УДК 330.42

РАЗРАБОТКА МОДЕЛЕЙ ОПТИМИЗАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ОЦЕНКИ СТРАХОВАНИЯ ИНФОРМАЦИОННЫХ РИСКОВ

Табаков А.Б. – аспирант

Финансовая академия при Правительстве РФ

В статье предложена и описана математическая модель оптимизации системы информационной безопасности организации, основанная на теории графов и на теории вероятности.

Информационная безопасность – один из главных приоритетов современного бизнеса, поскольку нарушения в этой сфере приводят к гибельным последствиям для бизнеса любой компании. Применение высоких информационных технологий XXI века, с одной стороны, дает значительные преимущества в деятельности предприятий и организаций, а с другой – потенциально создает предпосылки для утечки, хищения, утраты, искажения, подделки, уничтожения, копирования и блокирования информации и, как следствие, нанесение экономического, социального или других видов ущерба, т.е. проблема информационных рисков и нахождения путей снижения ущерба становится с каждым годом все острее.

Практика функционирования автоматизированных информационных систем показывает, что достижение 100 %-го уровня безопасности – дело дорогое и не всегда целесообразное, так как:

- даже самая совершенная на сегодня система информационной защиты не может противодействовать угрозам, которые могут возникнуть в последующем;

- стоимость комплексной защиты может оказаться значительно выше, чем стоимость защищаемых информационных ресурсов.

Важность проблемы защиты информации в нашей стране подчеркивает факт создания доктрины информационной безопасности по инициативе Президента Российской Федерации. Методы обеспечения информационной безопасности Российской Федерации, согласно Доктрине, разделяются на правовые, организационно-технические и экономические.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования, совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Именно соединение классических (программных и технических) методов защиты информации и механизма страхования могут помочь компании создать наиболее надежную систему информационной безопасности (СИБ).

К сожалению, страхование информационных рисков продолжает оставаться в нашей стране эксклюзивным видом страхования. Основная причина этого заключается в стоимости услуги. Профессиональные андеррайтеры, работающие в страховых компаниях, не могут искусственно занижать размер страховых тарифов в погоне за потенциальными клиентами. Необходимо помнить, что именно из собираемых страховщиками премий формируется фонд, который впоследствии идет на компенсацию убытков страхователей. Недобор премий из-за несоответствия величины риска тарифной ставки может привести к тому, что страховым компаниям будет просто не из чего осуществлять выплаты в случае массового наступления страховых случаев.

Однако, учитывая тот факт, что в столь новом виде страхования, как страхование информационных рисков, еще не существует жестких стандартов работы с клиентами, и то, что страховщикам приходится пропагандировать индивидуальный подход к потенциальным клиентам, страхователь может торговаться по поводу стоимости своей страховой защиты. Причем торг этот должен идти на основе математических выкладок, аргументированно доказывающих, что работа по обеспечению информационной безопасности ведется и осуществляется на должном уровне.

Страхователь должен четко представлять, что чем больше он потратил на безопасность своей информационной системы, чем надежней СИБ, тем ниже вероятность того, что злоумышленнику удастся проникнуть и нарушить целостность хранящейся информации, тем меньше ему придется заплатить страховой компании за полис.

Большую помощь в построении эффективной СИБ могут оказать методы математического моделирования. Во-первых, именно с их помощью можно наглядно доказать менеджерам, что вложение средств в СИБ действительно экономит деньги компании (недооценка необходимости СИБ менеджерами компании является в большинстве случаев основным препятствием в ее развитии). Во-вторых, в условиях ограниченности ресурсов, отпущенных на СИБ, с помощью этих методов можно выбрать наиболее оптимальный комплекс средств защиты, а также смоделировать, насколько созданная СИБ окажется эффективной в борьбе против наиболее распространенных угроз. В рамках данной статьи рассматривается моделирование несанкционированного доступа (НСД).

Решение первой задачи можно осуществить с помощью модели, основанной на использовании коэффициента *roi*, определяемого по формуле:

$$roi = \frac{\Delta Доходы - \Delta Расходы}{\Delta Инвестиции},$$

где *roi* – показатель изменения ROI *(Return on Investment)* из-за инвестиций в ИБ;

$\Delta Доходы$ – изменение в доходах, обусловленное инвестициями в ИБ;

$\Delta Расходы$ – изменение в расходах, обусловленное инвестициями в ИБ;

$\Delta Инвестиции$ – инвестиции, сделанные в ИБ.

Прямого влияния на рост доходов система информационной безопасности не имеет, поэтому, как правило, не следует ожидать увеличения выручки компании после инвестиций в СИБ. Однако нельзя $\Delta Доходы$ сразу приравнивать к нулю, так как существует ряд стандартных информационных систем, в которых именно грамотно построенная система защиты информации сказывается на росте доходов компании. Например, согласно исследованиям компании PriceWaterhouseCoopers, именно недостаточно обеспеченная безопасность электронных платежей стала основным барьером для пользователей, т.е. создание надежной СИБ в таких системах обусловливает доверие клиентов, а значит, и приток денег.

Внедрение системы информационной безопасности, как правило, приводит к более продуктивному использованию рабочего времени сотрудниками. Это связано, например, с ограничением доступа к информации, не требующейся для работы, в результате исключается доступ к развлекательным сайтам, а также уменьшается объем неслужебной переписки.

При построении СИБ обойтись без расходов невозможно, так как всегда присутствуют операционные затраты: это и разработка проекта, и обучение, и создание средств защиты информации. Но есть составляющие, которые могут это компенсировать и даже привести к снижению расходов после реализации проекта.

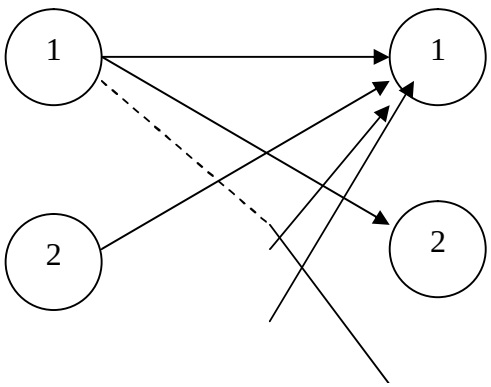
Главное направление уменьшения расходов, т.е. то, ради чего система информационной безопасности строится или модернизируется, – увеличение рискозащищенности.

Для эффективного функционирования системы информационной безопасности предприятия её необходимо оснастить комплексом аппаратных и программных средств защиты от различных информационных угроз таким образом, чтобы улучшить некоторый критерий оптимальности создания СИБ. При этом считается, что информационные угрозы между собой не связаны.

В общем случае полагаем, что задано множество информационных угроз (ИУ), которые могут возникнуть в автоматизированной информационной системе (АИС) предприятия, и множество аппаратных и программных средств защиты (СЗ), с помощью которых эти угрозы могут быть нейтрализованы. Причем для каждого сочетания ИУ–СЗ определено число $r_1(ij)$ – эффективность нейтрализации *i*-м средством защиты *j*-й информационной угрозы. Для построения математической модели введем переменную *y(i,j),* равную 1, если *j*-я ИУ нейтрализуется с помощью *i*-го СЗ, и равную нулю в противном случае.

Дадим содержательную и формальную постановку задач выбора оптимальной СИБ в терминах теории графов, а также представим методы их решения. Для этого построим такой двудольный граф *G (X,U),* ($X = \cup X_i$, i = 1,2), что вершины множества в X_1 отвечают аппаратным и программным средствам защиты, а вершины множеств в X_2 – соответствующим информационным угрозам (рис. 1). Каждый элемент (вершина) множества X_1 характеризуется ценой и эффективностью по нейтрализации информационных угроз.

$X_1 X_2$



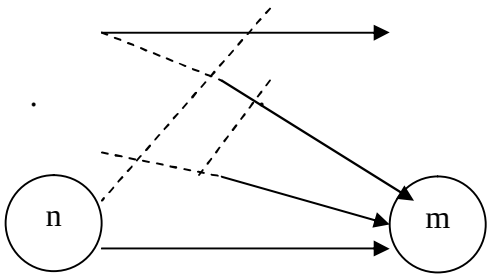


Рисунок 1 – Двудольный граф

Каждой вершине множества X / X_2 присваивается вес, равный стоимости, что соответствует СЗ, а каждой дуге $(i,j) \in U$ – вес, $z(i,j)$ = 1,0. Тогда задача выбора оптимальной СИБ будет заключаться в максиальной эффективности нейтрализации множества информационных угроз различными средствами защиты при ограничениях на объем затрат Q. Формальная постановка задачи имеет следующий вид:

$$\sum_{j=1}^{m}\sum_{i=1}^{n} r_1(ij)\,y(ij) \Rightarrow max$$

при ограничениях

$$\sum_{i=1}^{n} r_2(i) * sign\sum y(ij) \le Q,$$

$$x_j \in X_2$$

$$\forall x_j \in X_2, \sum^{n} y(ij) = 1;$$

$$x_i \in X_1$$

$$\forall (ij) \in U, y(ij) = 1{,}0.$$

где $r_2(i)$ – затраты на приобретение i-го СЗ.

Если необходимо минимизировать затраты на средства защиты от информационных угроз в АИС предприятия при ограничении на заданный уровень эффективности P, то формальная постановка задачи будет иметь вид:

$$n\ m$$

$$\sum_{i=1} r_2(i) * sign \sum_{j=1} y(ij) \Rightarrow min$$

$$\sum_{j=1}^{m} \sum_{i=1}^{n} r_1(ij) y(ij) / \sum_{i=1}^{n} (max\, r_1(ij)) \le P;$$

$$\forall x_j \in X_2, \sum y(ij) = 1;$$
$$x_i \in X_1$$

$$\forall (ij) \in U, y(ij) = 1{,}0.$$

В данной модели предполагается, что наивысший уровень эффективности СИБ будет тогда, когда для нейтрализации каждой угрозы будет выбрано средство защиты с максимальной эффективностью. Наивысший уровень эффективности СИБ равен сумме максимальных элементов в каждом столбце матрицы $r_1(ij)$.

Следует учитывать, что выбор наиболее оптимального набора классических средств защиты информации в условиях ограничения на объем ресурсов не гарантирует того, что данная система действительно окажется эффективной при противодействии информационным рискам. При этом следует учитывать, что практическое применение механизма страхования, а значит, и создание эффективной СИБ становится возможным лишь в случае, если вероятность наступления рисков причинения вреда АИС компании является достаточно малой величиной.

Рассмотрим модель, позволяющую определить вероятность причинения вреда АИС компании при НСД.

Защита от НСД строится на практике как последовательность преград, после успешного преодоления которых злоумышленник получает доступ к информационным и/или программным ресурсам АИС.

Нарушитель в состоянии проникнуть в систему лишь при условиях, когда:

- во-первых, ему станет известна (в том числе случайным образом) система защиты в части, необходимой для достижения его целей;
- во-вторых, он успеет получить доступ к информационным и/или программным ресурсам системы до того, как эта система защиты видоизменится (после чего перед нарушителем возникнет проблема повторного преодоления защитных преград);

Обозначим через k_j номер преграды, препятствующей доступу к информации j типа. Тогда вероятность того, что изначально безошибочная информация j в процессе хранения в базе данных не окажется умышленно искаженной из-за НСД к моменту выдачи пользователю $P_{инф.j}$ определяется выражением:

$$P_{инф.j} = 1 - \prod_{k_j=0}^{n} P_{n.n.j},$$

где $P_{n.n.j}$ – вероятность преодоления преграды;

n – количество преград системы защиты.

При условии существования стационарных распределений времени между соседними изменениями параметров системы защиты и времени вскрытия системы защиты, вероятность преодоления преграды существует, она равна:

$$P_{\text{прегр}} = f \int_0^{\infty} (1 - F_{\text{смены}}(t)) G_{\text{преод.}}(t) dt,$$

где $F_{смены}$ – функция распределения времени между соседними изменениями параметров преграды системы защиты;

f – величина, обратная математическому ожиданию времени между соседними изменениями параметров системы защиты, $G_{преод.}$ – функция распределения времени преодоления преграды системы защиты.

Исходя из этого выражения, можем записать формулу вероятности преодоления всей системы защиты, то есть преодоление всей последовательности преград механизмов защиты:

$$P_{\text{прегр}} = \prod_{k=1}^{n} f \int_{0}^{\infty} (1 - F_{\text{смены}}(t)) G_{\text{преод.}}(t) dt ,$$

где k – номер преграды системы защиты,

n – количество преград системы защиты.

Возможных вариантов для функции распределения времени между соседними изменениями параметров системы защиты преграды $F_{смены}$ может быть несколько:

Вариант 1. Параметры системы защиты изменяются через постоянный интервал времени, т.е. $F_{смены}$ является детерминированной:

$$F_{смены} = \begin{cases} 0, t < f^{-1} \\ 1, t \geq f^{-1} \end{cases}.$$

Вариант 2. Интервалы времени между соседними изменениями параметров определяются случайным образом, например, с помощью генератора псевдослучайной последовательности:

$$F_{смены} = 1 - exp(-ft).$$

Возможные варианты для функции распределения времени для преодоления преграды системы защиты $G_{преод}(t)$:

Вариант 1. Время преодоления преграды системы защиты является постоянным:

$$G_{преод}(t) = \begin{cases} 0, t \leq g^{-1} \\ 1, t > g^{-1} \end{cases}.$$

Вариант 2. Рассмотрим случай, когда время преодоления злоумышленником преграды системы защиты неизвестно:

$$G_{преод}(t) = 1 - exp(-gt),$$

где g – масштабный коэффициент, с помощью которого мы можем учитывать как трудоемкость операций, так и уровень подготовленности и технической оснащенности злоумышленника.

Соответственно вероятность преодоления всей системы защиты будет определяться на основе следующих формул в зависимости от времени преодоления защиты информации:

- в случае, когда параметры системы защиты меняются через постоянные промежутки времени, а время преодоления системы защиты является постоянным:

$$P_{\text{прегр}} = \begin{cases} 0, f \geq g \\ 1 - f/g, f < g \end{cases};$$

- смена параметров системы осуществляется через равные промежутки времени, а время преодоления преграды неизвестно:

$$P_{\text{прегр}} = (1 - f/g)(1 - \exp(-g/f)),$$

- время между соседними изменениями параметров определяется случайным образом, а время преодоления преграды системы защиты является постоянным:

$$P_{\text{прегр}} = \exp(-f/g),$$

- время между соседними изменениями параметров определяется случайным образом, время преодоления преграды неизвестно:

$$P_{\text{прегр}} = g/(g + f).$$

Создание надежной системы информационной безопасности компании возможно, но только в случае активного соединения классических (программных и технических) и экономических методов защиты информации. Эффективное же задействование экономических механизмов, позволяющих сгладить убытки компании, связанные с

причинением ущерба АИС, возможно только в случае наличия СИБ, гарантирующей с большой вероятностью сохранность информации. Именно в создании наиболее эффективной относительно противодействия информационным рискам СИБ в условиях ограничений на выделяемые ресурсы, а также при определении вероятности причинения ущерба АИС основными информационными угрозами (задействование механизма страхования) существенную помощь может оказать приведенный выше комплекс моделей.