9 МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 34.03:004.056.5

МАТЕМАТИЧЕСКИЕ МОДЕЛИ ОЦЕНКИ ИНФРАСТРУКТУРЫ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Ю.А. Гатчин, И.О. Жаринов, А.Г. Коробейников

Рассматриваются математические основы проектирования инфраструктуры системы защиты информации на предприятиях. Приводятся математические модели минимизации затрат на построение инфраструктуры системы защиты информации и максимизации уровня защищенности информационных активов предприятия, а также результаты их практического использования.

Ключевые слова: защита информации, математические модели.

Введение

Современные промышленные предприятия осуществляют выпуск сложной продукции, интеллектуальной составляющей которой является новое научно-техническое знание (ноу-хау), подлежащее информационной защите. Помимо ноу-хау, защита на предприятиях должна осуществляться в отношении коммерческой, банковской, медицинской, государственной и других видов информации (бизнес-операций) в зависимости от сферы деятельности конкретного предприятия.

Модели, методы и средства защиты информации (ЗИ), используемые на предприятиях, различны и, как правило, выбираются в результате решения одной из задач вида $\langle S \to \min, R \ge R_{\text{доп}} \rangle$ или $\langle R \to \max, S \le S_{\text{доп}} \rangle$, где S – затраты на разработку, внедрение и сопровождение системы ЗИ на предприятии; R – уровень защиты, обеспечиваемый выбранным вариантом системы ЗИ; $S_{\text{доп}}$ – допустимая стоимость системы ЗИ на предприятии; $R_{\text{доп}}$ – допустимый уровень качества системы ЗИ в целом. Обе задачи математически эквивалентны и могут быть решены методами многокритериальной оптимизации. Традиционно в задачах многокритериальной оптимизации используется подход [1] на основе формирования множества Парето-оптимальных проектных решений по построению системы ЗИ, который, к сожалению, имеет ограниченное практическое применение, обусловленное значительной размерностью получаемого множества недоминирующих решений и неразрешенностью компромисса при допустимых значениях параметров $\{S, R\}$. Для решения задачи проектирования инфраструктуры системы ЗИ предлагается использовать метод последовательных уступок [2], в котором выделяется ряд частных показателей качества ЗИ, имеющих превосходство над остальными показателями, переводимыми в разряд ограничений.

Модель минимизации затрат на построение инфраструктуры ЗИ

Пусть $x_{ij} = 1$, если *i*-е средство ЗИ разработчик выбирает для защиты *j*-го информационного актива предприятия, и $x_{ij} = 0$ – в противном случае (при этом допускается, что *i*-е средство используется для защиты от *i*-ой угрозы). Требуется минимизировать затраты вида

$$S = \sum_{i \in I} \sum_{j \in J} S_{ij} x_{ij} + \sum_{i \in I} S_i y_i \to \min$$

при соблюдении следующих граничных условий:

$$\sum_{i \in I} \sum_{j \in J} a_j r_{ij} x_{ij} \ge R_{\text{äîï}},\ \sum_{i \in I} x_{ij} = 1, \forall j \in J,\ \sum_{j \in J} a_j = 1,\ x_{ij} \in \{0;1\},\ y_i \in \{0;1\},$$

где S_{ij} – затраты на защиту *j*-го информационного актива *i*-м средством; S_i – затраты, общие для всех информационных активов, на защиту *i*-м средством; I – множество средств ЗИ на предприятии; J – множество защищаемых информационных активов; r_{ij} – оценка качества защиты *i*-м средством *j*-го информационного актива (частный коэффициент защищенности, показывающий, какая часть атак угрозы *i*-го вида отражается); a_j – весовой коэффициент *j*-го информационного актива в общей оценке качества ЗИ; y_i – булева переменная, принимающая значение «1», если *i*-е средство ЗИ может быть использовано в системе защиты, и «0» в противном случае, причем *i*-е средство защиты в системе может быть использовано только один раз.

Модель максимизации уровня защищенности информационных активов предприятия

Модель максимизации уровня защищенности описывает двойственную задачу по отношению к модели минимизации затрат. В этом случае ограничение на уровень качества ЗИ становится критерием, а

критерий – ограничением:

$$R = \sum_{i \in I} \sum_{j \in J} a_j r_{ij} x_{ij} \to \max .$$

Таким образом, в данной модели требуется максимизировать уровень R качества ЗИ при соблюдении следующих граничных условий:

$$S = \sum_{i \in I} \sum_{j \in J} S_{ij} x_{ij} + \sum_{i \in I} S_i y_i \le S_{\text{доп}}, \ \sum_{i \in I} x_{ij} = 1, \forall j \in J, \ x_{ij} \in \{0;1\}, \ y_i \in \{0;1\} .$$

При построении оценки интегрального уровня R защищенности информации на предприятии принята единая схема расчета коэффициентов защищенности отдельных бизнес-процессов $R_{\text{б-п}}$ предприятия:

$$R_{\text{б-п}} = 1 - \frac{\sum_{b \in B} p_b \sum_{i \in N_b} \lambda_{ib} t_b (1 - r_i)}{\sum_{b \in B} p_b \sum_{i \in N_b} \lambda_{ib} t_b},$$

где N_b – количество наиболее вероятных информационных угроз для b-ой бизнес-операции на предприятии; r_i – коэффициент защищенности от i-ой угрозы; λ_{ib} – интенсивность потока атак i-го вида угроз на b-ую бизнес-операцию ($i \in N_b$), для $i \notin N_b$, $\lambda_{ib}=0$; t_b – время выполнения b-ой бизнес-операции; B – количество бизнес-операций в бизнес-процессе предприятия; p_b – вероятность выполнения бизнес-операции b в общем бизнес-процессе.

Сравнение вариантов построения структур систем ЗИ на предприятиях

Сравнение вариантов построения структур систем ЗИ на предприятиях основано на анализе многопараметрического критерия, зависящего от ряда частных показателей качества работы системы ЗИ.

Как следует из исходной задачи оптимизации $\langle S \to \min, R \ge R_{\text{доп}} \rangle$ или $\langle R \to \max, S \le S_{\text{доп}} \rangle$, основанием для вывода об абсолютном превосходстве одних показателей над другими служит степень различия отдельных показателей по важности, при которой сравнение оценок вариантов построения системы ЗИ осуществляется только по самому важному показателю без учета остальных, затем только по второму показателю и т.д. В общем виде задача оптимизации эквивалентна задаче нахождения условного экстремума основного критерия:

$$F_1 = \arg\limits_j \left\{ \min\limits_{j=1,2,...,N} \left\{ \xi_1^j \middle| \min\left\{\xi_i^j\right\} \le \xi_i^j \le \max\left\{\xi_i^j\right\}, i = 1,2,...,\zeta \right\} \right\},$$

$$F_2 = \arg\limits_j \left\{ \min\limits_{j=1,2,...,N} \left\{ \xi_2^j \middle| \min\left\{\xi_2^j\right\} \le \xi_2^j \le \max\left\{\xi_2^j\right\}, i = 1,2,...,\zeta \right\} \right\},$$

$$\vdots$$

$$F_\zeta = \arg\limits_j \left\{ \min\limits_{j=1,2,...,N} \left\{ \xi_\zeta^j \middle| \min\left\{\xi_i^j\right\} \le \xi_i^j \le \max\left\{\xi_i^j\right\}, i = 1,2,...,\zeta \right\} \right\},$$

где $\{\xi_1, \xi_2, ..., \xi_\zeta\}$ – частные показатели качества системы ЗИ; N – общее число вариантов проектных решений по выбору системы ЗИ.

Информация об абсолютном превосходстве определенных показателей позволяет проранжировать возможные варианты $F_1 \overset{lex}{>} F_2 \overset{lex}{>} ... \overset{lex}{>} F_\zeta$ с использованием процедуры лексикографической оценки. Реализация этой процедуры предусматривает декомпозицию исходной многомерной задачи оценки методом последовательных уступок в определенную последовательность задач (стратегию) оценки по иерархически упорядоченным скалярным показателям $\{\xi_1, \xi_2, ..., \xi_\zeta\}$.

Таким образом, предполагается, что первый показатель ξ_1 важнее второго ξ_2, второй ξ_2 – третьего ξ_3, и т.д. до ξ_ζ, так что $\boldsymbol{G}_F \supseteq F_1 \supseteq F_2 \supseteq .... \supseteq F_\zeta$, при условии $F_\zeta \ne \varnothing$, т.е. каждый последующий частный показатель сужает множество $\boldsymbol{G}_F$ проектных решений, получаемых с помощью всех предыдущих показателей. Это означает, что если в исходной задаче оптимизации с одним скалярным показателем имеется несколько решений и для дальнейшего выбора последовательно применяются дополнительные показатели, то получаемые в результате стратегии решения будут оптимальными для соответствующей лексикографической задачи с векторным показателем, состоящим из всех этих поочередно рассматриваемых показателей. Очевидно, для принятой модели минимизации затрат решающее правило по выбору конкретного варианта структуры системы ЗИ имеет вид

$$\hat{i} = \arg\limits_i \min \left\{ S_i \middle| R_i \ge R_{\text{доп}} \right\} .$$

Аналогично в модели максимизации уровня защищенности решающее правило по выбору конкретного варианта структуры системы ЗИ имеет вид

$$\hat{i} = \underset{i}{arg}\max\left\{R_i \middle| S_i \le S_{\text{доп}}\right\}.$$

Оценка значения величины $S_{\text{доп}}$ не вызывает затруднений и определяется финансовой состоятельностью предприятия и рисками (ущербом) от реализации атак на инфраструктуру ЗИ. Оценка значения уровня $R_{\text{доп}}$ может быть определена из шкалы предпочтений, представленной в табл. 1.

Значение показателя $R_{\text{доп}}$, усл. ед.	Характеристика состояния системы информационной безопасности предприятия
Менее 0,50 *Слабая защита*	Блокируется несущественная часть атак. Потери очень значительны. Фирма за короткий период (до года) теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы
0,51–0,75 *Средняя защита*	Неотраженные информационные атаки приводят к значительным потерям положения фирмы на рынке и в прибыли. Фирма теряет существенную часть клиентов
0,76–0,87 *Повышенная защита*	Блокируется значительная часть атак. Финансовые операции не ведутся в течение некоторого времени, за это время фирма терпит убытки, но ее положение на рынке и количество клиентов изменяются незначительно
0,88–0,95 *Сильная защита*	Ущерб от реализации информационных атак не затрагивает положение фирмы на рынке и не приводит к нарушению финансовых операций
0,96–0,98 *Очень сильная защита*	Раскрытие информации и реализация информационной атаки принесут ничтожный экономический ущерб фирме
0,99–0,99999… *Особая защита*	Отражаются практически все информационные атаки, ущерб фирме минимален или отсутствует

Таблица 1. Классификация значений комплексного показателя информационной защищенности

Экспериментальная проверка моделей построения инфраструктуры системы ЗИ

Для апробации на практике моделей построения инфраструктуры системы ЗИ была проведена серия экспериментов. Анализу подлежали различные варианты проектных решений по выбору системы ЗИ, представленные в табл. 2.

Вариант системы ЗИ	Состав системы ЗИ	Значение показателя *S*, усл. ед.	Значение показателя *R*, усл. ед.
1	Видеокамеры слежения	87	0,73
	Датчики разбития стекла		
	Охрана		
2	Firewall глобальной сети	121	0,71
	Электромагнитная защита		
	Смарт-карты разграничения доступа по помещениям		
	Охрана		

Таблица 2. Варианты систем ЗИ на предприятии

Как следует из табл. 2, построение системы ЗИ по варианту 1 оказывается удовлетворительным на основе модели минимизации затрат на построение инфраструктуры системы ЗИ при условии $0,51 \le R \le 0,75$ (средняя защита). Вариант 2 в этом случае оказывается также удовлетворительным по критерию $0,51 \le R \le 0,75$, однако является экономически более затратным. Не трудно видеть, что при использовании модели максимизации уровня защищенности предпочтительным является также вариант 1 построения системы ЗИ. Перспективно объединение составов обоих вариантов систем защиты информации.

Заключение

Предлагаемая методика и математические модели расчета показателей качества работы системы защиты информации на предприятии позволяют для произвольно выбранного числа компонентов и сложности структуры системы защиты информации осуществлять оценку эффективности ее использования для парирования информационных угроз.

Модели учитывают вероятностную природу угроз и систему бинарных правил специализации каждого средства защиты для соответствующего вида угрозы. Табулированная шкала предпочтений по уровню показателя защищенности предприятия позволяет оценивать приемлемое для конкретного предприятия качество защиты.

Проблема выбора при многопараметрическом критерии разрешена методом лексикографической оценки для основного критерия и системой ограничений для второстепенных. Варианты проектных решений по выбору системы защиты информации могут быть ранжированы в кортеж по предпочтениям от наиболее предпочтительного до наименее предпочтительного, но приемлемого.

Литература

1. Ногин В.Д. Проблема сужения множества Парето: подходы к решению // Искусственный интеллект и принятие решений. – 2008. – № 1. – С. 98–112.
2. Трояков И.Б. Методы оценки информационной безопасности предприятия на основе процессного подхода: дисс. канд. техн. наук … по спец. 05.13.19. – СПб: СПбГУ ИТМО, 2010. – 134 с.

Гатчин Юрий Арменакович – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, доктор технических наук, профессор, зав. кафедрой, gatchin@ifmo.ru

Жаринов Игорь Олегович – ФГУП «СПб ОКБ «Электоавтоматика» имени П. А. Ефимова», доктор технических наук, доцент, начальник отдела, igor_rabota@pisem.net

Коробейников Анатолий Григорьевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, доктор технических наук, профессор, korobeynikov_a_g@mail.ru

УДК 004.056

ПОИСК ВРЕДОНОСНЫХ ПРОГРАММ НА ОСНОВЕ АНАЛИЗА ПРОЦЕССА РАСПРОСТРАНЕНИЯ

И.А. Зикратов, Р.С. Василенко

Печатается в порядке дискуссии

Определены основные проблемы традиционных методов обнаружения вредоносного программного обеспечения, основанных на обновлении антивирусных баз. Рассмотрены альтернативные методы, основанные на облачных вычислениях. Предложен новый метод обнаружения на основе анализа процесса распространения неизвестного программного обеспечения.

Ключевые слова: вредоносные программы, процесс распространения, репутационные сервисы.

Введение

Из отчетов ведущих антивирусных компаний за 2010–2011 г.г. [1–4] следует, что, помимо увеличения общего количества вредоносных программ, постоянно увеличиваются темпы появления нового вредоносного программного обеспечения (ПО). Практически все существующие технологии антивирусных продуктов, так или иначе, используют антивирусные базы на стороне пользователя, отсюда возникает проблема своевременного выпуска обновлений пользователям. Деятельность антивирусных компаний по выпуску обновлений антивирусных баз можно условно разделить на следующие этапы [5]:

- поступление образца в антивирусную лабораторию;
- анализ образца (ручной или, что чаще, автоматический);
- создание обнаруживающей записи (эвристической или по бинарным маскам);
- тестирование записи;
- выпуск баз обновлений.

Алгоритмы, используемые антивирусными компаниями для решения данной задачи, являются закрытыми и, вероятно, разными для каждой компании, однако есть один общий факт – каждый этап занимает определенное время. В среднем с момента попадания образца в антивирусную лабораторию до выхода обновления проходит время t, которое обычно не меньше двух часов. С начала распространения вредоносной программы до момента ее обнаружения проходит от 5 до 98 часов [5, 6].

Обладая данной информацией, создатели вредоносных программ оптимизируют свои алгоритмы выпуска вредоносных программ таким образом, чтобы максимально понизить эффективность выпущенных обновлений. В худшем случае это приводит к тому, что выпущенная антивирусной компанией обнаруживающая запись оказывается бесполезной, так как вредоносный образец, который она обнаруживает, уже прекратил свое существование.