ЗАДАЧИ ПРОЕКТНОГО УПРАВЛЕНИЯ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Владимир Булдыжов

Национальный университет кораблестроения имени адмирала Макарова
54025, Украина, г. Николаев, проспект Героев Сталинграда, 9.
Тел.: (0512) 477095, E-mail: vib.nuk@gmail.com

Аннотация

Проблемами управления корпоративной информационной безопасностью (далее – ИБ) являются неполнота и нечеткость исходных данных, трудность обоснования затрат, сложность оценки состояния ИБ и, как следствие, оценки эффективности мер обеспечения ИБ как результата сравнения двух или нескольких состояний ИБ. Широко применяемые методики анализа рисков значительно повышают эффективность управления ИБ, представляя собой связующее звено между ИТ и руководством предприятия, а также позволяя управлять затратами на обеспечение ИБ. Однако такие методики существенно зависят от субъективности эксперта и не всегда обеспечивают повторяемость результатов. Ввиду того, что предметная область включает в себя психологические аспекты, в том числе угрозы ИБ со стороны человека, задача управления ИБ не является полностью формализуемой и всегда будет содержать элементы творчества и участия человека. Для оценки состояния ИБ предлагается использовать аппарат комплексных чисел, а также отрицательные значения риск-фактора при анализе рисков. Использование матрицы комплексных рисков и искусственного интеллекта при обработке статистики ущерба позволяют установить связь между мнимой частью комплексного риска и его влиянием на экономическую эффективность мероприятий по управлению ИБ.

1. Задачи управления корпоративной информационной безопасностью

Угрозы и нарушения информационной безопасности (далее – ИБ), такие как утечка информации, вредоносное ПО, ошибки и халатность персонала, ведут к значительному ущербу в современном бизнесе, включая материальный и нематериальный ущерб, простой бизнеса, утерю конкурентного преимущества и упущенную выгоду.

Характерная тенденция информационных систем современного бизнеса – взаимное проникновение. С увеличением использования мобильных информационных технологий (далее – ИТ) границы предприятия или организации становятся более размытыми, поэтому концепция защиты периметра с каждым годом утрачивает свою эффективность. Приобретающая популярность концепция «глубокой» или многослойной защиты (defence-in-depth) большей частью концентрируется на инфраструктурных компонентах и связях, в то время как основной ущерб от нарушений ИБ возникает из-за недостатков в бизнес-процессах, а также по мотивационным и другим психологическим причинам.

2. Методы и подходы обеспечения информационной безопасности

Традиционно проблемами управления ИБ являются неполнота и нечеткость исходных данных, трудность обоснования затрат, сложность оценки состояния ИБ, и, как следствие – оценки эффективности мер обеспечения ИБ как результата сравнения двух или нескольких состояний ИБ. Одним из наиболее наглядных способов обоснования затрат является метод расчета возврата инвестиций (ROI). Трудность применения данного метода состоит в оценке прибыли как функции от мер обеспечения ИБ. Предлагаемый способ оценки данной прибыли заключается в применении понятия предотвращенного ущерба, по обратной аналогии с тем, как в финансовом анализе убытком считается, кроме прочего, упущенная выгода.

С экономической точки зрения, управление корпоративными ИБ сводится к одной из двух оптимизационных задач соответственно принятому подходу:

а) наиболее эффективное распределение фиксированного бюджета ИБ,

б) компромиссный вариант, основанный на первом подходе и расчете бюджета ИБ, необходимого для достижения заданного уровня ИБ.

Смещение терминологических акцентов в ИТ отражает смену подхода к защите корпоративной информации. Современные стандарты ИТ и ИБ, такие как ISO 27000 [1, 2] и COBIT [3], концентрируют внимание не на обеспечении ИБ, а на управлении ИБ, неявно фиксируя принцип необходимости постоянной адаптации к новым угрозам, принцип недостижимости полной безопасности и необходимости оптимизации затрат на ИБ. Таким образом, управление ИБ предприятия или организации представляет собой деятельность с высоким уровнем неопределенности, с непрерывным появлением новых уникальных угроз и проблем, для которых необходим поиск новых контрмер (в терминах ISO 27000 – средств управления ИБ).

Широко применяемые методики анализа рисков значительно повышают эффективность управления ИБ, представляя собой связующее звено между ИТ и руководством предприятия, а также позволяя управлять затратами на обеспечение ИБ. Однако эти методики содержат высокую степень зависимости от

субъективности эксперта и не всегда обеспечивают повторяемости результатов. Тем не менее, ввиду того, что предметная область включает в себя психологические аспекты, о которых упомянуто выше, задача управления ИБ не является полностью формализуемой, и всегда будет содержать элементы творчества и участия человека. Поэтому ставится задача не полной формализации оценки уровня ИБ и анализа рисков, а приближения методов такой оценки и анализа к способам человеческого мышления и восприятия. При этом преследуется основная цель – обеспечение принятия правильных решений при управлении ИБ.

Перечисленные особенности управления ИБ, уникальность задач такого управления, длительный период реализации мероприятий, большое количество необходимых ресурсов, неопределенность и нечеткость исходных данных обуславливают исключительную эффективность применения теории проектного менеджмента при управлении корпоративной ИБ. Решение описанных выше оптимизационных задач служит исходными данными при планировании проекта, в частности, его целей, качества, области охвата, сроков и бюджета.

3. Переход от использования действительных положительных значений риск-фактора при анализе рисков к комплексным значениям

Известный криптолог, ученый и борец за гражданские права Брюс Шнайер в своей работе «Психология безопасности» [4] предлагает различать действительную и ощущаемую безопасность. Приводятся примеры принятия неправильных решений из-за недооценки или переоценки рисков, классификация причин расхождения действительной и ощущаемой безопасности. Однако в этой же работе Шнайер делает вывод, что ощущаемая безопасность не является вредным фактором, и, в некоторой мере, нужна для сближения действительной и ощущаемой безопасности. Затраты на создание и внедрение паллиативных средств безопасности позволяют правильно управлять остаточной субъективной долей, которая неизбежно присутствует при принятии решений.

Ключевым понятием при оценке эффективности мероприятий, результативности проекта, целесообразности бюджета является понятие состояния ИБ. В данном случае под состоянием ИБ подразумевается совокупность состояний по каждой из обрабатываемых угроз ИБ, а также взаимосвязь данных состояний.

Для оценки состояния ИБ автор предлагает использовать аппарат комплексных чисел. Состоянием ИБ по конкретной угрозе является комплексное число

$$S = R + Fi, \quad (1)$$

где R – действительное состояние ИБ, рассчитываемое на основе одной из методик анализа рисков; F – мнимое состояние ИБ, характеризующее ощущение эксперта о состоянии ИБ по данной угрозе.

Также автор предлагает использовать отрицательные значения риск-фактора при анализе рисков. За нулевую точку риск-фактора принимается риск, соответствующий допустимому уровню риска в терминах ISO 27000. Согласно общепринятому подходу к управлению рисками, риски ниже допустимого при управлении ИБ осознанно принимаются, риски выше – обрабатываются. Взаимосвязь состояний ИБ описывается системой коэффициентов. Представление риск-фактора в виде комплексного числа в четырех квадрантах позволяет приблизить понятие риска к способу восприятия и обработки его человеком, в том числе проводить графический анализ.

Связь угроз и средств управления рисками описывается в матрице рисков ИБ. Данная матрица учитывает уровень воздействия каждого средства управления на каждый риск, включая его действительную и мнимую части. С использованием искусственного интеллекта и анализа статистики ущерба устанавливается взаимосвязь между средствами управления ИБ и их эффективностью при снижении рисков. При накоплении базы знаний устанавливается оптимальная конфигурация средств управления ИБ с использованием критерия оптимизации по затратам во времени и приближения комплексного риск-фактора к заданному уровню.

Таким образом, использование матрицы комплексных рисков и искусственного интеллекта при обработке статистики ущерба позволяет установить связь между мнимой частью комплексного риска и его влиянием на экономическую эффективность мероприятий по управлению ИБ.

Литература:

[1] ISO/IEC 27001:2005 "Information technology — Security techniques — Information security management systems — Requirements". International Organization for Standardization, 2005.
[2] ISO/IEC 27002:2007 "Information technology — Security techniques — Code of practice for information security management". International Organization for Standardization, www.iso.org, 2007.
[3] Control Objectives for Information and related Technology, version 4.1, 2007. IT Governance Institute, www.itgi.org, ISBN 1-933284-72-2.
[4] Брюс Шнайер, «Психология безопасности», http://www.securitylab.ru/analytics/350799.php