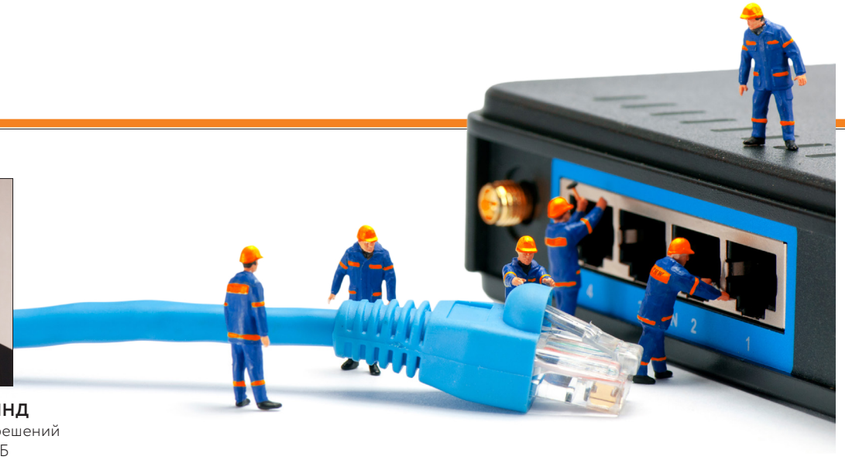
Дмитрий МИТЮШИН
инженер отдела решений
по управлению ИБ
АО «ЭЛВИС-ПЛЮС»

Дмитрий ТАЙГИНД
инженер отдела решений
по управлению ИБ
АО «ЭЛВИС-ПЛЮС»



ПРОАКТИВНОЕ МОДЕЛИРОВАНИЕ СЕТЕВЫХ УГРОЗ В КОНТЕКСТЕ ЗАДАЧ УПРАВЛЕНИЯ ИБ

Обеспечение ИБ на сегодняшний день является одним из неотъемлемых элементов корпоративного управления. Во всё большем количестве компаний различных отраслей прослеживается тенденция по изменению подходов к обеспечению ИБ, что для компаний кредитно-финансового сектора, как наиболее зрелых в части применения практик по ИТ и ИБ, уже не в новинку — обеспечение ИБ всё чаще рассматривается как непрерывный, регламентированный и прогнозируемый процесс управления, а не как эксплуатация набора технических средств. Этот процесс в идеале взаимоувязан с целями и задачами бизнеса компании, распространяется на зоны ответственности широкого круга структурных подразделений, а также управляется непосредственно высшим руководством.

Процессный подход к управлению ИБ является основой для обеспечения соответствия различным отраслевым и международным стандартам, например, ISO 27001, СТО БР ИББС-1.0–2014, PCI DSS v3.1. При этом одними из основополагающих моментов являются процессы по моделированию угроз и оценке рисков, в том числе, с учетом результатов выполнения задач по управлению:

- Активами (инвентаризация).
- Изменениями.
- Техническими уязвимостями.
- Сетевой безопасностью.
- Инцидентами.
- Контролем защитных мер.

Неавтоматизированные методы реализации перечисленных задач управления ИБ в условиях большого объема данных и постоянно изменяющейся информационной среды **являются неэффективными**, что снижает или сводит на нет возможность оперативного контроля состояния защищенности и принятия персоналом обоснованных решений по снижению рисков ИБ.

ОБЩИЕ ПОДХОДЫ К АВТОМАТИЗАЦИИ ПРОЦЕССОВ УПРАВЛЕНИЯ ИБ

Для автоматизации любой из задач в рамках процессов управления ИБ требуется собрать исходные данные из различных источников. Такими источниками могут быть средства защиты информации, инфраструктурные элементы и корпоративные информационные системы. От качества и полноты исходных данных зависит очень многое, поэтому в процессе внедрения средств автоматизации процессов, как правило, вскрываются проблемы функционирования систем защиты информации (ложные срабатывания правил в SIEM, отсутствие результатов анализа защищенности для отдельных сегментов, различие в версиях используемого ПО, отсутствие актуальной информации об активах, сетевой топологии и т.п.).

После сбора данных в единую универсальную базу в составе системы требуется выполнить их программную обработку, целью которой является расчет ключевых показателей и наглядное представление сводной информации, поддерживающих принятие управленческих решений пользователями различных уровней (с учетом ролевой модели и матрицы разграничения доступа), либо подлежащих передаче в целевые системы.

На уровне государственного управления РФ в последнее время также отмечается высокая озабоченность проблемами ИБ — **реализуется и планируется ряд глобальных инициатив, требующих высокой степени автоматизации,** по повышению регулируемости и управляемости отрасли ИБ, а также повышения уровня защищенности российских компаний в целом.

Примером может служить создание Банка данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю (ФСТЭК России), а также Финансовый центр мониторинга и реагирования на инциденты ИБ (**FinCERT**), созданный в середине 2015 года на базе Главного центра управления безопасности и защиты информации Банка России, и являющийся ведомственным центром в составе Государственной системы обнаружения, предупреждения и устранения последствий компьютерных атак (**ГосСОПКА**), взаимодействующим с Главным центром — Национальным координационным центром по компьютерным инцидентам, созданным на базе 8 центра ФСБ РФ.

При обработке данных учитываются следующие параметры:

- Целевые формы представления и передачи данных.
- Роль пользователя, для которого эти данные предназначены.
- Характеристики имеющихся в компании процессов по управлению ИБ — цели использования и срок хранения, контролируемые параметры защиты, частота и аудитория предоставления, целевые системы для выдачи данных.

Таким образом, средство автоматизации вскрывает следующий пласт проблем — выявляется реальный уровень зрелости процессов управления ИБ в компании, который значительно улучшается при внедрении средств автоматизации процессов управления ИБ, так как для настройки системы требуется согласовать и документально зафиксировать все основные процедуры и метрики целевых и смежных с ними процессов (например, управление обновлениями ПО при устранении выявленных уязвимостей).

ТЕНДЕНЦИИ И ПРАКТИКА

Одним из первых этапов подготовки к автоматизации процессов управления ИБ является построение процесса управления информационными активами[1]. Наиболее важным активом, напрямую влияющим на функционирование информационных систем, является сетевая инфраструктура. Знание уровня её защищенности и реального статуса функционирования необходимо как ИТ-, так и ИБ-подразделению.

Популярные и наиболее хорошо освоенные средства автоматизации процессов управления ИБ предоставляют либо первичную информацию о состоянии защищенности информационно-телекоммуникационной инфраструктуры и способах её использования, либо возможности по **реактивной обработке** зарегистрированных событий и инцидентов ИБ **без учета** возможности автоматического ранжирования обрабатываемых данных с учетом **действующих конфигураций применяющихся технических средств защиты, модели угроз и оценки рисков.**

Реализация данной задачи возможна **путем создания** (в рамках выделенной подсистемы) **модели** информационно-телекоммуникационной инфраструктуры, отражающей её основные характеристики (данные об активах, уязвимостях и принятых технических мерах обеспечения ИБ), логические связи между её компонентами (например, сетевой доступ), а также позволяющей проводить оценку соответствия заданным контролям ИБ (например, соответствия политике сетевого доступа) и **проактивное моделирование возможных негативных ситуаций** в отношении информационных активов.

Создание модели позволит не только консолидировать данные об информационных активах, и выполнять проверку планирующихся изменений (например, в части изменения сетевого доступа), но и **проводить эффективную приоритизацию уязвимостей** с использованием процессов **моделирования сетевых атак**.

* * *

В виду большого объема разнородных данных, в настоящий момент все, либо выделенные **процессы управления ИБ, не могут быть полностью автоматизированы.** При этом значительная часть функций все равно будет выделена на выполнение специалистами подразделений ИТ и ИБ.

На рынке есть ряд продуктов, в которых решаются задачи автоматизации процессов по управлению ИБ, но их внедрение должно быть постепенным, последовательным, с адаптацией под требования конкретной компании и с применением заложенных производителем лучших практик. Результаты становятся видны уже на этапе внедрения, когда решаются проблемы с источниками данных, описываются или уточняются описания действующих процессов, а у пользователей появляется осознание важности и целей проводимой работы.

Подводя итог, хотелось бы отметить, что применение систем с возможностью моделирования различных негативных ситуаций ИБ, позволяет подготовиться к внедрению полноценной системы по автоматизации процессов управления ИБ и **качественно повысить эффективность автоматизируемых процессов.**

Использованные в данных системах подходы по моделированию информационно-технологической инфраструктуры, сетевых атак, а также проактивному управлению ИБ, на наш взгляд, являются перспективными. Подтверждением этого является и то, что, ряд существующих и разрабатываемых SIEM решений уже содержат или будут включать в свой состав функциональные компоненты по моделированию сетевой инфраструктуры и сетевых атак.

1 Здесь и далее по тексту под информационными активами понимаются конкретные технические средства информационно-телекоммуникационной инфраструктуры (например: АРМ, серверы, сетевое оборудование) и информационные системы, базирующиеся на данных средствах.