Практика 2.

Выбор программно-аппаратных средств защиты информации

Средства защиты, в зависимости от класса автоматизированной системы, для которой они предназначены, могут работать на разных уровнях взаимодействия. В некоторых случаях программные и аппаратные средства могут работать самостоятельно, но чаще всего они дополняют функциональные возможности друг друга.

Программно-аппаратная защита информации находится на стыке технической и криптографической защит информации. Надёжность защиты подтверждается сертификацией на соответствие требованиям руководящих документов по определённому классу средства. Сертификация технических средств защиты проводится ФСТЭК России, за сертификацию криптографических средств защиты отвечает ФСБ России.

Выбор средств для защиты коммерческой информации обусловлен только финансовыми возможностями владельца информации. Однако для защиты государственной тайны, служебной информации ограниченного распространения и персональных данных **обязательно** использовать сертифицированные средства защиты. Сведения о выданных сертификатах, сроках их действия и ограничениях на использование содержатся в реестрах сертификатов, ведущихся ФСТЭК и ФСБ.

Сертификация может проводиться не только для средства защиты, но и для любого оборудования или программного обеспечения. Как правило, оборудование и ПО, не являющееся средствами защиты, сертифицируют на отсутствие недекларированных возможностей и/или соответствие техническим условиям, обусловливающим технологию производства. Такие сертификаты позволяют использовать оборудование и программное обеспечение в защищенных информационных системах, однако ни в коем случае не приравнивают его к средствам защиты информации.

К средствам программно-аппаратной защиты информации могут относиться:

- антивирусы,
- электронные замки,
- средства доверенной загрузки,
- системы защиты от несанкционированного доступа,
- системы экстренного уничтожения информации на машинных носителях,
- системы предупреждения вторжений,
- шифровальные системы,
- средства электронной подписи,
- системы защиты от несанкционированного копирования или использования программного обеспечения.

Некоторые средства защиты информации обладают заранее заданными параметрами взаимной совместимости. Однако не все производители оборудования и программного обеспечения обладают возможностями по тестированию продуктов сторонних фирм. Обычно информация о совместимости или несовместимости имеется в документации на средство защиты информации.

Важно учитывать, что средство защиты информации не должно создавать чрезмерных дополнительных затрат. Например, нецелесообразно закупать СЗИ, срок действия сертификата на которое истекает менее чем через 1 год (в случае неопределённости относительно продления сертификата), или если это СЗИ предназначено для компьютерных систем, которые в ближайшем будущем лишатся поддержки изготовителя. Пример — Windows XP, поддержка уже окончилась, ФСТЭК определила переходный период для перевода защищенных КС на другие операционные системы 2016 годом. Соответственно, закупать СЗИ, работающие в Windows XP и не тестировавшиеся на совместимость с более новыми версиями, нецелесообразно.

Кроме этого, важно учитывать класс автоматизированной системы. Требования к защищенности для классов описаны в РД ФСТЭК «Автоматизированные системы...». Чем выше класс защищенности, тем дороже обойдётся СЗИ. Пример: из двух версий СЗИ DallasLock 8.0 **8.0-К** используется для защиты коммерческой тайны, в то время как DallasLock **8.0-С** — для защиты государственной тайны. Если на предприятии государственная тайна не обрабатывается, закупка 8.0-С экономически нецелесообразна. Для информационных систем персональных данных и государственных информационных систем существует дополнительная классификация, в этом случае следует ориентироваться на требования приказов ФСТЭК №№ 17 и 21 от февраля 2013 г. и Постановление Правительства РФ № 1119 от 1 ноября 2012 г.

Задачи ЛР — ознакомиться с текущим ассортиментом сертифицированных средств защиты информации и выбрать по одной конфигурации, состоящей из следующих средств защиты информации:

1. Криптопровайдер,
2. Система защиты от несанкционированного доступа,
3. Электронный замок и/или средство доверенной загрузки для информационных систем.

Научиться определять класс АС в зависимости от уровня конфиденциальности информации в АС, уровня полномочий субъектов доступа и режима обработки данных в АС. Варианты исходных данных для АС представлены в таблице:

ФИО	Уровень конфиденци-альности	Уровень полномочий	Режим обработки данных*	Максимальный уровень обрабатываемой информации
Иванов Иван Иванович	Один	Один	ОП	Особой важности
Маринина Марина Дмитриевна	Различный	Один	МП	Секретно
Сергеев Сергей Сергеевич	Различный	Различный	МП	Банковская тайна
…				
Юрьев Юрий Юрьевич	Один	Один	ОП	Коммерческая тайна

***Режимы обработки данных**:
ОП – Однопользовательский
МП – Многопользовательский

Задание:

Составить отчёт в электронном виде (документ Word), в котором будет содержаться следующая информация:

1. Описание параметров вашей системы (уровень конфиденциальности, уровень полномочий режим обработки данных, максимальный уровень обрабатываемой информации)
2. Класс вашей АС, который нужно определить исходя из параметров системы
3. Обоснованный перечень сертифицированных СЗИ для вашей АС. Прокомментируйте, какую функцию будет исполнять каждое средство защиты.

Контрольные вопросы:

1. Сколько групп АС и сколько классов АС вы знаете?
2. Чем отличаются группы АС ?
3. В чем отличие классов АС внутри одной группы?
4. Назовите основные этапы классификации АС.
5. Для чего необходимо деление АС на классы?
6. Расшифруйте аббревиатуры: НСД, СВТ, НДВ, СЗИ, ФСТЭК.

При ответе на контрольные вопросы необходимо руководствоваться руководящими документами ФСТЭК России, в частности документом **«Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.»**