УДК 004.056.4

ОЦЕНКА ЭФФЕКТИВНОСТИ АТАК ЗЛОУМЫШЛЕННИКА В ПРОЦЕССЕ ПОСТРОЕНИЯ ЕГО МОДЕЛИ

А.И. Спивак

Проектирование системы защиты информации всегда сопровождается созданием модели нарушителя безопасности. Общеизвестным подходом является использование характеристик злоумышленника в качестве основных параметров для оценки атак на систему защиты. Изменение свойств объекта защиты может быть использовано для выполнения оценки действий нарушителя безопасности.
Ключевые слова: модель, безопасность, злоумышленник, оценка, информация.

Введение

В процессе построении системы информационной безопасности на одном из этапов производится оценка эффективности атак злоумышленника. На основе данных об объекте защиты и возможных атаках строится модель защиты. Полнота описания угроз безопасности, а также правильность модели нарушителя позволяют системе защиты информации учитывать большую часть атак и иметь адекватные меры по препятствованию их реализации.

Сложность оценки обусловливается широким спектром характеристик нарушителя. Наряду с очевидными, такими как техническая оснащенность злоумышленника, его профессиональная подготовка, обеспеченность вычислительными мощностями, методы воздействий, мотивационные факторы, существуют и другие переменные характеристики. Их количество, характер, взаимосвязи, а также количественные показатели являются сложно прогнозируемыми величинами. В связи с этим возникает необходимость в оценке воздействия злоумышленников на систему защиты информации, не учитывающей характеристики нарушителей безопасности.

Существующие подходы к построению модели нарушителя

Основные подходы к решению задачи оценки эффективности атак злоумышленника реализуются в рамках построения модели нарушителя. Остановим свое внимание на описательной части построения модели нарушителя, включающей в себя этап оценки эффективности действий злоумышленника по преодолению системы защиты объекта. Одной из используемых методик построения описательной части такой модели является использование в качестве основополагающего фактора осведомленности [1]. Знания злоумышленника о системе защиты информации существенно повышают вероятность реализации угрозы информационной безопасности. Выделяют несколько уровней осведомленности – от самого высокого до самого низкого. К высокой степени осведомленности относится злоумышленник, которому известна вся проектная документация, и на основе этой информации он обладает данными об уязвимых точках системы. Нарушитель с низким уровнем знаний об объекте имеет информацию только о внешних, общедоступных составляющих системы, и предполагается, что вероятность реализации атаки таким нарушителем ниже, чем злоумышленником с высоким уровнем знаний о системе защиты.

Другим подходом является ранжирование по виду доступа, которым обладает потенциальный нарушитель безопасности [2]. В зависимости от особенностей работы различные категории пользователей системы имеют разные права доступа. Обычный пользователь системы может пользоваться только строго определенным набором средств, список которых и выполняемые действия регламентированы. При этом администратор безопасности обладает доступом ко всем системам обеспечения безопасности и имеет гораздо больше полномочий и, как следствие, возможностей для атаки на систему защиты. Разграничение доступа к системе определяет различные способы для реализации угроз безопасности. Вероятность успешности атаки лежит в прямой зависимости от типа доступа злоумышленника к системе.

Эффективность действий злоумышленника при использовании описанных подходов является производной величиной от характеристик, связанных с нарушителем. В случае с осведомленностью полнота знаний о системе защиты позволяет говорить о большой эффективности действий злоумышленника по реализации угрозы безопасности. Аналогичное значение имеет тип доступа к системе во втором подходе. Данные виды оценки базируются только на одной из характеристик злоумышленника. При учете одновременно двух подходов образуется сложность в выявлении взаимных влияний со стороны различных характеристик. Дальнейшее расширение списка параметров субъекта воздействия вызовет еще большее усложнение процесса построения модели [3].

Оценка эффективности атак на основе изменения вероятности реализации угрозы безопасности

Одним из возможных вариантов решения может служить подход к оценке эффективности атак злоумышленника на основе изменения вероятности достижения цели нападения. Если принять во внимание, что конечной целью является оценка эффектив-

ности действий злоумышленника по реализации угрозы безопасности, то данный подход представляется более универсальным, чем другие. Оценку можно проводить по показателям, определяющим состояние защищаемого объекта, а именно изменение вероятности быть взломанным под воздействием нарушителей. Отличие от существующих подходов заключается в том, что характеристики объекта защиты являются основными при измерении эффективности действий злоумышленника. В таком случае оценка эффективности осуществляется с точки зрения приближения злоумышленника к цели в результате реализации угрозы безопасности. Переориентирование акцента на оценку изменений в свойствах защищаемого объекта позволяет упростить описательную часть построения модели нарушителя. Вместо расчета разнообразных характеристик злоумышленника, учета их взаимосвязей и взаимовлияний достаточно измерить только один параметр объекта воздействия, на который направлены действия нарушителя безопасности.

Одновременно интересен вопрос возможного способа измерения вероятности реализации угрозы безопасности при использовании ориентированного на объект защиты подхода. Характеристики объекта защиты служат тем фактором, изменение которого позволяет связать эффективность действий злоумышленника и приближение его к цели этого воздействия – взлому. Система защиты информации включает в себя некоторое количество уровней безопасности, и злоумышленнику для реализации угрозы нужно их преодолеть. Условимся считать, что рассматриваемые уровни защиты одинаковы по своим характеристикам, а сложность их преодоления злоумышленником не меняется в зависимости от свойств конкретного уровня. Знания о количестве уровней превалируют над информацией об их параметрах, влияющих на их прохождение злоумышленником в процессе взлома. Одним из возможных способов измерения вероятности взлома можно назвать количество пройденных нарушителем за время атаки уровней. Сопоставление данного числа с общим количеством уровней защиты приведет к получению изменения вероятности взлома системы защиты.

Деструктивное воздействие

Введем понятие деструктивного воздействия, которому поставим в соответствие действия злоумышленника, приводящие к снижению общего уровня безопасности объекта. В действительности такого рода воздействия могут представлять собой широкий круг угроз безопасности, таких как нарушение целостности объекта защиты, его конфиденциальности, злонамеренное блокирование доступа к защищаемому объекту.

Формулировка понятия указывает на то, что действия строго направлены на преодоление уровней безопасности объекта защиты и приводят, в конечном счете, к увеличению вероятности реализации угрозы.

Определим способ, который используется для оценки деструктивного воздействия. Очевидно, что деструктивное воздействие направлено на достижение конкретной цели. Деструктивное воздействие подобно понятию ценности информации. Воздействие, также как и получение информации, направлено на достижение цели, т.е. в результате этого воздействия вероятность достижения цели либо не меняется (воздействие ни к чему не привело), либо происходит приближение к цели (вероятность достижения цели возрастает), возможно также уменьшение вероятности вследствие получения неверной информации (дезинформации). Использование соотношения Корогодина [4] для оценки ценности является наиболее удобным способом представления деструктивного воздействия злоумышленника. Такое представление позволяет связать вероятности реализации угроз безопасности до и после момента измерения с действиями злоумышленников между выполняемыми измерениями. Соотношение имеет вид

$$C_i = \frac{P_i - p_i}{1 - p_i},$$

где p_i – вероятность достижения цели до начала деструктивного воздействия для i-го объекта, P_i – вероятность достижения цели после окончания деструктивного воздействия для i-го объекта, C_i – величина деструктивного воздействия для i-го объекта. Значение деструктивного воздействия лежит в пределах от 0 до +1, что позволяет говорить о деструктивном воздействии как о приращении вероятности реализации угрозы безопасности после деструктивного воздействия со стороны злоумышленника.

Достаточно важным представляется момент оценки собственно вероятности реализации угрозы безопасности. Возможным вариантом такой оценки является предположение о том, что реализация угрозы безопасности зависит от количества уровней защиты на конкретном защищаемом объекте. При увеличении количества таких уровней вероятность реализации угрозы безопасности объекта защиты будет стремиться к обратно пропорциональной зависимости от числа уровней защиты. Чем больше уровней защиты фигурирует в соотношении, тем более корректно оно отображает связь между вероятностью реализации угрозы и количеством уровней защиты. Это утверждение очевидно: чем больше уровней защиты нужно преодолеть злоумышленнику для взлома системы, тем меньше вероятность реализации угрозы.

Вероятность реализации угрозы (p_i) для i-го объекта будет равна

$$p_i \sim \frac{1}{n_i},$$

где n_i – количество уровней защиты i-го объекта. Использование данного выражения позволяет соотношению деструктивного воздействия обрабатывать информацию о количестве уровней защиты, которое имеет объект защиты, и на основе этого формировать значение вероятности реализации угрозы. Затем информация об уровнях защиты, которые были преодолены злоумышленником в процессе воздействия, используется для вычисления деструктивного воздействия. Если известно количество уровней защиты, которые злоумышленник в результате деструктивного воздействия смог преодолеть, то можно выполнить оценку величины этого деструктивного воздействия, используя соотношение

$$p_i \sim \frac{1}{n_i - s_i} - \frac{1}{n_i},$$

где n_i – количество уровней защиты i-го объекта, s_i – количество взломанных уровней защиты i-го объекта, p_i – вероятность реализации угрозы безопасности i-го объекта. При $n_i=s_i$ $p_i = 0$, так как деструктивное воздействие ни к чему не привело, приращение вероятности реализации угрозы в этом случае равно нулю.

Использование величины деструктивного воздействия можно связать с эффективностью действий злоумышленника. Деструктивное воздействие, как было показано, характеризуется вероятностью реализации угрозы безопасности, а именно ее изменением. Чем выше вероятность реализации угрозы, тем больше воздействие на систему защиты объекта и тем более эффективными являются действия злоумышленника. Таким образом, величина деструктивного воздействия соответствует эффективности действий злоумышленника, так как отражает успешность действий нарушителя безопасности.

Использование величины деструктивного воздействия

Рассмотренная величина может использоваться для оценки эффективности действий злоумышленника при условии ограниченности или полного отсутствия знаний о

нарушителе безопасности. В таком случае можно опираться при оценке на показатели безопасности объекта защиты, а именно изменение вероятности реализации угрозы. Одной из предложенных для измерения характеристик является количество преодоленных нарушителем уровней защиты системы безопасности. Подход не исключает использование других характеристик, а также их сочетаний.

Заключение

Описанный способ оценки эффективности действий злоумышленника является дополнительным инструментом для построения описательной части модели нарушителя. Совокупность различных подходов к оценке воздействий позволяет получить наиболее полную модель угроз безопасности, а на ее основе спроектировать адекватный набор мер по эффективному противодействию угрозам безопасности.

Возможность базирования в оценке воздействий на систему защиты информации не на характеристики злоумышленника, а на результаты его действий является важным инструментом при построении модели системы защиты информации.

Литература

1. Дровникова И.Г., Буцынская Т.А. Модель нарушителя в системе безопасности // Системы безопасности. – 2008. – №5.
2. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – М.: Военное издательство, 1992. – 12 с.
3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия–Телеком. 2004. – 280 с.
4. Корогодин В.И., Корогодина В.Л Информация как основа жизни. – Дубна: Феникс+, 2000. – 208 с.

Спивак Антон Игоревич – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, аспирант, anton.spivak@gmail.com