Тимашев Н.Н., Феоктистов Н.А.

«Сетевые технологии управления безопасностью крупных предприятий»

Для того чтобы быть конкурентоспособным игроком на рынке, компании необходимо правильно и быстро обрабатывать информацию, уметь надежно ее защищать, обеспечить необходимый уровень доступности данных и приложений, максимально эффективно использовать свои, как технологические, так и человеческие ресурсы. Решение всех этих задач сегодня невозможно без внедрения современных информационных технологий.

Как раз недавно, на международной техновыставке GITEX и на форуме ITU, проходивших одновременно в Дубаи, «Лаборатория Касперского» официально сообщила о своих планах по созданию собственной операционной системы, о которой ходили слухи в течение нескольких лет.

Операционная система от “Лаборатории Касперского” не является конкурентом Windows или Mac. Это продукт для индустриальных и промышленных систем. Суть в том, чтобы ограничить функциональность и сделать решение максимально надежным и безопасным. Фактически речь идет об интеллектуальной системе противоаварийной защиты нового поколения, которая учитывает весь комплекс показателей предприятия сразу и не позволяет привести к аварии ни в результате неправильных действий оператора, ни в результате ошибок в ПО, ни в результате кибератак. Помимо прочего, такая система сможет дополнить традиционные средства защиты, что позволит отслеживать более сложные и комплексные сценарии происходящего.

По мнению “Лаборатории Касперского”, максимально безопасная среда для контроля информационной инфраструктуры должна соответствовать следующим требованиям:

* ОС не может быть основана на каком-то уже существующем программном коде, поэтому должна быть написана с нуля.
* В целях гарантии безопасности она не должна содержать ошибок и уязвимостей в ядре, контролирующем остальные модули системы. Как следствие, ядро должно быть верифицировано средствами, не допускающими существования уязвимостей и кода двойного назначения.
* По той же причине ядро должно содержать критический минимум кода, а значит, максимально возможное количество кода, включая драйверы, должно контролироваться ядром и исполняться с низким уровнем привилегий.
* Наконец, в такой среде должна присутствовать мощная и надежная система защиты,  поддерживающая различные модели безопасности.

В системе ИБ можно условно выделить несколько уровней защиты, которые реализуются с помощью набора программных или программно-аппаратных решений: защита внутреннего периметра (Интернет и почтовые шлюзы передачи данных) и защита внешнего периметра (сервера приложений и данных, персональные и мобильные компьютеры работников).

 техническая реализация политики ИБ на современных промышленных предприятиях должна заключаться в построении комплексной системы информационной безопасности, охватывающей как технические, так и организационные меры защиты и контроля. Если в этой комплексной системе отдельно выделить техническую часть, то в ее основе будут находиться программно-аппаратные средства, каждое из которых ориентировано на устранение определенных видов угроз: вирусов, утечки конфиденциальной информации, несанкционированного доступа по различным каналам связи и т.д. Перечень угроз для каждого предприятия является уникальным, но, учитывая то, что в основе построения современных ИТ-инфраструктур лежат достаточно общеизвестные и распространенные технологии, большинство возникающих при этом угроз является типовыми. Поэтому можно выделить набор стандартных средств защиты, который определяет базовый «контур» комплексной системы ИБ, защищающий от наиболее серьезных и распространенных угроз. К таким средствам можно отнести межсетевые экраны, IDS/IPS, антивирусы, Identity and Access Management, средства фильтрации контента, СКЗИ, СЗИ от НСД и т.д.

**Межсетевой экран** или **сетевой экран** — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

**Система обнаружения вторжений (СОВ) (англ. Intrusion Detection System (IDS))** — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть.

Использование IDS помогает достичь нескольких целей:

* Обнаружить вторжение или сетевую атаку;
* Спрогнозировать возможные будущие атаки и выявить уязвимости для предотвращения их дальнейшего развития. Атакующий обычно выполняет ряд предварительных действий, таких как, например, сетевое зондирование (сканирование) или другое тестирование для обнаружения уязвимостей целевой системы;
* Выполнить документирование существующих угроз;
* Обеспечить контроль качества администрирования с точки зрения безопасности, особенно в больших и сложных сетях;
* Получить полезную информацию о проникновениях, которые имели место, для восстановления и корректирования вызвавших проникновение факторов;
* Определить расположение источника атаки по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

**Управление доступом и учетными данными (Identity and Access Management**) – это комплекс подходов, практик и специальных программных средств, основной целью которых служит значительное повышение степени контроля за доступом пользователей во всевозможные системы и приложения, используемые на предприятии, а также сокращение издержек предприятия, связанных с осуществлением такого контроля.

**Средства криптографической защиты информации (СКЗИ) -**  это совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем и осуществлять криптографическое преобразование информации для обеспечения ее безопасности.

Одним из таких средств защиты является Крипто Про CSP. Этот программно-аппаратный комплекс реализуется на следующих алгоритмах:

* Алгоритм зашифрования/расшифрования данных и вычисление имитовставки реализован в соответствии с требованиями ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая".
* Алгоритмы формирования и проверки ЭЦП реализованы в соответствии с требованиями ГОСТ Р 34.10-94 "Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма" и ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".
* Алгоритм выработки значения хэш функции реализован в соответствии с требованиями ГОСТ Р 34.11-94 "Информационная технология. Криптографическая защита информации. Функция хэширования".

Ключевая система КриптоПро CSP обеспечивает возможность парно-выборочной связи абонентов сети с использованием для каждой пары абонентов уникальных ключей, создаваемых на основе принципа открытого распределения ключей.

Так же при защите информации необходимо учитывать риск (как возможность потерь в результате какого-либо действия или события, способного нанести ущерб), угрозу (как действие или событие, способное нанести ущерб безопасности) и **уязвимость** (т.е. слабость в защите ресурса или группы ресурсов, допускающая возможность реализации угрозы).

Существует множество методик по управлению рисками, например, OCTAVE, CRAMM, MAGERIT и др. Рассмотрим более подробно OCTAVE.

**Сущность методология OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)** заключается в том, что для оценки рисков используется последовательность соответствующим образом организованных внутренних семинаров (workshops). Оценка рисков осуществляется в три этапа, которым предшествует набор подготовительных мероприятий, включающих в себя согласования графика семинаров, назначения ролей, планирование, координация действий участников проектной группы.

**На первом этапе**, в ходе практических семинаров, осуществляется разработка профилей угроз, включающих в себя инвентаризацию и оценку ценности активов, идентификация применимых требований законодательства и нормативной базы, идентификацию угроз и оценку их вероятности, а также определение системы организационных мер по поддержанию режима информационной безопасности.

**На втором этапе** производится технический анализ уязвимостей информационных систем организации в отношении угроз, чьи профили были разработаны на предыдущем этапе, который включает в себя идентификацию имеющихся уязвимостей информационных систем организации и оценку их величины.

**На третьем этапе** производится оценка и обработка рисков информационной безопасности, включающая в себя определение величины и вероятности причинения ущерба в результате осуществления угроз безопасности с использованием уязвимостей, которые были идентифицированы на предыдущих этапах, определение стратегии защиты, а также выбор вариантов и принятие решений по обработке рисков. Величина риска определяется как усредненная величина годовых потерь организации в результате реализации угроз безопасности.

Существует три основных вида угроз: природные, техногенные, человеческие. Природные угрозы человек научился прогнозировать и избегать. Риск техногенного фактора можно уменьшить путем отдаления информационных центров от технически опасных участков предприятия. Человеческий же фактор представляет основную угрозу, так как его сложнее всего предугадать. Если человек создает систему безопасности , то он может добиться ее нарушения, путем проникновения или занесения вируса.

**Список литературы:**

1. hi-tech.mail.ru /article/misc/kaspersky\_gitex\_itu.html
2. http://www.i-teco.ru/article192.html
3. http://www.cryptopro.ru/products/csp/csp-3-6
4. Балашов П. А., Кислое Р. И., Безгузиков В. П. Оценка рисков информационной безопасности на основе нечеткой логики // Безопасность компьютерных систем. Конфидент. 2003. № 5. С. 56-59.