МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)

Кафедра теоретической экономики

Доклад
по дисциплине «Информационная безопасность»
на тему «Аппаратные средства защиты информации»

Работу выполнил _____ 30.11.18 _____ Ванян Б.К.
(подпись, дата)

Факультет экономический

Направление 38.04.05 – Бизнес-информатика

Научный руководитель

д.э.н., проф._____ Сидоров В.А.
(подпись, дата)
30.11.2018

Краснодар 2018

Защита информации – это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования и блокирования информации.

Аппаратные средства защиты информации – это любые электрические, электронные, оптические, лазерные и другие устройства, которые встраиваются в информационные и телекоммуникационные системы: специальные компьютеры, системы контроля сотрудников, защиты серверов и корпоративных сетей. Они препятствуют доступу к информации, в том числе с помощью её маскировки.

К аппаратным средствам относятся: генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить.

С точки зрения степени сложности устройства ТСЗИ делятся на следующие.

1. Простые устройства – несложные приборы и приспособления, выполняющие отдельные процедуры защиты.

2. Сложные устройства – комбинированные агрегаты, состоящие из некоторого количества простых устройств, способные к осуществлению сложных процедур защиты.

3. Системы – законченные технические объекты, способны осуществлять некоторую комбинированную процедуру защиты, имеющую самостоятельное значение.

Все больше компаний стремится интегрировать защитные средства с другими системами ИТ-структур, в частности, SIEM, которые в режиме реального времени анализируют события безопасности, приходящие от сетевых устройств и приложений. Цена организации корпоративной системы защиты сведений складывается из множества составляющих. В частности, она зависит от сферы деятельности компании, количества сотрудников и пользователей,

территориальной распределенности системы, требуемого уровня защищенности и др. На стоимость работ влияет цена приобретаемого оборудования и ПО, объем выполняемых работ, наличие дополнительных сервисов и другие факторы. Так, стоимость программно-аппаратного комплекса Cisco WebSecurity варьируется от 170 дол. (при количестве пользователей до 1000) до 670 дол. (5000-10 000 пользователей).

Локально развертываемое устройство McAfee WebGateway стоит от 2000 дол. до 27 000 дол. Цена веб-фильтра Websense WebSecurity может достигать 40 000 дол. Стоимость Barracuda WebFilter стартует от 1500 дол. за оборудование, обслуживающее до 100 пользователей одновременно (аппарат для обслуживания 300-8000 пользователей обойдется в 4000 дол.). При этом ежегодное обновление ПО обойдется еще в $400–1100. В том числе безопасность компании помогают обеспечить и системы корпоративного управления паролями.

С точки зрения сопряженности со средствами вычислительной техники ТСЗИ бывают следующие.

1. Автономные – средства, выполняющие свои защитные функции независимо от функционирования средств вычислительной техники.

2. Сопряженные – средства, выполненные в виде самостоятельных устройств, но выполняющие защитные функции в сопряжении с основными средствами вычислительной техники.

3. Встроенные – средства, которые конструктивно включены в состав аппаратуры вычислительной техники.

Далее рассмотрим примеры автономных средств защиты.

Межсетевые экраны (также называемые брандмауэрами или файрволами). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней.

VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых невозможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.

Дисковые хранилища отличаются высочайшей скоростью доступа к данным за счет распределения запросов чтения/записи между несколькими дисковыми накопителями. Применение избыточных компонентов и алгоритмов в RAID массивах предотвращает остановку системы из-за выхода из строя любого элемента, так повышается доступность. Доступность, один из показателей качества информации, определяет долю времени, в течение которого информация готова к использованию, и выражается в процентном виде: например, 99,999% («пять девяток») означает, что в течение года допускается простой информационной системы по любой причине не более 5 минут.

Ленточные накопители (стримеры, автозагрузчики и библиотеки) попрежнему считаются самым экономичным и популярным решением создания резервной копии. Они изначально созданы для хранения данных, предоставляют практически неограниченную емкость (за счет добавления картриджей), обеспечивают высокую надежность, имеют низкую стоимость хранения, позволяют организовать ротацию любой сложности и глубины, архивацию данных, эвакуацию носителей в защищенное место за пределами основного офиса.

Помимо рассмотренных технологий следует также упомянуть обеспечение физической защиты данных (разграничение и контроль доступа в помещения, видеонаблюдение, охранная и пожарная сигнализация), организация бесперебойного электроснабжения оборудования.

eToken – Электронный ключ eToken – персональное средство авторизации, аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП). eToken выпускается в форм-факторах USB-ключа, смарт-карты или брелока. Модели eToken следует использовать для аутентификации пользователей и хранения ключевой информации в автоматизированных системах,

обрабатывающих конфиденциальную информацию, до класса защищенности 1Г включительно.

Комбинированный USB-ключ eToken NG-FLASH – одно из решений в области информационной безопасности от компании Aladdin. Он сочетает функционал смарт-карты с возможностью хранения больших объёмов пользовательских данных во встроенном модуле. Он сочетает функционал смарт-карты с возможностью хранения больших пользовательских данных во встроенном модуле flash-памяти. eToken NG-FLASH также обеспечивает возможность загрузки операционной системы компьютера и запуска пользовательских приложений из flash-памяти.

Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов – это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения, и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов и др.). Средства пожаротушения относятся к системам ликвидации угроз.

Поскольку применение сертифицированной аппаратуры и рекомендуемое размещение аппаратуры и кабелей в условиях коммерческого предприятия часто невыполнимы, полезным может быть размещение в составе абонентского терминала генераторов электромагнитного шума. При этом излучающие системы (антенны) генераторов должны быть максимально совмещены в пространстве с излучающими элементами аппаратуры.

Современные электронные системы охраны весьма разнообразны и в целом достаточно эффективны. Однако большинство из них имеют общий недостаток: они не могут обеспечить раннее детектирование вторжения на территорию объекта. Такие системы, как правило, ориентированы на обнаружение нарушителя, который уже проник на охраняемую территорию или в здание. Это касается, в частности, систем видеонаблюдения; они зачастую с помощью

устройства видеозаписи могут лишь подтвердить факт вторжения после того, как он уже произошел.

Инфракрасные системы. Активные лучевые ИК системы. Лучевые инфракрасные системы (их часто называют также линейными активными оптико-электронными извещателями) состоят из передатчика и приемника, располагаемых в зоне прямой взаимной видимости. Такой датчик формирует сигнал тревоги при прерывании луча, попадающего на фотоприемный блок. Отличительная особенность активных лучевых систем – возможность создания очень узкой зоны обнаружения.

Основная проблема лучевых ИК-охранных приборов – ложные срабатывания при неблагоприятных атмосферных условиях (дождь, снегопад, туман), уменьшающих прозрачность среды. Надежность в таких случаях обеспечивают за счет многократного превышения энергии луча над минимальным пороговым значением, необходимым для срабатывания датчика.

Источником помех может быть также прямая засветка приемника солнечными лучами. Кроме того, ИК системы могут срабатывать при попадании в луч птиц, листьев и веток деревьев или др. Для повышения устойчивости и надежности ИК-лучевых систем их делают многолучевыми (обычно используют 2 или 4 независимых луча).

Подводя итоги можно выделить некоторые достоинства и недостатки аппаратных средств защиты информации. К достоинствам можно отнести универсальность данных систем и средств, простота реализации, надежность и безотказность в работе, а также возможность модификации и гибкость систем.

К недостаткам относятся: снижение функциональных возможностей АСОД, подверженность случайным неверным модификациям, а также их ориентированность исключительно на определенные типы ЭВМ.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Буя П.М. Конспект лекций по курсу «Защита информации в телекоммуникационных системах». URL: https://studfiles.net/preview/5443545/

2. Мизинов С.В., Русинов С.Г., Добряков П.С., Нефедов Е.Ю. Обзор средств аппаратной защиты информации. Научная работа. URL: http://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=27&pa=13&ar=3

3. Реферат по теме «Аппаратные средства защиты информации». URL: https://works.doklad.ru/view/9Ycl39up0DI.html

4. Способы защиты информации. Аппаратные средства защиты информации. URL: https://studfiles.net/preview/5866837/