Интегрированные системы комплексной защиты периметра предприятия

Светлана Конявская, *заместитель генерального директора ЗАО "ОКБ САПР", к.ф.н.*

Специалист подобен флюсу, поэтому так сложно создать на предприятии действительно интегрированную систему безопасности. Даже подсистемы защиты информации не всегда могут договориться между собой (даже если удалось договориться их разработчикам, что тоже маловероятно), что уж говорить о таких, казалось бы, разных явлениях, как доступ к прикладной задаче на автоматизированном рабочем месте (АРМ) и доступ на территорию организации. За это даже отвечают разные подразделения, и этот факт сам по себе в свое время был прорывом — осознание того, что защита информации — это целая отдельная область знаний и умений, пришло не сразу.

Теперь пришло время обратного процесса – осознания того, что никаких причин, препятствующих созданию единой интегрированной системы контроля доступа – от входа в ворота до входа в учетную запись пользователя, – нет. Кроме того, что за них отвечают разные подразделения. Это серьезный контраргумент, но, думается, владельцу системы решать, насколько он перевешивает плюсы интеграции.

Интеграция систем защиты информации и контроля доступа позволит достичь ощутимых преимуществ.

1. Объединение персональных идентификаторов сотрудников, применяемых ими в СЗИ НСД и в СКУД, даст возможность сократить количество инцидентов, связанных с забыванием идентификаторов, передачей другому лицу или оставлением их без присмотра в момент отсутствия пользователя на рабочем месте, а также практически исключить воздействие человеческого фактора на выполнение правила блокировки рабочего места пользователя в момент отсутствия последнего.

2. Объединение систем управления СКУД и СЗИ НСД путем создания третьей управляющей системы позволит сформировать правила доступа во взаимосвязанности результатов выполнения действий доступа к информационным ресурсам и помещениям. Например, СКУД будет позволять покинуть комнату, заблокировав рабочее место, но не будет позволять покинуть территорию предприятия, если рабочее место не выключено надлежащим образом или не завершен сеанс работы того пользователя, который хочет покинуть территорию. А СЗИ НСД, в свою очередь, не будет позволять пользователю доступ в информационную систему, если нет информации от СКУД, что он вошел на территорию предприятия, и так далее. При этом все факты таких нестандартных ситуаций будут зарегистрированы и могут быть (и должны быть!) проанализированы ответственным за безопасность лицом.

Взаимоувязывание событий СКУД и СЗИ НСД в общие правила может исключить обход правил безопасности, который возможен из-за разорванности этих систем.

Рассмотрим пример

С точки зрения СЗИ НСД разблокировка сессии и включение СВТ являются разными событиями, и в отношении этих событий весьма вероятна настройка разных ограничений. Например, разблокировка сессии зачастую возможна не только тем пользователем, чья это сессия, но и администратором или другим пользователем с аналогичной ролью (или входящим в коллективную учетную запись), при этом разблокируется та же самая сессия. Иначе в случае включения АРМ – если АРМ будет включаться, то под тем профилем, кто его включает, а не под тем, кто его выключил. Для разблокировки сессии могут быть установлены совершенно другие ограничения по времени, в которое допустима разблокировка, в отличие от времени, в которое разрешено включение АРМа. Соответственно, если перед уходом пользователь (случайно или умышленно) не выключил АРМ, а только заблокировал сессию, то он открывает злоумышленнику возможность осуществить те или иные манипуляции с его рабочим местом, которые тот не смог бы осуществить, будь АРМ корректно выключен. Если же интегрированная система безопасности не выпустит пользователя за пределы организации, пока тот не выключит компьютер надлежащим образом, то атака такого рода будет невозможна. Таких примеров может быть масса.

"Рассвет-СВМиКД"

Для создания такой интегрированной системы видеомониторинга и контроля доступа (СВМиКД) мы предлагаем решение, состоящее из Сервера интеграции комплексов "Рассвет-СВМиКД". Сервер обеспечивает взаимодействие серверов управления СЗИ НСД "Аккорд" и СКУД, что дает возможность формирования новых, более сложных и комплексных правил доступа. А комплексы "Рассвет-СВМиКД", помимо взаимодействия с Сервером интеграции, выполняют функцию передачи видеоизображения с экрана монитора подконтрольного АРМ на заданный сервер, видеоизображения с IP-видеокамеры (входит в состав комплекса), снимающей оператора, на заданный сервер видеонаблюдения, а также при необходимости может усилить подсистему аутентификации, например считывателем биометрических данных. ●

Разумеется, не может быть коробочного решения, интегрирующего любую систему защиты информации с любой СКУД сразу, как только его достали из упаковки. Интеграция вообще не может быть коробочным решением. Однако это не должно становиться препятствием к ее осуществлению там, где она возможна и уместна. "Рассвет-СВМиКД" дорабатывается для каждой конкретной системы не только в части процедур взаимодействия с каждой новой СКУД, но и в части правил доступа, которые формируются согласно потребностям и представлениям эксплуатирующей организации, а не нашим собственным.

NM ●
АДРЕСА И ТЕЛЕФОНЫ ЗАО "ОКБ САПР"
см. стр. 80