УДК 004.056

Адаптивное управление средствами защиты от инсайдерских атак в информационных системах специального назначения

В 2010 и 2013 гг. мировой общественный резонанс получили инциденты разглашения секретной информации, связанные с деятельностью специалиста по анализу информации Бредли Мэннинга и сотрудника Агентства национальной безопасности США Эдварда Сноудена. Как правило, основная причина утечки информации ограниченного распространения в этих и многих других подобных случаях [1], которые собственники скомпрометированных сведений предпочитают не разглашать, является низкая эффективность современных систем защиты информации от инсайдерских атак в информационных сетях. В статье рассматривается возможный подход к адаптивному управлению средствами защиты от инсайдерских атак, разработанный авторским коллективом при выполнении ряда научно-исследовательских работ.

Л.Л. УТИН,
начальник кафедры связи УО «БГУИР»,
канд. техн. наук, доцент

С.Н. КАСАНИН,
начальник военного факультета УО «БГУИР»,
канд. техн. наук, доцент

А.Р. МАЦЫЛЕВИЧ,
научный сотрудник ГУ «НИИ ВС РБ»

А.В. ФЕДОРЦОВ,
научный сотрудник ГУ «НИИ ВС РБ»

Введение. Результатом незаконной деятельности пользователей на средствах вычислительной техники (СВТ), подключенных к информационным системам, является инсайдерская атака. Под инсайдерской атакой понимают форму нарушения безопасности информации, вызванную деятельностью пользователей, имеющих санкционированный доступ к ресурсам и инфраструктуре информационной системы с определенными полномочиями. Выявление и принятие адекватных мер по противодействию атакам подобного типа является сложной проблемой, что обусловлено увеличением объема памяти машинных носителей информации (МНИ) с одновременным снижением их габаритных размеров [2–4]. В результате при недостаточной эффективности мер защиты, реализованных в информационных системах, пользователи, имеющие к ней доступ, могут за непродолжительное время скопировать большие объемы информации, хранимой на СВТ, и незаметно вынести ее за пределы контролируемой зоны.

Как правило, положение усугубляется недостаточной автоматизацией процессов контроля действий пользователей на СВТ. Кроме того, привлечение к построению системы защиты специалистов, имеющих лишь базовые знания об устройстве и функционировании СВТ, при одновременном отсутствии специализированных компьютерных программ, позволяющих своевременно выявлять незаконную деятельность пользователей на СВТ, создает потенциальную опасность утечки информации ограниченного распространения.

Основная часть. В основе одного из простых решений противодействия инсайдерским атакам лежит признание всех лиц, допущенных к работе на СВТ из состава информационной системы, потенциальными нарушителями и применение для них

одинаковых организационных и технических мер защиты. Однако такой подход приводит к определенной избыточности в создаваемой системе защиты, является экономически расходным. Кроме того, снижение доверия к должностным лицам может негативно сказаться на их морально-психологическом состоянии при выполнении задач по предназначению [4, 5].

Одной из первых решением проблемы противодействия инсайдерским атакам стала заниматься научно-исследовательская компания *IDC*. Специалисты данной компании уже в 2006 г. предложили классифицировать инсайдеров на лояльных (граждане, нарушители) и злонамеренных (отступники, предатели) [1].

В результате анализа классификационных признаков, предложенных компанией *IDC*, была сформирована таблица 1, содержащая обобщенные характеристики типов инсайдеров.

Подход компании *IDC* к классификации инсайдеров имеет следующие недостатки.

Во-первых, не анализируется мотивация нарушителей. Во-вторых, не учитываются опыт нарушителей и используемые методы для достижения поставленных целей. В-третьих, нет четкой привязки действий нарушений с основными параметрами безопасности информационных ресурсов, как целостность, подлинность, конфиденциальность, доступность и сохранность информации. В-четвертых, характер угроз активам компании не связан с потенциальным и реальным ущербом, который может быть нанесен информационным ресурсам. При этом не совсем ясно, какие угрозы хуже – случайные, серьезные или реальные.

Большую практическую ценность представляет подход к классификации инсайдеров, предложенный российской компанией *InfoWatch*. Специалисты данной компании делят инсайдеров на халатных, манипулируемых, обиженных, нелояльных, подрабатывающих и внедренных [1] (таблица 2).

Предложенный компанией *InfoWatch* подход позволяет учесть особенности поведения, цели и мотивацию нарушителей при совершении инсайдерской атаки. В результате подход может использоваться при расследовании инцидентов, произошедших в организации, и поиске виновных. Следует отметить, что специалистами компании разработано большое количество программных комплексов, отдельные из которых имеют лицензии в Республике Беларусь и могут применяться для защиты информационных систем от инсайдерских атак [6].

Вместе с тем и предложенный подход компании *InfoWatch* имеет ряд замечаний, к основным из которых можно отнести следующие.

Во-первых, при выборе классификационных признаков основной упор был сделан на характеристиках групп пользователей, имеющих доступ к ресурсам информационных систем компании. В результате не рассматриваются сотрудники, имеющие постоянный или временный доступ к работе на автономных СВТ.

Во-вторых, не учитывается уровень доступа пользователей к информационным ресурсам и средствам защиты информационных ресурсов. В результате не рассматривается такой важный признак, как заданный уровень доверия к пользователю со стороны службы безопасности.

В-третьих, предложенная классификация позволяет разработать типовые сценарии действий различных групп пользователей и выработать необходимый и достаточный комплекс мер для защиты от типовых инсайдерских атак. Как правило, такой комплекс мер носит статический характер, а следовательно, не может быть адаптирован к изменяющемуся поведению пользователей.

В-четвертых, подход компании *InfoWatch* не позволяет оценивать действия пользователя по величине потенциального (реального) ущерба, который может быть нанесен им в результате неправомерных действий.

Устранение указанных замечаний позволит повысить эффективность разрабатываемых средств защиты информации по противодействию инсайдерским атакам.

В ходе проведенного анализа характерных признаков действий инсайдеров по реализации угроз

Таблица 1 – Характеристики типов инсайдеров (подход компании IDC)

Тип инсайдеров	Периодичность нарушения	Характер нарушения	Характер угроз активам компании
Граждане	Крайне редко	Возникают по неосторожности	Не представляют
Нарушители	Редко	Действия носят, в основном, неумышленный характер и связаны с применением компьютерных программ и информационных ресурсов, не разрешенных к использованию	Случайные
Отступники	Часто	Действия носят умышленный характер и связаны с злоупотреблением своими привилегиями по доступу к информационным ресурсам (в том числе интернет) в обход имеющихся средств защиты, допускаются факты передачи за пределы контролируемой зоны отдельной информации	Серьезные
Предатели	Регулярно	Действия носят умышленный характер и связаны со скрытым хищением информации	Реальные

Таблица 2 – Характеристика типов инсайдеров (подход компании *InfoWatch*)

Тип инсайдеров	Особенности поведения	Опыт работы в сфере информационных технологий	Мотивация		Цели	Характер угроз	Действия при отказе доступа к ресурсам	Постановка задач	Скрытие фактов атаки
			Умысел	Корысть					
Халатные	Невнимательные, неосторожные	Низкий	Нет	Нет	Нет	Ненаправленные	Обращение к коллегам или администратору	Нет	Нет
Манипулируемые	Ставшие жертвами мошенничества	Низкий	Нет	Нет	Нет	Неумышленные	Обращение к коллегам или администратору	Путем мошенничества	Нет
Обиженные (саботажники)	Собирающиеся продолжать работать, но считающие, что их деятельность не была по достоинству оценена (низкая зарплата, невысокая должность, отсутствие поощрений и .т. д.)	Средний	Да	Нет	Нанесение ущерба, компрометация, шантаж	Направленные на нарушение конфиденциальности целостности, сохранности и доступности	Изменение целей атаки (уничтожение материальной собственности)	Самостоятельно	Да
Нелояльные	Собирающиеся увольняться с работы и осуществляющие сбор любой информации «на всякий случай»	Средний	Да	Нет	Хищение баз данных, персональных данных клиентов, интеллектуальной собственности	Ненаправленные (уносят максимум информации, не вникая в ее ценность)	Имитация уважительной причины	Самостоятельно	Нет
Подрабатывающие	Решившие дополнительно заработать, или ставшие жертвами шантажа	Средний	Да	Да	Заработок путем продажи информации, выполнение требований шантажистов	Направленные на нарушение конфиденциальности	Отказ от атаки, изменение целей атаки, имитация уважительной причины, подкуп коллег, взлом системы защиты	Самостоятельно или под руководством внешнего заказчика	Да
Внедренные	Устраивающиеся на работу в подразделения по защите информации с хорошими рекомендациями, работающие до момента получения прав доступа к информационным ресурсам	Высокий, могут использовать программно-аппаратные средства взлома системы защиты информации	Да	Да	Хищение, модификация или уничтожение информационных ресурсов	Направленные на нарушение конфиденциальности целостности, сохранности и доступности	Взлом системы защиты	Под руководством внешнего заказчика	Да

нанесения ущерба в информационных сетях было определено, что инсайдеры, как правило, действуют по определенным сценариям. Базовый набор действий и логическая последовательность их выполнения нарушителем при осуществлении незаконной деятельности на СВТ имеет вид, представленный на рисунке 1.

Исследования, проведенные в области защиты информации, показывают, что наибольшая эффективность в противодействии инсайдерским атакам обеспечивается путем создания в организациях объединенной системы обеспечения безопасности связи и защиты информации, при условии наличия в ней подсистемы мониторинга угроз и оценки эффективности мер, принятых по их

Рисунок 1 – Базовый сценарий действий нарушителя при осуществлении атаки

нейтрализации. Для описания процессов управления системой обеспечения безопасности связи и защиты информации целесообразно использовать процессную модель управления Деминга. Реализация процессного подхода позволяет связать в замкнутый цикл мероприятия по планированию мер защиты, их реализации на практике, проверке эффективности нейтрализации угроз безопасности связи, корректировке спланированных мероприятий [5].

С учетом изложенного выше разработан подход к адаптивному управлению средствами защиты информации, сущность которого заключается в следующем:

1. Устанавливается принадлежность пользователей к заданной группе ($Г_x$,).

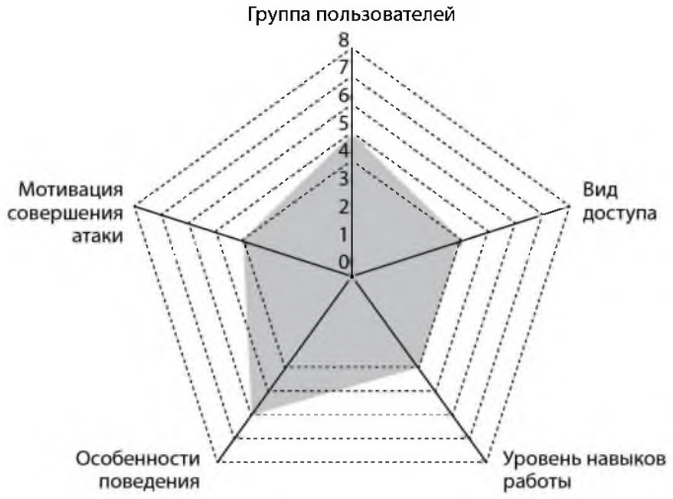

Рисунок 2 – Вариант портрета пользователя ОИ СВТ

Возможен следующий перечень групп: не имеющие доступ к СВТ; имеющие доступ к автономному СВТ; имеющие доступ к СВТ, подключенным к локальным информационным системам; имеющие доступ к СВТ, подключенным к распределенной информационной системе; имеющие доступ к системе защиты информации. Учет групп пользователей необходим для расчета возможностей инсайдеров нанести ущерб информационным ресурсам в зависимости от условий эксплуатации СВТ и определения необходимого и достаточного количества средств защиты информации с учетом критерия разумной достаточности и необходимости выполнения требований действующих нормативных правовых актов в сфере защиты информации.

2. Для каждого пользователя определяются соответствующие ему права доступа ($Д_x$): разрешение на чтение информации; разрешение на модификацию информации; разрешение на копирование (печать) информации; разрешение на удаление информации. Учет вида доступа позволяет при проведении расчетов определить потенциальную возможность инсайдера по нарушению конфиденциальности, целостности, сохранности, подлинности и доступности информационных ресурсов, а также задать допустимый объем информации, который за установленный промежуток времени пользователь имеет право копировать на МНИ.

3. По результатам тестирования определяется уровень навыков пользователя в работе с информационными технологиями ($У_x$), который необходим для уточнения весовых коэффициентов, влияющих на способность пользователя в заданные сроки совершить инсайдерскую атаку. Предложено задавать четыре уровня: низкий; средний; высокий; профессиональный.

4. Для каждого пользователя определяются особенности его поведения ($П_x$): (ответственный, наивный, легкомысленный, небрежный, халатный, агрессивный, корыстный, другие). Особенности поведения пользователей позволяют определить минимальный набор мер безопасности, необходимый и достаточный для предотвращения атаки конкретным пользователем.

5. Для каждого пользователя определяется возможная мотивация совершения атаки ($М_x$). Возможны следующие типы мотивации: отсутствие мотивации; обеспечение комфортной работы на СВТ; получение материальной выгоды; действия по религиозным, политическим, расовым, националистическим, идеологическим убеждениям; демонстрация пренебрежения к требованиям нормативных правовых актов в области защиты информации; совершение действия в результате обмана, злоупотребления доверием, шантажа.

Данный параметр является дополнением к параметру $У_x$ и позволяет учитывать причины совершения нарушения для конкретизации возможностей пользователя в заданные сроки совершить инсайдерскую атаку.

6. Осуществляется построение портрета пользователя (рисунок 2).

7. С заданной периодичностью осуществляется контроль СВТ с оценкой действий пользователя за рассматриваемый период. При этом осуществляется построение текущего профиля и сравнение его с заданным. При обнаружении нарушений уровень полномочий пользователя по доступу к ресурсам и инфраструктуре изменяется, вплоть до полной блокировки СВТ.

Заключение. Разработанный подход к адаптивному управлению средствами защиты информации позволяет:

- учитывать условия эксплуатации СВТ;
- оценивать потенциальные возможности пользователей совершать инсайдерскую атаку с учетом мотивации, уровня навыков работы и целей атаки;
- оптимизировать использование ресурсов системы защиты информации на СВТ путем определения для конкретного типа пользователей их минимального набора, необходимого и достаточного для недопущения незаконной деятельности;
- определить потенциальный ущерб, который конкретный пользователь может нанести информационным ресурсам и организации в целом;