональности.



3. Программно-аппаратные средства защиты информации

4 – Операционные системы для обеспечения безопасности

Примеры



3. Программно-аппаратные средства защиты информации

5 – СКЗИ (средства криптографической защиты информации)

СКЗИ – это различные программные и программно-аппаратные комплексы, реализующие алгоритмы криптографического преобразования информации.



3. Программно-аппаратные средства защиты информации

Типы средств криптографической защиты информации и средств защиты электронной подписи

Согласно Положению о лицензировании [57] принято различать:

- средства шифрования – аппаратные, программные и программно-аппаратные криптографические СЗИ (например, криптошлюзы и шлюзы безопасности), которые реализуют алгоритмы шифрования информации для ее безопасной передачи по каналам связи, хранения и обработки;
- средства имитозащиты – защищающие информацию от внесения изменений в исходные данные;
- средства электронной подписи (ЭП) – предназначенные для создания и проверки подлинности ЭП, а также выпуска открытых и закрытых ключей;
- средства кодирования – в которых некоторые криптографические преобразования выполняются вручную или специальными автоматизированными решениями;
- средства изготовления ключевых документов.



3. Программно-аппаратные средства защиты информации

5 – СКЗИ (средства криптографической защиты информации)

Примеры



3. Программно-аппаратные средства защиты информации

6 – Средства защиты электронной подписи

Использовать электронную **подпись** не получится без **средств** криптографической **защиты** информации.

ЭП представляет собой информацию в электронной форме, которая присоединена к другой информации в электронной форме или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

ФЗ №63 «Об электронной подписи»



3. Программно-аппаратные средства защиты информации

6 – Средства защиты электронной подписи

1) простая ЭП обеспечивает подтверждение факта формирования ЭП путем использования специальных кодов, паролей или иных средств;

2) усиленная неквалифицированная ЭП обеспечивает определение лица, подписавшего документ, и позволяет обнаружить факт изменения документа после его подписи. Такая ЭП получается в результате криптографического преобразования информации с использованием ключа ЭП;

3) усиленная квалифицированная ЭП также позволяет определить лицо, подписавшее документ, и установить факт изменения документа после его подписания. Такая ЭП соответствует всем требованиям неквалифицированной ЭП, ключ проверки такой подписи указан в квалифицированном сертификате, а средства создания такой подписи соответствуют требованиям закона № 63-ФЗ.



3. Программно-аппаратные средства защиты информации

6 – Средства защиты электронной подписи

Примеры



ViPNet CSP



3. Программно-аппаратные средства защиты информации

7 – Антивирусные средства защиты



4. Программно-аппаратные средства защиты информации (дополнительные)

1 – Межсетевые экраны уровня веб-приложений (WAF)

Межсетевой экран уровня веб-приложений (WAF) – это межсетевой экран, предназначенный для обнаружения и блокирования сетевых атак на веб-приложения.

WAF относится к межсетевым экранам типа «Г». В отличие от классических межсетевых экранов WAF работают на прикладном уровне модели OSI.

WAF является наложенным средством защиты – это означает, что он устанавливается перед основным веб-приложением для анализа трафика, причем как входящего, так и исходящего.



Функционал WAF включает в себя следующее.

1. Сигнатурный анализ для фильтрации трафика. Сигнатурный метод в своей реализации использует словарь вредоносного трафика для сравнения [43]. Если в пришедшем трафике нашлась часть запроса (сигнатура), которая соответствует вредоносному трафику, то WAF блокирует этот запрос.

2. Репутационный фильтр IP-адресов. Метод основан на белых и черных списках IP-адресов и доменов. Ссылаясь на эти списки, WAF оценивает входящие запросы [42].

3. Поведенческий анализ строится на машинном обучении. Это позволяет обнаружить аномалии в поведении на глубоких уровнях понимания. Такой механизм может обучаться как с учителем, так и без учителя на идентификаторах доступа. Входящими параметрами могут служить идентификаторы доступа, такие как HTTP-параметры, идентификатор ресурса (URL, URN), идентификатор сессии [41]. Таким образом создается эталонная математическая модель допустимых идентификаторов доступа. При несовпадении с этой моделью очередной запрос будет заблокирован [44]. Это позволяет отражать как известные атаки, так и атаки нулевого дня [42].

4. Защита от DoS-атак. Кроме защиты информации WAF могут предоставлять функции по ее доступности, борясь с DoS-атаками. При обнаружении атаки ограничиваются или блокируются пользователи,

4. Программно-аппаратные средства защиты информации (дополнительные)

2 – Универсальный шлюз безопасности (UTM)

Универсальный шлюз безопасности (Unified Threat Management, UTM) – это модификация классического межсетевого экрана, которая дополнена системами обнаружения и предотвращения вторжений (IDS/IPS), VPN-сервером, средствами антивирусной защиты информации, системой контентной фильтрации и спам-фильтром.



4. Программно-аппаратные средства защиты информации (дополнительные)

2 – Универсальный шлюз безопасности (UTM)

Вместо конфигурирования нескольких устройств или программных комплексов имеется возможность гибкой настройки всех вышеперечисленных систем из одной консоли администратора. Для достижения высокой производительности UTM, как правило, используется специализированное аппаратное и программное обеспечение (ПО).



4. Программно-аппаратные средства защиты информации (дополнительные)

3 – Межсетевой экран нового поколения

Межсетевой экран нового поколения (Next Generation Firewall, NGFW) – это модифицированный межсетевой экран, интегрированный с системами обнаружения и предотвращения вторжений, системами антивирусной защиты, системами контентной фильтрации на уровне приложений, а также с технологией DPI для глубокой фильтрации трафика (поведенческий анализ трафика).

NGFW создавался для крупных предприятий в отличие от UTM-решений, которые разрабатывались для среднего бизнеса.



4. Программно-аппаратные средства защиты информации (дополнительные)

4 – Инфраструктура открытых ключей (PKI)

Инфраструктура открытых ключей (Public Key Infrastructure, PKI) – это совокупность материальных и технических средств, человеческих ресурсов, распределенных служб и компонентов, задачей которой является поддержание криптографических задач, использующих открытые и закрытые ключи.



4. Программно-аппаратные средства защиты информации (дополнительные)

4 – Инфраструктура открытых ключей (PKI)

и закрытые ключи [60, 61]. Основой функционирования PKI являются криптографические системы с открытым ключом и следующие принципы:

- закрытый ключ известен только его владельцу;
- удостоверяющий центр создает специальный документ под названием «Сертификат открытого ключа»;
- открытый ключ свободно распространяется;
- никто не доверяет друг другу, но все доверяют удостоверяющему центру;
- удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа лицу, который владеет соответствующим закрытым ключом.



4. Программно-аппаратные средства защиты информации (дополнительные)

5 – SIEM-система

Система сбора, корреляции и обработки событий ИБ (Security Information and Event System, SIEM) – это централизованная система сбора событий ИБ из различных источников, корреляции и обработки таких событий, а также выявления компьютерных инцидентов.



4. Программно-аппаратные средства защиты информации (дополнительные)

5 – SIEM-система



Рис. 10. Работа SIEM

4. Программно-аппаратные средства защиты информации (дополнительные)

5 – SIEM-система

Система сбора, корреляции и обработки событий ИБ (Security Information and Event System, SIEM) – это централизованная система сбора событий ИБ из различных источников, корреляции и обработки так их событий, а также выявления компьютерных инцидентов.



4. Программно-аппаратные средства защиты информации (дополнительные)

5 – SIEM-система

ется использование SIEM-систем. основополагающий принцип системы SIEM заключается в том, что данные о безопасности информационной системы собираются из разных источников и результат их обработки предоставляется в едином интерфейсе, доступном для аналитиков безопасности, что облегчает изучение характерных особенностей, соответствующих инцидентам безопасности.



СИСТЕМА МОНИТОРИНГА СОБЫТИЙ ИБ (SIEM)

КОМРАД

Enterprise SIEM

MaxPatrol SIEM



4. Программно-аппаратные средства защиты информации (дополнительные)

Остальные –

<https://reader.lanbook.com/book/404549?lms=7eca6610f4ba8af8a1cf65abe2516751>

