СЕКЦИЯ 1. ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДИКА АУДИТА УЯЗВИМОСТЕЙ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

А.А. Зубко, А.М. Прудник

С ростом числа пользователей банковского дистанционного обслуживания, растет и количество угроз для этих систем. Злоумышленники могут использовать уязвимости не только клиента банка, но и самого банка, а вернее системы ДБО. Используя эти уязвимости, злоумышленник может получить большие возможности по манипуляции данными в системе ДБО, в том числе может управлять счетами клиентов. Поэтому есть необходимость в проведении аудита уязвимостей системы ДБО по определенному методу.

Этап 1. Выявление уязвимостей, который начинается с создания и поддержания текущей базы данных всех IP-устройств, подключенных к сети. Организации должны категоризировать устройства согласно их ценности для бизнеса, чтобы расположить их по приоритетам для будущего процесса устранения уязвимостей. Элементы в базе данных включают все аппаратные средства, программное обеспечение, приложения, сервисы и конфигурации. Необходимо очень ответственно подойти к данному этапу. Правильно организованный контроль за этой работой даст компании два преимущества: будет идентифицировано, какие уязвимости влияют на определенные параметры IT инфраструктуры и бизнес процессы, кроме того, точная инвентаризация гарантирует, что в процессе исправления будут отобраны и применены правильные патчи. Проведение инвентаризации также помогает ускорить процесс сканирования, поскольку сокращается время на поиск устройств с одного рода уязвимостями.

Этап 2. Поиск уязвимостей путем сканирования всей инфраструктуры на наличие слабых мест. Система сканирования периодически тестирует и анализирует IP-устройства, сервисы и приложения. Отчет после сканирования указывает на фактические слабые места и на то, что именно нужно исправить.

Этап 3. Распределить уязвимости по категориям. Корпорация Microsoft, например, выделяет четыре категории устранения риска: критически важный, важный, умеренный и низкий с соответствующими показателями.

Этап 4. Процесс исправления уязвимостей. Вносятся изменения в IT-инфраструктуру, применяются различные патчи. Иногда высокая стоимость внесения исправлений вместе с большим объемом недостатков в приложениях от поставщиков вынуждают организации откладывать процесс устранения недостатков на неопределенное время. К сожалению, задержка может оказаться фатальной, поскольку потенциальные слабые места быстро обнаруживаются злоумышленниками — как показывают исследования, временной интервал между появлением угрозы и вторжением постоянно сокращается. Поэтому важно устранить уязвимость как можно быстрее и тем самым минимизировать риски.

Литература

1. *Лямин Л.* Системы Применение технологий электронного банкинга: риск-ориентированный подход. М., 2011.

2. https://www.qualys.com/forms/cloud-agent/

МЕТОДИКА ОБОСНОВАНИЯ КОЛИЧЕСТВА ПОДРАЗДЕЛЕНИЙ КОМПЛЕКСНОГО ТЕХНИЧЕСКОГО КОНТРОЛЯ

В.Н. Корделюк

Армии иностранных государств проводят по отношению к другим мероприятия по добыванию, обработке и анализу разведывательной информации в интересах обеспечения преимуществ своему государству в военной сфере. В связи с этим в целях защиты информации о своих объектах необходимо проводить различные мероприятия противодействия разведкам, в том числе и их техническим средствам.

Обязательными составляющими мероприятий противодействия техническим средствам разведки (ПД ТСР) являются мероприятия комплексного технического контроля (КТК) [1], основными задачами которого являются выявление и анализ демаскирующих признаков своих

объектов защиты (ОЗ), а также вскрытие возможных каналов утечки информации от этих объектов. Качественное проведение мероприятий КТК призвано обеспечить оценку эффективности проводимых в войсках мероприятий маскировки и ПД ТСР противника, выполнение которых оказывает существенное влияние на снижение вероятности обнаружения противником ОЗ и получения им достоверной информации о составе, положении, состоянии, предназначении и характере деятельности войск (сил), а также замысле предстоящих действий.

Для выполнения мероприятий КТК создаются специально подготовленные подразделения КТК, основной задачей которых является проведение КТК на всех ОЗ.

В предлагаемой методике обоснования количества подразделений КТК используется математическая модель определения оптимальных маршрутов движения данных подразделений, перемещаясь по которым они смогут осуществить мероприятия КТК с заданным эффектом. Данная методика позволит должностному лицу, принимающему решение по применению подразделений КТК, равномерно распределить между ними нагрузку и назначить каждому подразделению свой район КТК.

Литература

1. Основы защиты от технических разведок: учеб. пособие / Ю.К. Меньшаков; под общ ред. М.П. Сычева. М. : Изд-во МГТУ им. Н.Э. Баумана, 2011. 478 с.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО БИЗНЕСА

В.С. Князькова

Электронный бизнес (ЭБ) — вид предпринимательской деятельности, основанной преимущественно на интернет-технологиях. Интернет предоставляет огромные возможности для выстраивания различных бизнес-процессов, но, как следствие, влечет за собой дополнительные к традиционным видам деятельности риски.

Для построения модели угроз организации ЭБ необходимо определить уровень интеграции ЭБ в бизнес-процессы организации. Он может быть различным. Так, с помощью интернет-технологий организация может:

– предоставлять сведения об организации и основных видах ее деятельности (например, сайт-визитка);

– реализовывать часть бизнес-процессов посредством интернет-технологий (например, интернет-магазин для промышленного предприятия);

– выносить большинство бизнес-процессов в среду ЭБ (например, маркетинг и/или финансы, и/или логистика, и/или оказание услуг);

– реализовывать все свои бизнес-процессы в среде ЭБ (например, новостной портал).

– типичными для всех уровней интеграции ЭБ будут следующие угрозы:

– угроза потери целостности информации о бизнес-процессах и бизнес-операциях;

– угрозы вирусной атаки и подверженность мошенничеству со стороны потребителей и иных лиц посредством несанкционированного доступа к информации;

– несоблюдение требований нормативно-правового регулирования финансово-хозяйственной деятельности и, в частности, ЭБ из-за отсутствия четко выработанной законодательной системы в этой сфере;

– сбой или отказ систем и элементов информационных инфраструктур.

Дальнейший и бурный рост числа экономических субъектов, внедряющих современные информационные технологии или полностью ориентированных на электронный бизнес, обусловлен, прежде всего, тем, что при ведении финансово-хозяйственной деятельности в современной электронной среде значительно снижаются транзакционные издержки, т.е. издержки, сопряженные с переходом прав собственности на потребительский результат.

Обычно руководство и лица, наделенные руководящими полномочиями экономического субъекта, вовлеченного в электронный бизнес, оценивают бизнес- и ИТ-риски посредством внедрения системы информационной безопасности, создания надлежащей ее инфраструктуры и применения надлежащих средств контроля, которые направлены:

– на идентификацию и проверку подлинности потребителей и поставщиков;

– на обеспечение целостности информации о бизнес-операциях;

– на получение оплаты или обеспечения в отношении кредитных средств потребителей;

– на установку протоколов конфиденциальности и защиты информации.