- Aprecierea şi rezultatele riscului sunt în esență subiective atât în ceea ce priveşte procesul, cât şi metrica. Datele metrice independent obiective nu sunt utilizate.
- Percepția asupra valorii bunurilor țintă nu este dezvoltată pe o bază monetară obiectivă, ceea ce ar putea să nu reflecte valoarea efectivă supusă riscului.
- Nu este posibilă urmărirea performanței managementului riscului în mod obiectiv, din moment ce toate măsurile sunt subiective.

Cu toate acestea, nu este posibilă desfăşurarea unei aprecieri pur calitative a riscului. În realitate, cele două abordări au un caracter complementar, şi de aceea sunt recomandate de a fi, întotdeauna, puse în aplicare în combinație.

Bibliografie

1. Hrvoje Segudovic, *Qualitative risk analysis methodcomparison // http://www.infigo.hr/files/INFIGO-MD-2006-06-01-RiskAsses_ENG.pdf*
2. Ion I. Bucur, *Evaluarea și managementul riscurilor de securitate //* http://www.xanderzone.ro/cursurimaster/C-II-4.pdf.
3. Александр Астахов, *Искусство управления информационными рисками*, ДМК Пресс, Москва, 2010.

ТЕНДЕНЦИИ РАСПРОСТРАНЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дорошев Дмитрий, Корнеенко Ольга
УО «Гомельский государственный университет имени Франциска Скорины» (Гомель, Белоруссия)

In article attempt to carry out the analysis of threats of information security popular now is given. On the basis of reports of the leading companies in the field of information technology tendencies of distribution of the basic categories of threats are described.

В последние годы перед руководителями большинства компаний остро встал вопрос о сокращении издержек, в том числе и в сфере информационных технологий, где затраты некоторое время росли рекордными темпами. В конце 2008 года многие компании предпочли занять выжидательную позицию, сократив до минимума затраты на ИТ. Однако подобная стратегия не может быть долгосрочной, в связи с тем, что большинство компаний имеют серьезные ИТ-инфраструктуры, которые прочно интегрированы в бизнес, и для многих отказ от ИТ практически означает отказ от бизнеса.

Все ИТ-затраты условно можно разделить на три вида: затраты, ориентированные на поддержку, на обновления, на инновации. Очевидно, что без замены

вышедшего из строя оборудования, не обойтись, от расходных материалов тоже невозможно отказаться. Однако, многие проекты из категории «обновления», такие как переход на новые персональные компьютеры, обновление версий программ, могут быть отложены. При этом, как полагают аналитики, расходы на ИТ-безопасность потребуют дополнительных инвестиций.

Понять необходимость инвестиций в информационную безопасность в период урезания бюджетов подчас достаточно сложно. Отдача от таких инвестиций выражается не в том, что случилось и принесло прибыль, а в том, чего не случилось и что, предотвратило убыток.

Существуют количественные методики оценки возврата инвестиций от внедрения систем безопасности (ROI) [1]. Одну из них можно выразить формулой:

$$ROI = (C_1*N_1 + C_2*N_2 + C_3*N_3 + ... + C_n*N_n)/TIC,$$

где C_1 и C_2...C_n – средняя стоимость инцидента информационной безопасности;
N_1 и N_2...N_n – количество инцидентов информационной безопасности в год;
TIC – стоимость покупки и внедрения решения информационной безопасности.

Данную методику используют как для стоимостного, так и для качественного анализа угроз информационной безопасности. Для качественного анализа можно выбрать наиболее важные категории угроз (вирусные атаки, хакерские атаки, DDoS-атаки, интернет-мошенничество, инциденты информационной безопасности (IM-агенты), инциденты информационной безопасности по вине «мобильных» сотрудников, потери по причине несоблюдения требований, потери от деятельности инсайдеров, утечки данных) и изучить, какие из видов угроз имеют тенденцию к уменьшению, а какие – к увеличению.

Вирусы. В последнее время не наблюдается снижение темпов роста вредоносного программного обеспечения. Ежедневно появляются десятки тысяч новых и модификаций уже существующих вирусов. С 2000 года соблюдается экспоненциальный характер роста количества вирусных программ. Данный бизнес приобретает элементы групповой работы, присущие процессу написания сложного коммерческого программного обеспечения. Растет количество троянских программ, направленных на кражу информации о банковских аккаунтах. Киберпреступники продолжают проявлять повышенный интерес в поиске новых уязвимостей в популярном программном обеспечении, в первую очередь в MS Office и MS Windows, тем более что в странах СНГ остро стоит вопрос о лицензионном использовании данных программных продуктов.

Не следует забывать про рост атак на мобильные телефоны при параллельной их коммерциализации. Этот процесс становится следствием усиления конкуренции киберпреступников на технологическом уровне и их активной борьбы за увеличение числа зараженных компьютеров. По мере того как все больше устройств подключается к Интернету, количество угроз, связанных с проникновением в них вирусов, также растет.

Рост киберпреступности. Хакерские атаки, DDoS-атаки, интернет-мошенничество напрямую связаны с ростом киберпреступности. Особенно это заметно в период кризиса. Из-за нехватки легальных рабочих мест, актуальным становится нелегальный заработок, при этом происходит всё большая дифференциация киберпреступников, а каждая деятельность в зависимости от трудоемкости и опасности приобретает свою рыночную цену. По мере развития систем интернет-банкинга развитие получают фишинг, целью которого является получение доступа к конфиденциальным данным пользователей, и фарминг – автоматическое перенаправление пользователя на фальшивый веб-сайт. Подпольная киберэкономика становится международной. На черном киберрынке лучше всего продается информация о кредитных картах для доступа к банковским счетам и персональные данные граждан.

IM-агенты и социальные сети. Некоторое время назад в Интернет-пространстве широко обсуждалась тема жесткого контроля доступа в Интернет на работе. Однако концепция Web 2.0 свидетельствует, что общение с лучшими представителями сетевого сообщества – это огромный потенциал для компании. Запрещаемые одно время во многих компаниях программы Skype и различные мессенджеры уже активно используются в силу своей экономичности. А в социальных сетях «сидит» подавляющее большинство сотрудников как в рабочее так и в нерабочее время. Социальная активность сотрудников растет, и проконтролировать, где целевой, а где нецелевой web-доступ, очень сложно. Чем больше социальной активности – тем выше риск утечки информации. Кроме того, социальные сети становятся основной мишенью атак, так как содержат персональную информацию, которая может быть использована злоумышленниками.

«Мобильные» сотрудники. Известно, что с увеличением количества «мобильных» сотрудников вероятность инцидентов ИБ возрастает. Может расти количество командировок, в которые сотрудники едут с офисным ноутбуком. Офисные сотрудники могут переходить на режим работы из дома. Так что нередки случаи, когда офисный ноутбук становится домашним, а доступ к нему получает вся семья.

Соответствие требованиям и стандартам ИБ. В последние годы все больше отечественных компаний выходит на международный рынок, работает в тесной интеграции с западными партнерами, и их ИТ-инфраструктура все в большей степени подпадает под требования международных стандартов по ИТ-безопасности. Очевидно, что отсутствие у отечественных компаний систем безопасности международного уровня тормозит перспективы их сотрудничества с западными предприятиями. Необходим анализ существующих мер защиты и приведение их в соответствие с требованиями стандартов.

Инсайдеры. С точки зрения мотивов различают халатных, манипулируемых, обиженных, внедренных инсайдеров и т.д. Очевидно, что для перехода сотрудника из категории «лояльный» в категорию «инсайдер» более чем достаточно: увольнение, отпуск без содержания, отмена бонусов. Согласно опросам, в западных странах до 45% служащих готовы передать конкурентам корпоративную информацию в случае увольнения.

Все вышесказанное свидетельствует повышении риска инцидентов информационной безопасности. Следовательно, возможные потери от них будут расти быстрее, нежели стоимость внедрения решения информационной безопасности [2]. Можно утверждать, что важнейшим активом любой современной компании является информация. Как и всякий критически важный актив, информация нуждается в защите, а в случае ее утечки компания несет довольно серьезные убытки.

Литература

1. http://www.trainings.ru/library/dictionary/roi/
2. http://www.securelist.com/ru/analysis

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНВЕСТИЦИОННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Ремезова Екатерина Максимовна,
Владимирский государственный университет
им. А.Г. и Н.Г. Столетовых, Россия
Дорохов Михаил Александрович,
Харьковский национальный экономический университет,
Харьков, Украина

The purpose of this article is research of a problem of the accounting of uncertainty in case of support of information security of acceptance of the investment decision. Based on results of the detailed comparative analysis of existing methods, possible ways of overcoming of their shortcomings by means of use of the device of the theory of fuzzy sets and in particular type-2 fuzzy sets are considered.

Важным условием стабильного функционирования и развития любого крупного предприятия является эффективная инвестиционная политика, которая ведет к увеличению объемов производства, росту доходов, а, следовательно, наращиванию экономического потенциала. Обширная практика проведения реальных прогнозных расчетов инвестиционного проекта свидетельствует о необходимости всестороннего учета различных видов неопределенности при оценке, планировании и управлении инвестиционными проектами.

Действительность такова, что влияние факторов неопределенности на рассматриваемые проекты приводит к нарушению информационной безопасности инвестиционной деятельности предприятия, которое приводит к неожиданным потерям, убыткам, даже в тех проектах, которые первоначально признаны экономически целесообразными для предприятия. Под информационной