КАЗАКОВА И. И., ЦАРЕГОРОДЦЕВ А. В., ЦАЦКИНА Е. П.

МАТЕМАТИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ СЦЕНАРНОГО МОДЕЛИРОВАНИЯ ДЕЙСТВИЙ ИНСАЙДЕРА

Аннотация. В статье рассмотрено имитационное моделирование в качестве основы при разработке стратегии противодействия инсайдерской угрозе информационной безопасности. Проведен сравнительный анализ существующих программных комплексов, предназначенных для имитационного моделирования, и выявлен программный пакет, лучше других отвечающий требованиям построения модели поведения внутреннего нарушителя. Описываются внутренние угрозы информационной безопасности компании, а также способы их предотвращения.

Ключевые слова: инсайдер, внутренний нарушитель, имитационное моделирование, информационная безопасность, iThink.

KAZAKOVA I. I., TSAREGORODTSEV A. V., TSATSKINA E. P.

MATHEMATICAL AND INFORMATION SUPPORT OF SCENARY MODELING SYSTEM OF INSIDER ACTIONS

Abstract. The article considers the use of simulation modeling as a basis for developing strategies to counter the insider threat to information security. A comparative analysis of the software systems designed for simulation modeling is conducted. The software package which best meets the requirements of constructing a behavior model of insiders is identified. The article also provides a description of internal threats to the information security of a company and ways to prevent them.

Keywords: insider, simulation modeling, information security, iThink.

В наши дни информационные технологии (ИТ) проникли во все сферы общественной деятельности, и конкурентоспособность организации зачастую зависит от того, насколько эффективно она научилась внедрять, поддерживать, развивать и управлять ими. Ключевым нематериальным активом стала информация. Ввиду этого критически важной для выживания организации стала проблема обеспечения защиты информации и ИТ-инфраструктуры от внешних и внутренних угроз информационной безопасности (ИБ).

Исследования в области обеспечения ИБ до недавних пор концентрировались в основном на противодействии внешним угрозам ИБ (нарушений ИБ организации, совершенных вне предоставляемых полномочий). На тему обеспечения ИБ в условиях внешних угроз разработаны стандарты, методы и средства, претерпевшие несколько циклов совершенствования и в достаточной мере обеспечивающие защиту при правильном внедрении.

Вопрос защиты информационных активов и ИТ-инфраструктуры организации от внутренних угроз ИБ (нарушений ИБ организации, совершенных в рамках предоставляемых полномочий), поднялся не так давно, ввиду этого на данный момент не существует общепринятых подходов защиты информационных активов и ИТ-инфраструктуры от инсайдерской угрозы ИБ.

Инсайдер – это человек, имеющий легальный доступ к информационной системе, и выполняющий неправомерные действия в ней. Инсайдеры могут иметь пароли, которые дают им законный доступ к компьютерным системам. Пароли необходимы для выполнения своих обязанностей. Но такие разрешения могут быть использованы для нанесения вреда организации. Инсайдеры часто знакомятся с данными и интеллектуальной собственностью организации, а также с методами, которые применяются для защиты этих данных. Это помогает инсайдеру обходить известные ему средства и системы контроля доступа. Если инсайдер имеет физический доступ к данным, то ему не нужно взламывать организационную сеть через внешний периметр путем обхода брандмауэров. Вероятнее всего, что они уже находятся в здании, имея прямой доступ к внутренней сети организации. От внутренних угроз защищаться труднее, чем от внешних, так как инсайдер имеет законный доступ к информации и различным активам организации.

Инсайдер может попытаться украсть информацию и имущество в интересах другой организации или страны или в личных интересах. Осуществление угроз и атак может также проводиться с помощью вредоносных программ, которые бывшие сотрудники могли оставить в компьютерных системах. Инсайдерские угрозы – это угрозы, которые наносят существенный вред организации. Классификация этих угроз приведена в таблице 1.

Для предотвращения нарушений ИБ организациям необходимо принимать защитные меры по борьбе с инсайдерами. Для создания эффективных контрмер необходимо иметь больше данных о случаях шпионажа. Организации должны обмениваться этими данными, для того чтобы проводить анализ нарушений и выявлять причины шпионажа. В результате, можно собрать статистику по инцидентам нарушения ИБ и разработать методы борьбы с инсайдерами.

Внутренний нарушитель ИБ лучше понимает ИТ-инфраструктуру и внутреннюю организацию компании, а также действует в рамках предоставленных ему полномочий, ввиду чего его возможности по нанесению ущерба гораздо выше по сравнению с нарушителем внешним

Таблица 1

Классификация инсайдерских угроз

Тип угрозы	Описание
Угроза утечки конфиденциальной информации	Информация, несущая определенную ценность для организации, выносится за ее пределы и может попасть к лицам, которые не имеют прав доступа к этим данным и прав на их использование
Обход средств защиты от утечки конфиденциальной информации	Обман системы защиты путем обхода средств фильтрации почтовых сообщений и веб-трафика
Кража конфиденциальной информации по неосторожности	Подвергание риску секретной информации организации непреднамеренно
Нарушение авторских прав на информацию	Копировать определенные части документа одного автора в документ другого автора, а также в сообщения, передаваемые по почте, и в другие формы передачи информации
Мошенничество	Искажение документации организации, модификация и удаление секретной и важной информации, а также в превышение полномочий доступа к базе данных
Нецелевое использование информационных ресурсов компании	Злоупотребление сетевыми ресурсами
Саботаж ИТ-инфраструктуры	Нанесение существенного вреда организации по личным (чаще всего бескорыстным) мотивам – любой из описанных выше сценариев

Ключевым моментом в решении проблем, препятствующих эффективному решению проблемы инсайдеров, является построение модели внутреннего нарушителя.

Имитационное моделирование – это разновидность аналогового моделирования, реализуемого с помощью набора математических инструментальных средств, специальных имитирующих компьютерных программ и технологий программирования, позволяющих посредством процессов-аналогов провести целенаправленное исследование структуры и функций реального сложного процесса в памяти компьютера в режиме «имитации» и выполнить оптимизацию некоторых его параметров

При достаточном понимании поведения инсайдера и правильном представлении исходной информации имитационные модели характеризуются большей близостью к реальной системе, чем аналитические и численные модели. С помощью имитационного моделирования действий инсайдера и соответствующих современных программных средств можно создавать даже те модели, которые невозможно сформулировать традиционными методами. Кроме того, имитационное моделирование позволяет создавать модели тех

систем, с которыми нельзя провести эксперимент, что позволяет упростить и усовершенствовать управление ими.

Существует два подхода к имитационному моделированию – статический и динамический. Статические модели представляют собой системы уравнений, которые решаются один раз. Динамические модели включают в себя еще одну переменную - время. Модель поведения инсайдера является динамической моделью, так как математические расчеты параметров модели инсайдера выполняются на различных временных интервалах, позволяя тем самым исследовать развитие системы во времени.

На данный момент, существует множество инструментальных средств для моделирования динамики систем, например, iThink, Vensim, Powersim, Process charter и др. Эти продукты более всего различаются стилем моделирования, т. е. средой, посредством которой создаются модели. Например, в пакете Process Charter модель строится с помощью блок-схемы, а Powersim и iThink используют системную динамику. Сравнение пакетов имитационного моделирования представлено в таблице 2.

Таблица 2

Сравнение пакетов имитационного моделирования

Система моделирования	Производитель	Моделирующая среда и поддержка			
		Графическая конструкция ИМ	Авторское моделирование, программирование моделей	Анимация (в реальном времени)	Поддержка анализа результатов
iThink	High Performance System, Inc	CASE-средства, потоковые диаграммы	+	+	Анализ чувствительности
Vensim	Ventana Systems	Потоковые диаграммы	-	+	-
Powersim	Powersim Co.	Потоковые диаграммы	-	+	-
Process charter	Scitor	Блок-схемы	-	+	-

Как видно из таблицы 2, не все данные программные инструменты позволяют смоделировать поведение внутреннего нарушителя. К примеру, анализ чувствительности поддерживает лишь программный пакет iThink. Анализ чувствительности является одним из важнейших характеристик модели инсайдера, так как это дает возможность многократно исполнять модель с различными входными параметрами, чтобы сравнить результаты

нескольких прогонов. Кроме того, iThink использует CASE-средства, в состав которых входят графические средства анализа и проектирования, обеспечивающие создание и редактирование иерархически связанных диаграмм, образующих модель прогнозирования действий инсайдера. Также важной отличительной чертой iThink от других программных пакетов для имитационного моделирования является авторское моделирование, иными словами есть функция создания авторских моделей, с помощью которых разработчик включает в окно модели текст, геометрические изображения и управляющие блоки, чтобы пользователи могли самостоятельно модифицировать модель. На основании данных фактов можно сделать вывод, что для математического обеспечения системы сценарного прогнозирования действий инсайдера лучше всего подходит именно программный комплекс iThink.

Имитационная модель инсайдера разрабатывается для:

1) наглядного отображения влияния различных факторов шпионажа друг на друга (взаимосвязь этих факторов);
2) проведения анализа взаимодействий этих факторов;
3) получения результатов на основе анализа.

Данный подход и инструментальная среда позволяют смоделировать и спрогнозировать поведение инсайдеров. Кроме того, имитационная модель помогает:

- Лучше понимать и обобщать ключевые аспекты шпионажа.
- Обосновывать рекомендации исследования.
- Облегчать идентификацию эффективных контрмер.
- Анализировать поведение инсайдера.
- Исследовать трудные управленческие ситуации.
- Понять природу проблемного поведения нарушителя.
- Увидеть факторы, предшествующие угрозам со стороны инсайдера.
- Принять меры для смягчения или предотвращения преступления.
- Разработать стратегию поведения и тактику противодействия угрозам.
- Проанализировать изменения системы за длительный срок.
- Показать преимущества и недостатки системы.

В модель можно включить различные факторы: политические, административные, культурные, психологические и другие. Исключение этих факторов из модели не даст полного представления об описываемой ситуации. Таким образом, многие проблемы упускают из виду, что отчасти объясняется узкой направленностью в решении проблем.

Кроме того, имитационное моделирование сможет помочь решить следующие вопросы:

- Когда и где будет совершено нападение?
- Какой ущерб оно может нанести организации?
- Можно ли избежать угрозы нападения, если принимать контрмеры?
- Как повлияют современные тенденции в шпионаже на национальную безопасность через несколько лет?
- Какие еще факторы могут повлиять на риск шпионажа (в государственном масштабе)?

Анализ системно-динамической модели привел к таким основным наблюдениям, как:

1) личная предрасположенность и стрессовые события, включая организационные санкции, способствуют увеличению риска совершения правонарушений;

2) подозрительное поведение и технические действия инсайдера предшествуют совершению нарушений или происходят во время проведения шпионажа;

3) организации игнорируют (не реагируют) или не обнаруживают нарушения правил;

4) отсутствие или недостаток физических и электронных средств управления контролем доступа облегчают совершение шпионажа;

5) удачно совершенное преступление и получение вознаграждения за него приводит к увеличению совершения нарушений правил;

6) чрезмерное доверие к сотрудникам приводит к уменьшению проведения аудита и мониторинга;

7) наложение организационных санкций на сотрудника может привести и к уменьшению, и к увеличению совершения шпионских действий.

Имитационная модель поведения внутреннего нарушителя ИБ позволяет провести анализ инсайдерских угроз ИБ в организации и принять соответствующие меры по их минимизации. Она принципиально отличается по сложности, точности и подробности от неформального субъективного объяснения или «вербальной» модели, которую человек обычно формирует для достижения поставленной цели. Кроме того, она помогает выявить слабые места безопасности и предположить стратегию нарушителя. Основываясь на личных склонностях и интересах, профессиональных стрессах, которые приводят к неадекватным поведенческим реакциям и выражаются в совершении нарушений, поощренных недостаточным или несоответствующим вмешательством со стороны руководства, она описывает варианты действий нарушителя.

ЛИТЕРАТУРА

1. Кузнецов Ю. А., Перова В. И., Мичасова О. В. Работа с программным пакетом ITNINK. Учебно-методическое пособие. – Нижний Новгород: Изд-во Нижегородского университета, 2007. – 72 с.

2. Принципы и аксиомы анализа системной динамики [Электронный ресурс]. – Режим доступа: http://all-politologija.ru/knigi/modelirovanie-i-analiz-politicheskix-processov-ozhiganov/principi-i-aksiomi-analiza-sistemnoj-dinamiki.

3. Steven R. et al Band Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis: Technical Report. – Software Engineering Institute, 2006.

4. Обоснование структуры и содержания плана защиты информации с разработкой модели нарушителя [Электронный ресурс]. – Режим доступа: http://savestud.su/freework/4/Obosnovanie-strukturi-i-soderzhaniya-plana-zashchiti-informatsii-s-razrabotkoy-modeli-narushitelya-CHast-1.html.

5. Описание возможных нарушителей [Электронный ресурс]. – Режим доступа: http://ms.znate.ru/docs/151/index-64933.html?page=3.