С. С. Велигодский
Сбербанк России,
Н. Г. Милославская (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)

МОДЕЛИРОВАНИЕ ПРОЦЕССА ПРОТИВОДЕЙСТВИЯ НАРУШЕНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОГО ПОРТАЛА

Представлена модель процесса взаимодействия атакующей системы с корпоративным веб-порталом, позволяющая проводить анализ конфликтного взаимодействия сторон.

Введение

С развитием средств и методов нарушения информационной безопасности (ИБ) корпоративного портала задача обеспечения его функционирования при внешнем воздействии приобрела ярко выраженный конфликтный характер. Рассмотрение конфликта как формы целенаправленного изменения состояния противостоящих сторон (атакующего и защищаемого) при возмущающих воздействиях предполагает необходимость формирования модели противодействия нарушениям ИБ портала как модели конфликтного взаимодействия средств нарушения безопасности и объекта нарушения безопасности (корпоративного портала со средствами защиты). Для этого необходимо, в первую очередь, определить конкретное содержание «противостоящих сторон».

Во взаимодействии находятся две сложные интеллектуальные системы:

S_1 — атакующая система со средствами нарушения ИБ корпоративного портала, обеспеченная необходимыми техническими средствами для осуществления атак на корпоративные порталы (система S_2);

S_2 — объект нападения — корпоративный портал с соответствующими средствами обеспечения защищенности.

Состояния конфликтующих сторон определяются состояниями всех входящих в них элементов. Элементы обеих систем делятся на три класса:

· рабочие элементы $S_{Р1,2}$ (ядро систем), предназначенные для выполнения целевых задач систем S_1, S_2;

· защитные элементы $S_{З1,2}$, обеспечивающие порталам возможность противодействия внешнему воздействию противостоящей стороны;

· внешние активные элементы $S_{А1,2}$, предназначенные для воздействия на рабочие элементы с целью исключения возможности их функционирования.

В контур управления каждой из систем включен распорядительный центр (человек или экспертная система) $S_{И1,2}$.

1. Модель взаимодействия атакующей системы и объекта взаимодействия

На рис. 1 представлена модель взаимодействия двух систем: S_1 и S_2.

В настоящее время стало очевидным, что в силу скачкообразного развития современных Web-технологий, разработка которых ведется иногда без учета вопросов ИБ, развитие традиционных и появление новых угроз ИБ (угрозы современным Web-приложениям — SQL-injection, Command injection, Cross-site scripting и пр.) вызвало необходимость реализации целого комплекса мероприятий по обеспечению защищенности портала. Это в существенной степени усложняет условия функционирования средств воздействия (стороны S_1) и затрудняет практическую реализацию их генеральной стратегии, направленной на упреждение противостоящей стороны S_2 и максимизацию успешности (когда достигается максимум вероятности или минимум средней продолжительности) воздействия — исключение

возможности функционирования портала и/или несанкционированный доступ к его ресурсам. В свою очередь генеральная стратегия корпоративного портала (стороны S_2) в рамках указанного конфликтного взаимодействия состоит в исключении (затруднении) возможности практической реализации генеральной стратегии стороны S_1.

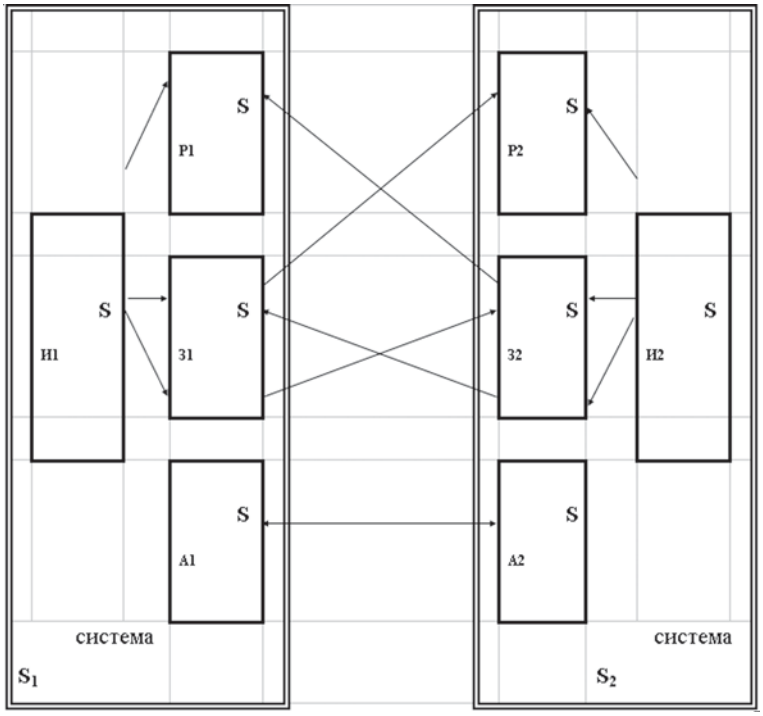

Рис. 1. Модель взаимодействия двух систем

1. Средства конфликтующих систем. Анализ решаемых в рамках указанного взаимодействия задач позволяет определить состав входящих в конфликтующие системы средств. Каждая из сторон имеет в своем составе:

· *средства поиска*, обеспечивающие решение задачи обнаружения и распознавания:

- для системы S_1 — средства анализа защищенности и поиска уязвимостей в корпоративном портале и средствах обеспечения его ИБ;

- для системы S_2 — средства обнаружения вторжений, средства журналирования событий, влияющих на ИБ, аудита ИБ и пр.;

· *средства противодействия*, исключающие возможность функционирования противостоящей стороны:

- для системы S_1 — средства осуществления атак, включающие, как правило, средства перехвата сетевого трафика, подбора паролей, так называемые эксплойты (от англ. «exploit») и rootkits и пр.;

- для системы S_2 — системы идентификации и аутентификации, межсетевые экраны, системы предотвращения вторжений, сканеры защищенности, средства построения виртуальных частных сетей, антивирусы, средства шифрования и пр.;

· *средства воздействия*, позволяющие активно или пассивно уклоняться от воздействия:

- для системы S_1 — средства сокрытия следов атак, например, анонимайзеры и ресселеры электронной почты, использование методов вставки, фрагментации, замедления, шифрования и пр.;

- для системы S_2 — средства ответной атаки и создания так называемых ложных целей — Honeynets и Honeypots и пр.

На основе такого подхода к детализации взаимодействующих сторон в табл. 1 определен возможный состав средств участников конфликта [1, 2]. Основными противостоящими элементами в условиях

конфликтного взаимодействия в соответствии с содержанием конфликтующих сторон являются технические средства поиска (специализированные инструментальные средства стороны S_1) и средства противодействия нарушениям ИБ (средства обеспечения защищенности корпоративного портала) стороны S_2.

Таблица 1. Возможный состав средств участников конфликта.

Система / Средства	Средства нарушения информационной безопасности портала (система S_1)	Корпоративный портал (система S_2)
Средства поиска	Технические средства анализа защищенности и поиска уязвимостей.	Технические средства обнаружения вторжений, средства журналирования и аудита ИБ, средства анализа политики безопасности.
Средства противо-действия	Средства реализации угроз ИБ (атак) – нарушения целостности, доступности и конфиденциальности информации: - перехват информации в каналах связи; - несанкционированный доступ к информации; - совершение операций в портале от имени пользователей; - незаконное копирование и распространение информации; - модификации информации; - уничтожение информации; - блокирования доступа; - нарушение работоспособности портала и т. д.	Методы и средства защиты: - идентификация и аутентификация субъектов доступа; - обеспечение и контроль целостности; - межсетевое экранирование; - криптографическая защита; - антивирусная защита; - системы обнаружения и предотвращения вторжений; - обеспечение доступности портала и его ресурсов; - управление системой ИБ и т. д.
Средства воздействия	Уничтожение следов воздействия: - повреждение оборудования или ПО; - «логическая бомба»; - ввод неверных данных; - удаление или изменение данных; - методы вставки, фрагментации, замедления, шифрования; - анонимайзеры и ресселеры и т. д.	Средства ответной атаки и создания так называемых «ложных целей» - Honeynets и Honeypots и т. д.

2. Моделирование конфликтного взаимодействия систем

Для практической реализации подхода к исследованию и обеспечению защищенности корпоративного портала в условиях воздействия средств реализации угроз ИБ важным является определение структуры модели их взаимодействия. Моделирование конфликтного взаимодействия систем является средством получения информации, необходимой для выработки рационального поведения системы в конфликте.

Поскольку во взаимодействии находятся системы с противоположными интересами и каждый из участников конфликта для достижения своей цели обладает свободой выбора управляющих воздействий, то есть непредсказуемым для взаимодействующей системы поведением, следовательно, строгое математическое описание (аналитическая модель) процесса конфликтного взаимодействия не будет адекватно отражать исследуемую проблему.

Конфликтное взаимодействие систем можно описать как процесс их взаимного управления с помощью системы многошаговых уравнений [3], определяющей взаимосвязь (Z^k_1, Z^k_2) — траекторий процессов смены состояний соответственно S_1, S_2 до момента t_{k+1} и (u^k, v^k) — совокупности управляющих воздействий систем S_1 и S_2 до момента t_{k+1} при возмущающих воздействиях L:

$$\begin{cases} Z^1_{k+1} = \phi_1(Z^k_1, u^k_1, v^k_1, \Lambda), \\ Z^2_{k+1} = \phi_2(Z^k_2, u^k_2, v^k_2, \Lambda), \\ Z^1_0 = Z^1_{\text{исх}}, \\ Z^2_0 = Z^2_{\text{исх}}, \\ k = 0(1)K - 1, \end{cases}$$

где $Z^1_{\text{исх}}$, $Z^2_{\text{исх}}$ — исходные состояния систем, K — количество шагов взаимодействия систем в конфликте.

Достигнутый стороной S_1 к моменту времени t_{k+1} результат в ходе конфликта может быть представлен следующим образом: $Y^1_{k+1} = h_1(Z^k_1, u^k, v^k, \Lambda)$, для стороны S_2 соответственно: $Y^2_{k+1} = h_2(Z^k_2, u^k, v^k, \Lambda)$.

Эффективности управляющих воздействий оцениваются текущими показателями: $W^1_{k+1} = M[f^1_{k+1}(Y^1_{k+1}, Y^1_{тр})]$, $W^2_{k+1} = M[f^2_{k+1}(Y^2_{k+1}, Y^2_{тр})]$ и интегральными показателями: $W^1 = M[f^1(Y^1, Y_{тр})]$, $W^2 = M[f^2(Y^2, Y_{тр})]$, где M — математическое ожидание, $Y^{1,2}$ — реальный результат применения системами своих управляющих воздействий; $Y_{тр}$ — требуемый результат.

На рис. 2 показана структура модели конфликтного взаимодействия средств нарушения ИБ корпоративного портала. Блоки 1 отображают процесс смены состояний системы и достигнутый результат применения управляющих воздействий (стратегий), который подается в блоки 2 для оценки показателей их успешности. По результатам оценки успешности (эффективности) управляющих воздействий (стратегий) в блоке 3 (распорядительном центре), обладающем оценкой функции распределения возможных вариантов воздействия конфликтующей стороны, вырабатывается внутреннее управление по выбору рационального образа действий. Управляющие воздействия вырабатываются в блоке 4 на основе управлений блока 3 и наличия активных средств, отраженных блоком 5. Активные средства представляются техническими характеристиками систем и совокупностью ресурсов различного вида, используемых в конфликте.

На каждый вид ресурсов накладываются ограничения (например, конечное количество пропускной способности каналов связи): $R^1_d < R^1_{d0}$, $d=1(1)D$, $R^2_m < R^2_{m0}$, $m=1(1)M$,

где d, m — номера видов ресурсов сторон S_1, S_2 соответственно; R^1_{d0}, R^2_{m0} — запас ресурсов d-го, m-го видов соответственно (например, пропусканная способность каналов связи или вычислительные мощности аппаратной платформы КИП).

Блок 6 отображает условия протекания взаимодействия в виде возмущающих факторов различной природы.

Такая структура модели конфликтного взаимодействия систем позволяет синтезировать поведение S_2 (корпоративного портала) в виде последовательности управляющих воздействий $v^* = \{v^0, v^1, ..., v^k\}$, удовлетворяющей условию $W^2(v^*) > W^2_{тр}$, где $W^2_{тр}$ — требуемый уровень успешности функционирования системы S_2 (должна соответствовать требуемому уровню защищенности).

3. Заключение

Анализ комплексной логико-аналитической модели конфликтного взаимодействия определяет необходимость решения ряда задач:

- синтеза исходных множеств стратегий участников конфликтного взаимодействия;
- оценки конфликтно-обусловленной эффективности управляющих воздействий.

Осуществление участниками противодействия своих генеральных стратегий возможно на основе принципа рационального поведения, определяющего активное поведение систем. Такой подход является условно-эффективным и позволяет избежать перебора всех возможных стратегий поведения при выборе последовательности действий и снизить требования к параметрам и ресурсам систем. При этом необходимо учитывать тот факт, что рациональному образу действий корпоративных порталов в условиях воздействия

средств нарушения ИБ, адекватна концепция активного (адаптивного) поведения и гибкого реагирования, основанная на использовании накопленной информации (экспертных данных) для достижения или сохранения определенного состояния при изменяющемся комплексе условий взаимодействия.

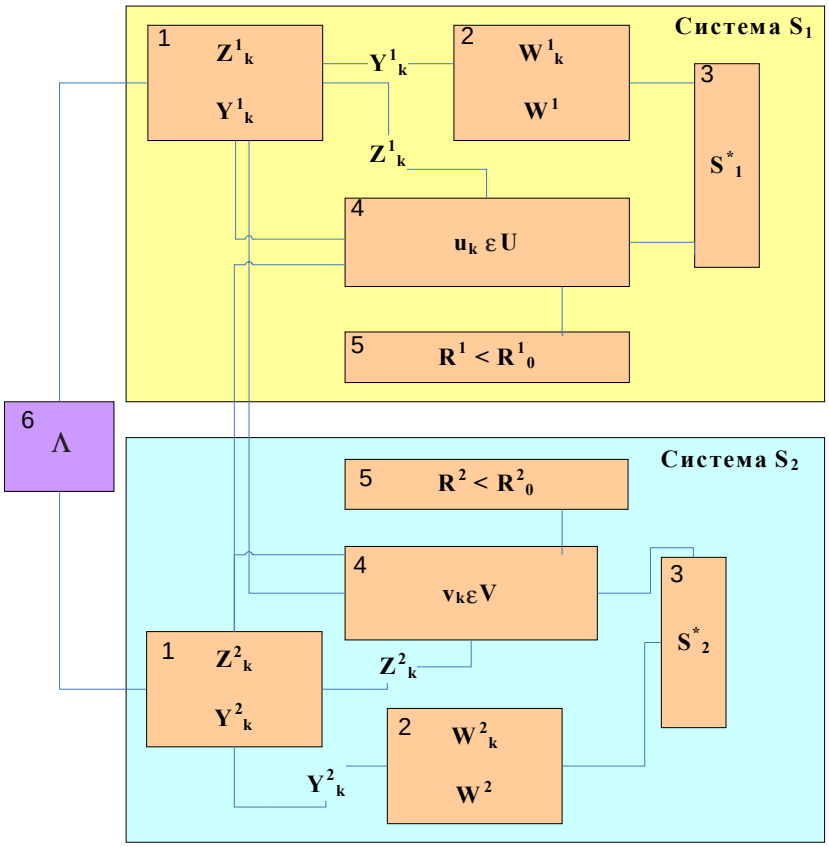

Рис. 2. Структура модели конфликтного взаимодействия средств нарушения ИБ корпоративного портала

Определяющее значение для начала, развития и исхода конфликта имеет объем знаний сторон о ситуации, который используется при выборе управляющих воздействия, а также оперативность сторон в осуществлении этих воздействий. Для этого средства защиты должны иметь возможность получения доступа к накопленной информации о существующих угрозах ИБ и способах их реализации в виде реальных атак. Так, в настоящее время подобный сервис предоставляют множество Интернет-ресурсов (в том числе и на платной основе). Из наиболее популярных и полных можно выделить CERT.ORG, SECURITYFOCUS.COM. Требуемый уровень оперативности реагирования может достигаться путем интеграции средств обнаружения/противодействия и средств реагирования/оповещения, а также она может быть усилена человеческим фактором — организационными мерами. Кроме того, при установлении закономерности рационального поведения корпоративных порталов в конфликте необходимо учитывать влияние на конфликтно-обусловленный выигрыш основных факторов взаимодействия.

СПИСОК ЛИТЕРАТУРЫ:

1. *Пярин В. А., Кузьмин А. С., Смирнов С. Н.* Безопасность электронного бизнеса / Под ред. В. А. Минаева. М., 2002.
2. *Садердинов А. А., Трайнев В. А., Федулов А. А.* Информационная безопасность предприятия: 4-е изд. М., 2007.
3. *Дружинин В. В., Конторов Д. С., Конторов М. Д.* Введение в теорию конфликта. М., 1989.