УДК 004.056

А. В. Скиба,
аспирант, НТУУ "КПІ"
О. Є. Архипов,
д. т. н., профессор кафедры информационной безопасности, НТУУ "КПИ"

ИНФОРМАЦИОННЫЕ РИСКИ: МОДЕЛИ РИСКОВ, ИССЛЕДОВАНИЕ И ИСПОЛЬЗОВАНИЕ

A. Skyba,
PhD student NTUU "KPI"
O. Arkhypov,
Dr. Sci. Tech., NTUU "KPI"

INFORMATION RISKS: THE RISK MODEL, RESEARCH AND USE

Рассматривается проблема оптимизации инвестиций в сферу защиты информации. В частности, анализируются подходы и решения, опирающиеся на существующие международные стандарты менеджмента рисков информационной безопасности, отмечается, что эти стандарты носят преимущественно концептуально — рекомендательный характер и не учитывают многих факторов, которые существенно влияют на точность и объективность оценок рисков и, как следствие, адекватность оценивания уровня инвестиций. В качестве альтернативы анализируются оптимизационные оценки объема инвестиций, основанные на исследовании экономических моделей. В первую очередь это модель Гордона — Лоеба, для которой, к сожалению, характерен формально-аксиоматический поход к описанию рисковой ситуации и практически исключается возможность конкретизации индивидуальных свойств объекта риска и реального профиля угроз. Кроме того, исследуются процедуры оптимизации инвестиций, использующие экономико — стоимостные эвристические модели, предназначнные для идентификации вероятностных параметров и структуры информационных рисков. В частности, введен ряд моделей, в основу которых положены допускающие простую и прозрачную интерпретацию мотивационно-стоимостных механизмов действий атакующей и защищающейся стороны. По результатам выполненных исследований получены оценки оптимального объема инвестиций в безопасность информации, учитывающие особенности структуры и параметров рисков в реальной организации.

The problem of optimizing the investment in information security is disclosed in the article and analysis of the approaches and solutions, based on existing international standards for information security risk management is proposed, it is noted that these standards are mostly conceptual — advisory in nature and doesn't take into account many factors that significantly affect the accuracy and objectivity of the risk assessment and, as a consequence, on the adequacy of estimating of the level of investment. Alternatively, optimization analyzes estimate the amount of investment based on economic models. The first is the model of Gordon — Loeb, which, unfortunately, is characterized by formal axiomatic trek to the description of the risk situation and virtually eliminates the possibility of specifying the individual properties of the object and the real risk profile of the threats. In addition, we study the optimization procedure investment using economic — cost heuristic model whic is used to identify the probabilistic parameters and structure of information risks. In particular, it introduced a number of models, which are based simple and clear interpretation of motivational-cost mechanisms of action of the attacking and defending side. The results of the research obtained estimates of the optimal investment in information security, especially taking into account the structure and risk parameters in a real organization.

Ключевые слова: информационная безопасность, стандарты менеджмента рисков информационной безопасности, методы оценки рисков, исследования инвестиций в информационную безопасность, психотипы злоумышленников.

Key words: information security, standards of information security risk management, risk assessment techniques, research investment in information security, psycho intruders.

ВВЕДЕНИЕ

Высокие темпы развития сферы информационных технологий обусловливают необходимость проявления пристального внимание к вопросам обеспечения информационной безопасности, соответствия ее состояния быстрым изменениям в технологиях, уменьшению вероятностей реализации рисков, связанных с информационными угрозами. Наибольшее внимание при формировании систем информаци-

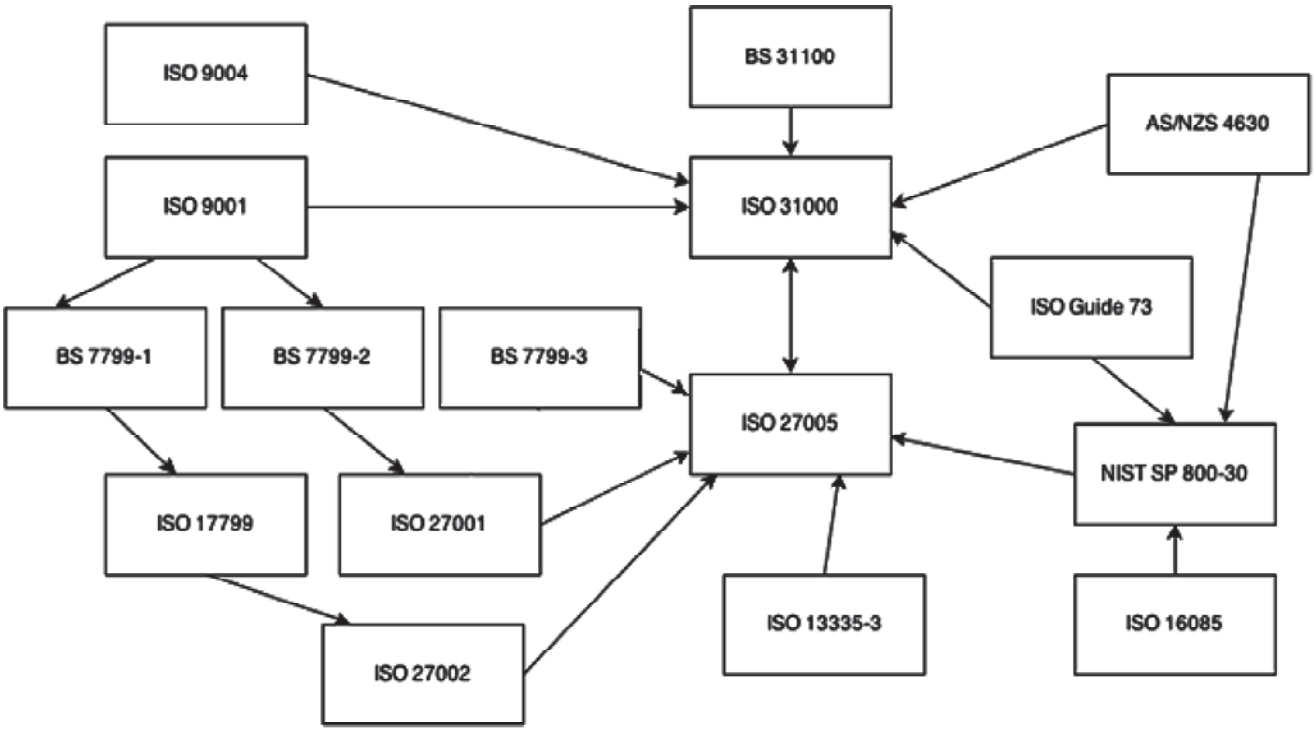

Рис. 1. Эволюция стандартов менеджмента рисками безопасности информации

онной безопасности в отечественных компаниях, предприятиях, учреждениях уделяют, как правило, выполнению требований нормативно-методической базы в сфере защиты информации, определяя эти требования как первооснову становления системы информационной безопасности, что, однако, само по себе еще не создает гарантий достаточного уровня защиты. Суть проблемы заключается в том, что при проектировании и построении системы защиты информации основное внимание должно быть уделено не минимизации воздействий по определенному перечню типовых угроз, составленного в соответствии с некоторой воображаемой средой функционирования организации, а выявлению и минимизации информационных рисков, связанных с практической деятельностью конкретной организации. Само формирование реального профиля рисков, связанных с процессами деятельности организации, уменьшение этих рисков или их нейтрализация при сохранении постоянного контроля рисковой ситуации составляет суть ведущих современных концепций создания систем защиты информации. К сожалению, сама сущность методологии рисков обусловливает определенные трудности в своем практическом применении, так как требует вычисления высокоточных оценок информационных рисков, предполагая определенную индивидуализацию, исключительность получаемых в рамках этого подхода решений.

Для того, чтобы получить более-менее четкое представление о ситуации, связанной с возможностями практического применения методологии рисков в области информационной безопасности, рассмотрим многочисленные рекомендации и примеры применения этой методологии, описанные в международных стандартах, национальных нормативных документах и установках по информационной безопасности.

ЭВОЛЮЦИЯ РАЗВИТИЯ СТАНДАРТОВ В СФЕРЕ ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ

Проблема оценивания и исследования информационных рисков обычно ассоциируется с британским стандартом BS 7799, прежде всего с его двумя частями: BS 7799-1. Правила менеджмента безопасности информации, BS 7799-2. Системы менеджмента безопасности информации, в которых впервые вопросы анализа состояния безопасности информации и формирования ее защиты были напрямую связаны с информационными рисками. Непосредственно аспекты оценки и управления рисками, гармонизированые с содержанием двух первых частей, было подробно рассмотрено в третьей части стандарта BS 7799-3. Руководство по менеджменту рисками безопасности информации [1]. Однако первым международным стандартом менеджмента рисками стал стандарт ISO/IEC TR 13335-3. Руководство по менеджменту безопасности информационных технологий (1998 г.). Через десять лет, в 2008 г. был издан стандарт ISO/IEC 27005. Менеджмент рисками безопасности информации [2], который сейчас стал одним из ведущих нормативных документов в сфере управления информационными рисками.

Практически все современные стандарты в области безопасности отражают общий подход к организации управления рисками, сложившийся в международной практике. При этом управление рисками представляться как базовая часть системы менеджмента качества организации. Стандарты носят откровенно концептуальный характер, что позволяет экспертам по информационной безопасности реализовывать любые методы, средства и технологии оценки, обработки и управления рисками.

Считается, что международные стандарты, формируемые на основе анализа и обобщения лучших методов, апробированных на практике как большими группами профессионалов, так и ведущими профильными организациями, в большинстве случаев определяют лучшие варианты действий при возникновении инцидентов информационной безопасности. Использование стандартов увеличивает ценность создаваемой информационной системы или технологии, но к сожалению нет таких стандартов, которые бы охватили все аспекты управления, безопасности и качества.

Эволюцию развития стандартов в области менеджмента рисками безопасности информации можно попытаться представить схемой, изображенной на рисунке 1.

Очевидно, что смысл эволюции — появление нового усовершенствованного стандарта, более высокий качественный уровень котрого базируется на "восприятии опыта" от стандартов-предшественников и обобщени, учете опыта применения стандартов в смежных отраслях. В частности, на данном этапе эволюции стандартов информационной безопасности происходит позитивный процесс замещения старой серии стандартов в области управления информационной безопасности ISO/IEC TR 13335 новой серией стандартов — ISO/IEC 27000. Новый стандарт ISO/IEC 27005 заменил сразу два морально устаревших стандарта ISO/IEC TR 13335-3 [3] и ISO/IEC TR 13335-4 [4], которые, однако, остались в числе базовых документов для нового стандарта. Кроме того, стандарт ISO/IEC 27005 также опирается на нормативно-методические документы, приведенные в его библиографическом перечне: ISO / IEC 16085 [5], BS 31100 [6], AS/NZS 4360 [7] и NIST SP 800-30 [8].

Существенное влияние на содержание нового стандарта проявила и разработка стандарта ISO/IEC 31000. Риск-менеджмент. Принципы и рекомендации, которая длилась практически одновременно с разработкой ISO/IEC 27005. Стандарт ISO/IEC 31000 обобщил в себе лучшие тенденции мировой практики по управлении рисками. В библиографическом списке этого стандарта такие стандарты, как: ISO/IEC 9001 — общие требования к системам менеджмента качества, ISO/IEC 9004 — рекомендации для устойчивого достижения целей в системах управления качеством, BS 31100 — набор практических и конкретных рекомендаций для менеджера информационной безопасности, ISO/IEC Guide 73 — набор терминов в сфере управления рисками, уже упомянутый выше AS/NZS 4360 — общие требования к условиям управления рисками. Вся нормативная документация, на которой базируется стандарт ISO/IEC 31000, относится к области управления и контроля качеством и применима к различным сферам деятельности, включая и сферу информационной безопасности .

Обобщение лучшего межотраслевого опыта является еще одним преимуществом стандарта ISO/IEC 27005, для которого ситуация выглядит следующей: с одной стороны, сильная теоретическая база, опирающаяся на обобщенный опыт практического управления системами защиты информации, а с другой — лучшее из опыта управления и контроля качества, проверенное во многих сферах применения.

Следует отметить, что вопреки распространенным ожиданиям, новый стандарт ISO/IEC 27005 вовсе не является международной версией BS 7799-3. Более того, в нем даже не встречается упоминания о последнем стандарте. Структура и содержание этих стандартов существенно различаются, причем существенно различаются и первичные источники на которых, базировалась разработка стандарта. Неизменным остается лишь общий понятийный аппарат, общий подход к процессу управления рисками .

В общем можно сделать вывод о том, что для стандарта ISO/IEC 27005, в отличие от предыдущих стандартов серии ISO/IEC 27000, в разработке которых использовались преимущественно наработки Британского института стандартов (BSI) и других британских организаций, в полной мере учтен существующий международный опыт.

Методики и рекомендации приведенных выше стандартов базируются на двух основных подходах к представлению оценок информационных рисков [9;10]: качественному и количественному.

Задачей качественной оценки является определение возможных видов рисков, оценка принципиального уровня серьезности угроз, а также выделение факторов, влияющих на уровень обоснования различных возможных контрмер. Эти методики не оказывают количественные или денежные значения компонентам и потерям. Они достаточно популярны, относительно простые и разработаны, как правило, на основе требований международного стандарта ISO/IEC 17799:2005 [11].

Количественные методики предоставляют реальные и осмысленные численные значения всем элементам процесса анализа рисков. Этими элементами могут быть стоимость защитных мер, ценность актива, ущерб для бизнеса, частота возникновения угрозы, эффективность защитных мероприятий, вероятность использования уязвимости и так далее. Количественный анализ позволяет получить конкретное значение вероятности (в долях единицы либо в процентах) реализации угрозы. Каждый элемент в процессе анализа вводится в количественном виде в уравнение для определения общего и остаточного риска.

Также довольно часто используется комбинация этих двух подходов, как правило, на начальных этапах анализа информационных рисков используется качественный, а на конечном — именно получение оценки — количественный.

Учитывая, что оценка рисков на качественном уровне не позволяет однозначно сравнить затраты на обеспечение информационной безопасности и полученной от них отдачи (в виде снижения суммарного риска), сосредоточимся на более точном количественном подходе. Отметим, что в этом случае процедура построения систем защиты информации (СЗИ) на базе методологии информационных рисков по применению установок основных стандартов характеризуется рядом "узких" мест.

Во-первых, это необходимость параметризации рисков. Общее математическое соотношение, исходя из которого исчисляется риск, обусловленный возможной реализацией угрозы *T*, имеет вид:

$$R_T = P_T q = P_t P_v q \quad (1),$$

где R_T — вероятность реализации угрозы T, q — убытки, возникающие в условиях реализации угрозы T, P_t — вероятность возникновения (активации) угрозы T, P_v — вероятность удачного использования атакующей стороной (злоумышленником) уязвимостей информационной системы, что приводит к реализации угрозы T. То есть вычисления риска требует знания двух (P_T, q) или трех (P_t, P_v, q) параметров риска R_T, часто определяемых экспертным путем [10; 12; 13], что может весьма существенно ухудшить качество оценок рисков и непредсказуемо повлиять на конечные результаты менеджмента рисков.

Во-вторых, наличие нескольких угроз (уязвимостей) характеризуется соответствующими частичными рисками, совокупное влияние которых описывается определенным интегральным риском, оценивание которого в общем случае может быть достаточно сложным [2].

В-третьих, методики управления рисками, разработанные по рекомендациям стандартов, чаще всего опираются на переборный подход: рассматривается несколько возможных вариантов построения СЗИ, в которых уровни рисков (интегрального риска) уменьшаются до приемлемых значений, и дальше по решению эксперта определяется рабочий вариант СЗИ (чаще всего он выбирается как наименее дорогостоящий). Кроме того, ориентация новых стандартов серии ISO 27000 на итеративную процедуру управления рисками по Шухарту — Демингу по своей сути изначально ориентирована на применение

переборного подхода в построении СЗИ, сужая возможности использования аналитических оптимизационных методов.

При этом вопросы качества рабочего варианта СЗИ (оптимальности принятого решения о выборе этого варианта СЗИ), эффективности инноваций в организацию СЗИ практически не исследуются. Замена эксперта любым инструментально-программным средством (ИПС) принципиально ситуации не меняет, так как прототипом при разработке этих ИПС чаще всего выступает именно эксперт, в связи с чем практически все наиболее распространенные ИПС — это интеллектуализированные информационные системы (системы поддержки принятия решений, экспертные системы и т.п.), в которых реализованы те или иные методы отображения и обработки знаний экспертами.

Определенной альтернативой управления рисками на базе методик, представленных в стандартах, является применение в менеджменте рисков математических моделей, связывающих уровень рисков (убытков), обусловленных реализацией информационных угроз, с объемом инвестирований в СЗИ [14—17]. Применение этих моделей для анализа и исследования рисков имеет целью среди прочего обеспечить возможность оценки эффективности инвестирований в СЗИ и прогнозирования характеристик рисков в зависимости от уровня инвестиций в систему защиты.

МОДЕЛЬНЫЕ ИССЛЕДОВАНИЯ ИНВЕСТИРОВАНИЙ В СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

На сегодня одной из наиболее распространенных и известных моделей, применяемых для анализа эффективности инвестирований в СЗИ, является модель, разработанная двумя американскими исследователями в области экономики Лоуренсом Гордоном и Мартином Лоебом из университета Мериленд, описання ими в 2002 году в статье [16]. Модель предназначена для определения экономически обоснованного инвестирования в информационную безопасность. Именно этим объясняется пристальное внимание и широкий резонанс, вызванный публикацией в научных и профессиональных кругах: многочисленные отзывы и комментарии как положительного, так и критического характера, замечания, предложения, дополнения [17—20].

Предложенный в статье Гордоном и Лоебом подход основывается на использовании некоторой функция вероятности нарушения защищенности информационных ресурсов (ФВЗИР), задание которой осуществляется в соответствии с системой из трех аксиом, формирующих определенную совокупность требований к свойствам ФВЗИР. Авторы предлагают два класса зависимостей, которые удовлетворяют указанным требованиям, причем выполненное ими дальнейшее исследование ФВЗИР для каждого из классов приводит к одинаковому выводу: оптимальный объем инвестиций в систему защиты информации (СЗИ) не может превышать 36,79% от величины максимальных потерь, которые могут возникнуть в случае реализации угроз информации. Здесь следует отметить, что в работе Гордона и Лоеба отсутствует доказательства полноты и достаточности введенной системы аксиом, не исключена возможность ее дополнения, развития и, как следствие, модификации полученного заключения о величины максимальных потерь. Поэтому вполне естественным стало появление в 2006 году статьи [4], где два класса функций (зависимостей), предложенных Гордоном и Лоебом, были дополнены еще четырьмя, двух статей Дж. Виллемсона (J.Willemson) [17,19], в которых несколько изменена и расширена исходная система аксиом Гордона-Лоеба, других модификаций положений подхода Гордона-Лоеба. При этом изменялась и величина оптимального объема инвестиций в СЗИ: в статье [18] она достигает 100% от величины максимально возможных потерь, а в новой статье Гордона и Лоеба [21], где они выступают в соавторстве с двумя другими исследователями (William Lucyshyn, Lei Zhou), предполагается, что оптимальный объем инвестиций может и превышать 100% от величины максимально возможных потерь. Не вдаваясь в детальный анализ положительных и отрицательных свойств подхода Гордона-Лоеба, отметим один его недостаток — формально-аппроксимативных способ задания ФВЗИР, в котором не рассматривается возможность учета при формировании структуры и параметров этой функции сведений о реальных механизмах развития и реализации информационных угроз и рисков. Это приводит к существенному ограничению практических аспектов применения указанного подхода и объективности полученных выводов, в том числе и главного постулата авторов о величине оптимального объема инвестиций в защиту информации. Последнее исследование в 2015 году, модификация оригинальной формулы Гордона и Лоэба позволила учесть упущенный фактор стоимости информации, но в целом ситуация не поменялась [21].

В этой ситуации интерес представляют модели, предложенные для исследования экономико-мотивационных отношений, характерных для ситуации "атака-защита" в информационной сфере [22; 23]. Для определения вероятностных параметров риска в этих моделях используются мотивационно-стоимостные и экономико-финансовые аппроксимативные соотношения, допускающие достаточно простую интерпретацию механизмов возникновения информационных угроз и соответствующих рисков. Рассмотрим ситуацию, возникающую при реализации атакующей стороной А (злоумышленник) угрозы T относительно некоторого информационного ресурса I, принадлежащего стороне В. Полагаем, что D-общая стоимость затрат атакующей стороны А на реализацию угрозы T, g-полученный при этом "выигрыш", величина которого обусловливается ценностью ресурса I для злоумышленника. Убытки, понесенные в этой ситуации стороной В (владелец ресурса I), то есть стоимость критической информации с точки зрения ее владельца, оценивается им как q, а общая стоимость реализованного в ИС комплекса защитных мероприятий равна c.

Приведенные данные дают стоимостные характеристики ситуации "атака-защита". На базе этих сведений можно построить логико-эвристическую схему экспертного оценивания вероятностных характеристик, используемых для вычисления информационных рисков.

ПРИМЕНЕНИЕ ЭКОНОМИКО-СТОИМОСТНЫХ МОДЕЛЕЙ ДЛЯ ОЦЕНКИ РИСКОВ И ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ИНВЕСТИЦИЙ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Чистая прибыль злоумышленника в случае успешной реализации им угрозы T составляет:

$$Q = g - D \qquad (2).$$

Если ценность ресурса I для атакующей стороны А значительная, интенсивность потока попыток доступа злоумышленника к ресурсу I будет очень высокой. В частности, если $g >> D$, можно предположить, что вероятность активации (возникновения) угрозы T будет практически равна 1, то есть злоумышленник попытается использовать любые шансы для реализации этой угрозы. Напротив, для малых значений g экономические мотивы возникновения угрозы T практически отсутствуют: при $Q = 0$ (или $g = D$) атака ресурса I становится нецелесообразной, в этом случае. Для $g < D$ попытка реализации угрозы T теряет экономический смысл. Исходя из этих соображений, в [22; 23] для оценки значений вероятности активации (возник-

новения) угрозы T предложено соотношение:

$$P_t = \frac{Q}{g} = 1 - \frac{D}{g} \quad (3).$$

Однако в выражении (2) никак не учитывается уровень индивидуальных мотивационных характеристик злоумышленника. Поэтому более гибким является вариант оценки вероятности P_t по формуле [24]:

$$P_t = \frac{\gamma g - D}{\gamma g} = 1 - \frac{D}{\gamma g} \quad (4),$$

где введено коэффициент мотивации γ, отражающий степень влияния величины "выигрыша" g на действия стороны А активации угрозы T.

В зависимости от индивидуальных свойств злоумышленника коэффициент мотивации γ может быть как больше 1 (атакующей стороне А свойственный азарт, авантюризм, уверенность в своем успехе), так и меньше 1 (злоумышленник осторожен, не горячится, считая, "что лучше иметь синицу в руке, чем журавля в небе"). Так как значение вероятности P_t ограничивается диапазоном [0,1], на область существования значений коэффициента мотивации γ накладывается условие: $\gamma \geq (D/g)$.

Особенностью приведенных выше результатов является то, что они получены для гипотетического злоумышленника, который действует по принципу исключительно экономической целесообразности. Это типичный "злоумышленник — прагматик". Однако возможны и другие варианты мотивации возникновения угрозы T, например, обиженный или мстительный злоумышленник ("злоумышленник — мститель"), доминантой действий которого является максимизация потерь q владельца информации при минимальных личных расходах D. Чаще всего причиной действий этого злоумышленника являются определенные личные мотивы, обусловленные недоразумениями или конфликтными ситуациями, возникшими по месту работы, службы, пр. Формула (6) в этом случае принимает вид:

$$P_t = \frac{\gamma q - D}{\gamma q} = 1 - \frac{D}{\gamma q} \quad (5).$$

Следует отметить, что приведенные выше формулы (4), (5) — модели, фактически отражающие сценарии действий злоумышленника, определяемые его психотипом, причем уровень доминантной психологической черты злоумышленника, которая является причиной его асоциального поведения, оценивается именно коэффициентом γ. Очевидно, можно выделить несколько классов психотипов злоумышленника, которые охватывают различные возможные случаи развития атаки и противоправных действий [25; 29].

Другим фактором в формировании сценария действий злоумышленника может быть его социализация, в частности, его профессиональный статус. Так получаем еще один распространенный тип злоумышленника — "злоумышленника — исполнителя", который выполняет чей-то заказ или приказ, то есть атакующие действия по реализации угрозы T— это его обычная работа, которую он просто обязан выполнять. Поэтому в этом случае вероятность активации угрозы T равна $P_t = 1$.

Как это следует из формулы (1), вероятность P_T реализации угрозы T — это произведение

$$P_T = P_t P_v \quad (6).$$

где P_v — вероятность удачного использования злоумышленником уязвимостей информационной системы (ИС), содержащий информационный ресурс и, поэтому вполне естественной является попытка экономико-стоимостной интерпретации этой вероятности. В общем случае P_v — обобщенная (интегрированная) вероятность успешного проведения комплекса атак, порожденных существованием совокупности уязвимостей ИС (включая уязвимостями самой системы защиты информации (СЗИ)). То есть значение вероятности P_v зависит от степени защищенности ИС, который в свою очередь обусловлено объемом вложений в СЗИ (величиной инвестиций c), и определенным образом учитывается моделью [22; 23]:

$$P_v = \frac{q}{q + sc} \quad (7),$$

где s — коэффициент, возможный диапазон значений которого связан с существующей в мировой практике зависимостью между уровнем инвестиций c в СЗИ и ценностью критической информации для ее владельца (сторона В). Так, для коммерческой тайны чаще $c = (0{,}05 \div 0{,}20)\, q$ [23]. В частности для конкретных данных, приведенных в [26], нижняя граница для s определяется из уловия: $s \geq 10 \div 60$. Из формулы (6) очевидно, что при отсутствии критической информации в ИС (т.е. $q = 0$) вероятность $P_v = 0$. При $q >> sc$, т.е. при значительном уровне критичности ресурса I и низких затратах на создание и функционирование СЗИ, следствием чего является объективная невозможность обеспечить адекватный уровень защиты критической информации в ИС, вероятность $P_v \to 1$. Во всех других случаях вероятность P_v отличается от 0, а ее значение при $q = const$ растет с спадением уровня инвестиций в СЗИ.

Однако в модели (7) никак не учитывается уровень профессиональной подготовки атакующнй стороны А, ее ресурсный потенциал, финансово-экономические возможности, отсутствует сопоставление этих характеристик с аналогичными характеристиками защиты. В этом плане болем удачной может оказазаться оценки вероятности реализации уязвимостей, вычисляемая в соответствии с выражением:

$$P_v = \frac{q}{q + s\dfrac{c^2}{D}} \quad (8).$$

Здесь в формуле для вероятности P_v учет ресурсных возможностей атакующей стороны А осуществляется путем умножения значения инвестиций *c* в знаменателе формулы (7) на мультипликатор c/D, позволяющий учесть инвестиции *D*, вносимые стороной *A* в реализацию атаки [24; 27; 28].

Приведенные выше формулы (3) — (8) могут быть применены непосредственно для параметризации и вычисления рисков любой конкретной организации при условии, что существует реальная возможность проанализировать и количественно оценить экономико-стоимостные характеристики реализации угрозы информации. Выходные данные для этих оценок можно получить, выполнив обследование (аудит) состояния информационной безопасности организации в соответствии с требованиями и рекомендациями вышеперечисленных стандартов менеджмента рисков при наличии определенной дополнительной информации.

Кроме того, эти же формулы (3) — (8) позволяют построить оптимизационные схему, по которой можно будет сделать выводы об эффективности и целесообразности инвестиций в СЗИ организации. Предположим [14; 24], что при нулевом инвестировании в СЗИ организации $P_v = 1$ потому исходное значение интегрального информационного риска организации равно $R_1 = P_t q$. Инвестирование в СЗИ средств в размере *C* приводит (при условии рациональных расходов этих средств на нужды защиты) к тому, что вероятность успешного использования уязвимости становится меньше 1, то есть $P_v < 1$. Остаточный риск в этом случае равен $R = P_t P_v q$. Таким образом, величина

потерь, которые удалось предотвратить благодаря инвестированию в СЗИ, составляет

$$R_1 - R = P_t q - P_t P_v q = (1 - P_v) P_t q = P_s P_t q \quad (9),$$

а соответствующая "прибыль" —

$$\Delta_R = R_1 - R - c = (1 - P_v) P_t q - c \quad (10).$$

Заменяя P_v в формуле (10) его развернутым выражением (7), получаем:

$$-c + \frac{sc}{q + sc} P_t q = \Delta_R \quad (11),$$

Из анализа выражения (11) следует, что если уровень инвестиций *c* превышает некоторое пороговое значение $c_{max} = q(P_t s - 1)/s$, "доход" от введения защиты становится отрицательным, то есть в общем случае диапазон возможных значений *c* рационально ограничить условием:

$$0 < c < \frac{q(P_T s - 1)}{s} \quad (12),$$

определяющим так называемым диапазоном "допустимых" инвестиций (термин заимствован из [16]). Из приведенного условия, исключая *c*, получаем неравенство, соблюдение которого накладывает ограничения на возможные значения коэффициента s: $s \geq 1/P_T$.

Полученные выше соотношения (9) — (10) имеют "прозрачную" и легко интерпретируемую структуру, количественные параметры которой фактически представляют собой комбинации параметров риска, которые, как это уже отмечалось выше, предполагают достаточно простую процедуру оценки, напрямую связанную с требованиями и рекомендациями стандартов менеджмента рисков. Анализ соотношения (11) как функции переменной c и исследование его на екстремум, приводит к соотношению:

$$\frac{d\Delta_R}{dc} = \frac{s(q + sc) - s^2 c}{(q + sc)^2} P_t q - 1 = 0 \quad (13).$$

Позволяющему определить [14; 26] объем инвестиций c_{eff}, обеспечивающий получение наибольшего значения Δ_R (по терминологии Гордона-Лоеба c_{eff} — оптимальный объем инвестиций):

$$c_{eff} = \frac{q}{s}(\sqrt{P_t s} - 1) \quad (14),$$

а также значения вероятности P_v и R риска для этого объема инвестиций:

$$P_v(c_{eff}) = \frac{1}{\sqrt{P_t s}},\ R(c_{eff}) = P_v P_t q = q\sqrt{\frac{P_t}{s}} \quad (15).$$

Теперь, имея значение инвестиций c_{eff}, мы можем считать их своеобразным эталоном для того, чтобы адекватно инвестировать в информационную безопасность.

Анализ формулы (14) дает возможность оценить максимальный объем оптимальных инвестиций в СЗИ. Для этого, исследуя на экстремум зависимость (14) как функцию переменной *s*, получаем:

$$\frac{dc_{eff}(s)}{ds} = q(s^{-2} - \frac{1}{2} s^{-3/2}\sqrt{P_t}) = 0 \quad (16).$$

Из равенства (16) находим, что своего экстремума функция $c_{eff}(s)$ достигает при значении $s = 4/P_t$. Этому значению переменной *s* соответствует максимум функции $c_{eff}(s)$:

$$\max[c_{eff}(s)] = c_{eff}(4/P_t) = 0{,}25 q P_t \quad (17).$$

Очевидно, что наибольшей величина оптимальных инвестиций в СЗИ окажется при P_t=1. Таким образом, максимальный объем оптимальных инвестиций в СЗИ равен $c_{eff\,\max} = 0{,}25q$, т.е. составляет 25% стоимости ресурса, который является объектом защиты. Полученное условие можно считать формализацией принципа разумной достаточности при построении СЗИ. Необходимо подчеркнуть, что согласно практическому опыту, накопленному в сфере защиты информации, значение $s \geq 10 \div 60$ [22; 23, 26], причем для высокоэффективных защитных решений $s = 40 \div 60$. Поэтому в соответствии с формулой (6) даже при P_t=1 объем инвестиций в СЗИ может оказаться на уровне 11—13% стоимости защищаемого ресурса.

Следует отметить, что введенное Л. Гордоном и М. Лоебом понятие оптимального объема инвестиций в СЗИ является довольно спорным, так как определяет оптимальным тот уровень инвестиций $c_{eff\,\max}$, при котором максимизируется разность между величиной предотвращенных потерь $R_1 - R$ и объемом *c* инвестиций в СЗИ, обеспечивших снижение риска до значения R_T. При этом совершенно не учитываются такие важные аспекты, как степень эффективности использования сделанных в СЗИ инвестиций или уровень подготовки и ресурсный потенциал атакующей стороны. Ответить на эти вопросы можно было бы, введя дополнительные показатели защищенности ресурса *I*, например, вероятность $P_v(c_{eff})$ и риск $R(c_{eff})$, однако при этом потребуется привлечение дополнительных сведений, а значит придется расстаться с одним из основных преимуществ подхода Гордона-Лоеба — минимальным объемом исходной информации, привлекаемой для оценки максимального объема инвестиций в СЗИ. Рассмотрим этот спорный момент более детально.

Выражение (7) формирует оценку вероятности P_v главным образом на основе "внутренних" представлений организации-владельца ресурса *I* (сторона В) о необходимом уровне защищенности этого ресурса исходя из собственного понимания его ценности q в сопоставлении с разумно достаточными (опять-таки с точки зрения стороны В) расходами на защиту. При этом ценность ресурса *I*, зависящая от важности и значимости ресурса для его владельца В, обычно совпадает с величиной потерь q. Однако реальная степень защищенности ресурса *I* в значительной мере определяется интенсивностью и силой атак стороны А, зависящих от ее представлений о ценности "добываемого" ресурса *I*, т.е. от величины g. Поэтому, если атакующая сторона А точно идентифицирована и для нее достоверно известна величина g, возможно более объективной оценкой вероятности P_v будет оценка, рассчитываемая по формуле [25]:

$$P_v = \frac{g}{g + sc} \quad (18).$$

При одинаковом понимании ценности информации сторонами А и В $g = q$. Тогда оценки, получаемые с использованием формул (7), (18), совпадают, в связи с чем справедливы все приведенные выше соотношения и выводы. Но в общем случае представления сторон А и В о ценности информации асимметричны.

Для владельца ресурса *I* (сторона В) его ценность q обычно рассчитывается на основе анализа стоимостных аспектов создания этого ресурса, процедура расчета часто носит типизированный характер, получаемые оценки достаточно устойчивы.

Для атакующей стороны А ценность g "добытой" информации формируется на основе рыночной стоимости ресурса *I* и количества потенциальных покупателей, желающих заполучить его в свою собственность. Еще один вероятный сценарий формирования g: "добытая" стороной А информация представляет собой информацию с ограниченным доступом (ИсОД), появление которой в открытом доступе может нанести вред ряду третьих сторон. Итог — предъявленные

этими сторонами претензии стороне В (не обеспечившей сохранность ИсОД), объем которых в денежном представлении равен g [25; 27]. Характерной особенностью оценивания значения g является многовариантность развития ситуации в случае достижения успеха атакующей стороной А, плохая прогнозируемость итоговых результатов, их зависимость от множества внешних обстоятельств и, как следствие, нестабильность и неустойчивость получаемых оценочных значений g.

Поэтому актуален вопрос о том, какой из, двух формул, (7) или (18), отдать предпочтение?

Предположим, что $g \neq q$, причем защищающейся стороне В известна оценка g. Тогда, с учетом формулы (18) получаем для соотношения (11) новую форму представления [23; 25]:

$$-c + \frac{sc}{g + sc} P_t q = \Delta_R \qquad (19),$$

а итоговые выражения (14), (17) преобразуются к виду:

$$c_{eff} = \frac{q}{s}\sqrt{P_t s} - \frac{g}{s} \qquad (20),$$

$$\max[c_{eff}(s)] = c_{eff}(4g^2 / P_t q^2) = 0{,}25 q^2 P_t / g \qquad (21).$$

Наибольшей величина оптимальных инвестиций в СЗИ окажется при P_t=1 и составит $c_{eff\max} = 0{,}25q^2 / g$ [25]. Анализ последнего выражения, а также сопоставление формул, полученных для случая $g = q$, с соответствующими им соотношениями при $g \neq q$, показывает, что несовпадение g и q может стать причиной недостаточного или наоборот, избыточного инвестирования в СЗИ. В частности, при $g > q$ расчеты, проведенные в предположении справедливости соотношений (7), (14), (17), ведут к занижению значения вероятности P_v и недостаточному инвестированию в СЗИ, при $g < q$ ситуация диаметрально противоположна. По-видимому, для получения объективных данных о наибольшей величине оптимальных инвестиций в СЗИ в случае $g > q$ желательно пользоваться формулой (18) и получаемыми на ее основе соотношениями (15) — (21), поэтому, помимо сведений об уровне потерь q защищающейся стороны В, необходима информация о ценности g ресурса *I* для атакующей стороны А. В случае $g \leq q$ для оценивания наибольшей величины оптимальных инвестиций в СЗИ следует использовать соотношение (7), учитывая при этом сделанное выше замечание о нестабильности и неустойчивости получаемых оценочных значений g.

В связи с возможным субъективизмом получаемых выше решений представляют интерес перспективы применения других моделей, описывающих вероятностные параметры рисков.

При оценивании вероятности P_v, как уже отмечалось выше, учет ресурсного потенциала атакующей стороны А и его сопоставление с аналогичными характеристиками защиты можно реализовать, используя формулу (8). В частности, введеный в знаменатель формулы (8) мультипликатор c/D позволяет сопоставить инвестиции *D*, вносимые стороной А в реализацию атаки [25; 27] с затратами с защиты: очевидно, что рост расходов *D* обусловливает увеличение вероятности P_v.

Использование формул (3), (8) для вычисления риска приводит к выражению вида:

$$R = P_t \frac{q}{q + s\dfrac{c^2}{D}} q = \left(1 - \frac{D}{g}\right) \frac{q^2 D}{qD + sc^2} \qquad (22).$$

График зависимости $R(c)$ представлен на рисунке 2. К сожалению, подстановка найденного риска (22) в выражение (9) для последующего построения оптимизационной процедуры, аналогичной рассмотренной выше (выражения (10) — (14)), не позволяет получить решение в явном виде. Зависимость $R_1 - R = (1 - P_v) P_t q$ после подстановки в нее выражения (22) приобретает логистический характер (рис. 3), а анализ неравенства $\Delta_R = R_1 - R - c \geq 0$ дает возможность лишь определить диапазон допустимых инвестиций [25]:

$$\frac{qP_t}{2}\left(1 - \sqrt{1 - \frac{4D}{sqP_t^2}}\right) \leq c \leq \frac{qP_t}{2}\left(1 + \sqrt{1 - \frac{4D}{sqP_t^2}}\right) \qquad (23).$$

Правой и левой границам неравенства (17) соответствуют обозначенис c_1 и c_2 на рисунке 3.

Наличие процедуры извлечения квадратного корня в формуле (17) предполагает очевидное условие $1 \geq 4D / sqP_t^2$, трансформирующееся в ограничение вида:

$$D \leq 0{,}25 sqP_t^2 \qquad (24),$$

накладываемое на объем инвестиций атакующей стороны А. Кроме того, необходимость применения формулы (3) для оценивания вероятности активации (возникновения) угрозы *T* вводит характерное ограничение $g \geq D$, которое, как показывает практика, является более слабым по сравнению с условием (24).

При интерпретации полученных выше результатов следует принимать во внимание, что, анализируя модель риска (23), следует учитывать наличие в ней двух существенных переменных, c и D, отражающих влияние на формирование ситуации риска ресурсных потенциалов двух сторон-антагонистов А и В. При этом можно выделить три базовых варианта (шаблона) рисковых ситуаций.

Вариант 1. Финансово-экономические возможности атакующей стороны крайне скромны, злоумышленник вероятнее всего одиночка, не имеющий достаточного опыта и знаний, необходимых для реализации эффективных атакующих действий. Полагая, что асимптотику для этого варианта получаем, исследуя соотношения (23) при $D \to 0$, оценим граничные значения диапазона допустимых инвестиций:

$$0 \leq c \leq qP_t \qquad (25).$$

Оценочное значение наибольшей величины оптимальных инвестиций в СЗИ для этого случая очевидно не превысит $c_{eff\max} = 0{,}25q$.

Вариант 2. Атакующая сторона — одна особа либо группа лиц, обладающих достаточным опытом и необходимыми профессиональными знаниями, но имеющая ограниченные финансово-экономические возможности. Исследуем этот вариант, увеличивая значения инвестиций D атакующей стороны. При $D \to 0{,}25 sqP_t^2$ правая c_1 и левая c_2 границы диапазона (23) сближаются, стягиваясь в точку $c = \dfrac{qP_t}{2}$ при $D = 0{,}25 sqP_t^2$. В этом предельном случае наибольшая величина оптимальных инвестиций в СЗИ составит $c_{eff\max} = 0{,}5q$.

Вариант 3. "Злоумышленник — исполнитель". Модель риска для этого варианта имеет вид:

$$R = \frac{q}{q + s\dfrac{c^2}{D}} q \qquad (26).$$

Выше уже не раз отмечалось, что в ситуации "атака-защита" обе стороны в своих действиях обычно руководствуется принципом экономической целесообразности (разумной достаточности). В частности, в двух представленных выше вариантах рисковых ситуаций этот принцип

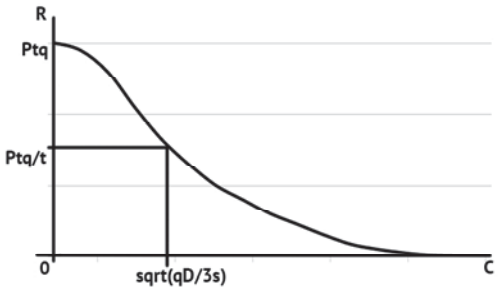

Рис. 2. Зависимость величины риска R от уровня инвестиций в СЗИ

учитывался наличием пары ограничений: $D \le 0{,}25sgP_t^2$ и $g \ge D$. Однако, как показано в [25; 27], при определенных обстоятельствах приведенные ограничения могут оказаться не актуальными. Например, это касается ситуации, в которой атакующая сторона для достижения своих целей прибегает к услугам наемного исполнителя (отсюда название модели — "Злоумышленник — исполнитель"), который при любых обстоятельствах обязан выполнять поставленные перед ним задания (т. е. для него вероятность активации угрозы $P_t \equiv 1$ и, соответственно, $P_T \equiv P_v$).

С другой стороны, применимость использованой ранее формулы (3) для описания ситуации "атака — защита" базировалась на сопоставлении чистой прибыли злоумышленника g— D с ценностью g ресурса *I*. Если эта ценность ресурса *I* для атакующей стороны А значительна, в частности, если $g >> D$, можно предположить, что злоумышленник попытается использовать любые шансы для реализации своей угрозы *T*. Очевидно, что в этой ситуации $P_t \to 1$, т. е. приходим к уже сформулированному выше тождеству $P_T \equiv P_v$.

Однако наиболее существенная особенность Варианта 3 состоит в том, что в случае особой важности поставленной перед "злоумышленником — исполнителем" цели, он может рассчитывать на привлечение для поддержки своих действий определенных дополнительных ресурсов: финансовых, технических, информационно-аналитических, оперативных. На практике это означает возможность реализации в рамках сценариев Варианта 3 очень высокозатратных атак. При этом очевидно, что если $D \to \infty$, то $P_v \to 1$, т. е. в этой ситуации успешная реализация угрозы атакующей стороной А оказывается практически гарантированной. Типичным примером подобной ситуации является выполнение особо важного задания сотрудником спецслужбы, являющимся профессионалом, подготовленным к осуществлению атакующих действий в киберпространстве.

Кроме того, если защищающаяся сторона В, создавая свою СЗИ, исходит из принципа разумной достаточности, основываясь исключительно на собственных ("внутренних") представлениях о ценности q защищаемого ресурса *I*, атакующая сторона может добиться успеха и при сравнительно низких расходах D (фактически получаем ситуацию с асимметричными представлениями сторон А и В о ценности одного и того же информационного ресурса *I*, уже рассмотренную выше, формула (21), случай $g > q$).

ВЫВОДЫ

Наиболее распространенным в практике защиты информации методам анализа и исследования рисков, приводимым в международных и национальных стандартах, присущ ряд недостатков, в частности, слишком общий концептуально-рекомендательный характер представления материалов, что практически исключает возможность учета при анализе характерных специфических свойств объектов риска и существенно уменьшает объективность и точность полученных результатов.

С другой стороны, использование известных моделей Гордона — Лоеба для исследования проблемы эффективности инвестирования в системы защиты практически исключает возможность учета в этих исследованиях конкретики реального объекта риска и фактически отделяет этот подход от прикладных исследований реальных объектов рисков. По сути модель Гордона — Лоеба не приспособлена для решения прикладных узкопрофильных задач.

В этой ситуации перспективным представляется применение для анализа и исследования инвестиций и рисков методологии, базирующейся на учете мотивационно-стоимостных и финансово-экономических особенностей ситуации "атака — защита" на объектах информационной деятельности через выделение ряда типовых сценариев возникновения и развития этой

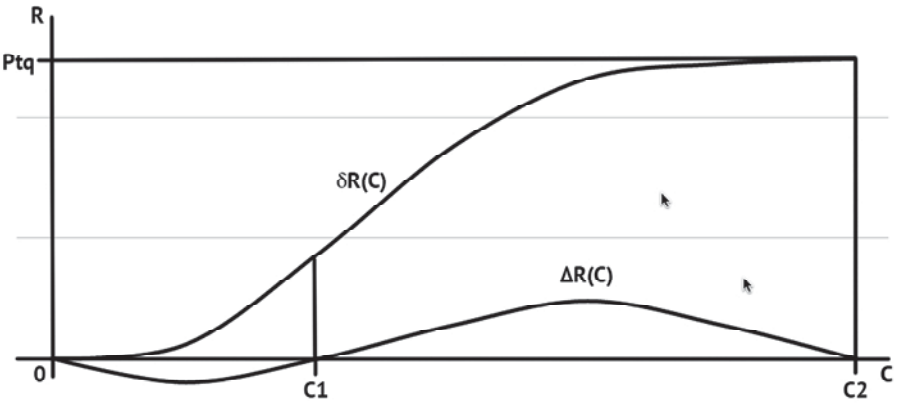

Рис. 3. Зависимость $\Delta_R = R_1 - R - c = (1 - P_v)P_t q - c$

ситуации и построения соответствующих моделей экономико-стоимостных, мотивационных и экономико-ресурсных отношений, характерных для ситуации "атака — защита" в информационной сфере. Для идентификации моделей могут быть вполне успешно использованы данные и сведения, определяемые в соответствии с требованиями и рекомендациями международных стандартов. В ходе выполненных исследований получена оценка рационального объема инвестиций в СЗИ, согласно которой этот объем не должен превышать 25% стоимости защищаемого информационного ресурса.

Литература:

1. BS 7799-3:2006 Information security management systems. Guidelines for information security risk management, available at: http://www.ganino.com/games/British%20standard/BS/BS%207799-3-2006.pdf (Accessed 10 Jan 2016).

2. ISO/IEC 27005:2011, "Information security risk management", available at: http://www.iso27001security.com/html/27005.html (Accessed 10 Jan 2016).

3. ISO/IEC TR 13335-3:1998 Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT Security, available at: http://shop.bsigroup.com/ProductDetail/?pid=-000000000001496613 (Accessed 10 Jan 2016).

4. ISO/IEC TR 13335-4:2000 Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards, available at: http://shop.bsigroup.com/ProductDetail/?pid=000000000030107710 (Accessed 10 Jan 2016).

5. ISO/IEC 16085:2006 Systems and software engineering — Life cycle processes — Risk management, available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=40723 (Accessed 10 Jan 2016).

6. BS 31100:2011 Risk management.Code of practice and guidance for the implementation of BS ISO 31000, available at: http://shop.bsigroup.com/ProductDetail/?pid=000000000030228064 (Accessed 10 Jan 2016).

7. AS/NZS 4360:2004 (In the form of AS/NZS ISO 31000:2009 — Principles and Guidelines on Implementation), available at: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=-web&cd=4&ved=0ahUKEwjs48Pdw-5zKAhUm83IKHSGnA3wQFggxMAM&url=http%3A%-2F%2Fwww.ua.ac.be%2Fdownload.aspx%3Fc%3D.ARGOSS%26n%3D63180%26ct%3D61288%-26e%3D160543&usg=AFQjCNH8YnUgELxLnfGWI7B-GA0SZwWh02g&sig2=0dczb_TLGN6MGTmQU8w-G9g&cad=rja (Accessed 10 Jan 2016).

8. NIST Special Publication 800-30 — Risk Management Guide for Information Technology Systems — Recommendations of the National Institute of Standards, available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (Accessed 10 Jan 2016).

9. Марцынковский Д.А., Владимирцев А.В., Марцынковский О.А. Марцынковский Д.А. Руководство по риск-менеджменту // Ассоциация по сертификации "Русский Регистр". — Санкт-Петербург: Береста, 2007.

10. Симонов С. Анализ рисков, управление рисками // JetInfo. — № 1. — 1999.

11. ISO/IEC 17799:2005 — Information technology — Security techniques — Code of practice for information security management, available at: http://www.iso.org/iso/ru/catalogue_detail?csnumber=39612 (Accessed 10 Jan 2016).

12. Олександрович Г.Я., Нестеров С.А., Петренко С.А. Автоматизация оценки информационных рисков компании // Защита информации. Конфидент. — 2003. — № 2. — С. 78—81.

13. Симонов С. Технологии и инструментарии для управления рисками // JetInfo — № 2 — 2003.

14. Архипов А.Е. Применение экономико-мотивационных соотношений для оценивания вероятностных параметров информационных рисков // Захист інформації — 2011. — №2 (51). — С. 69—76.

15. Левченко Є.Г., Рабчун А.О. Оптимізаційні задачі менеджменту інформаційної безпеки // Сучасний захист інформації. — 2010. — №1. — С.16—23.

16. Gordon L.A., Loeb M.P. (2002), "The Economics of Information Security Investment", ACM Transaction on Information and System Security, vol. 5, No 4, pp. 438—457.

17. Willemson J. (2010)"Extending the Gordon&Loeb Model for Information Security Investment" // Fifth International Conference on Availability, Reliability, and Security (ARES2010), pp. 258—261.

18. Willemson J. (2006) "On the Gordon & Loeb Model for InformationSecurity Investment" // Proceedings of The FifthWorkshop on the Economics of Information Security (WEIS 2006), pp. 101—112.

19. Hausken K. (2006) "Returns to Information Security Investment: The Effect of Alternative Information Security BreachFunctions on Optimal Investment and Sensitivity toVulnerability" // Information Systems Frontiers. — No. 5 (8). — pp. 338—349.

20. Huang C.D., Hu, Q., Behara, R.S. "Economics of Information Security Investment in the Case of Simultaneous Attacks" // Proceedings of the Fifth Workshop on the Economics of Information Security. Cambridge, 2006, England.

21. Gordon L.A., Loeb M.P., Lucyshyn W., & Zhou L. "Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. " // Journal of Information Security. — Vol. 6. — 2014.

22. Архипов А.Е. Применения мотивационно-стоимостных моделей для описания вероятностных соотношений в системе "атака-защита" //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2008. — Вип. 1 (16). — С. 57—61.

23. Архипов А.Е. Особенности анализа рисков в информационно-коммуникационных системах // Захист інформації — 2012. — № 4 (57). — С.18—27.

24. Архипов А.Е. Применение экономико-стоимостных моделей информационных рисков для оценивания предельных объемов инвестиций в безопасность информации // А.Е. Архипов. Захист інформації. — 2015. — Т. 17, № 3. — С. 211—218.

25. Архипов О.Є., Скиба А.В., Хоріна О.І. Розширення економіко-вартісних моделей інформаційних ризиків за рахунок використання соціально-психологічних типів зловмисника // Захист інформації. — 17 (1), Київ: 2015. — С. 60—72.

26. Андрощук Г.А., Крайнев П.П. Экономическая безопасность предприятия: защита коммерческой тайны. — К.: Изд. Дом "Ин Юре", 2000. — 400 с.

27. Архипов О.Є. Вступ до теорії ризиків: інформаційні ризики: моногр. — К.: Нац. Акад. СБУ, 2015. — 248 с.

28. Скиба А., Хоріна О.І. Прогнозування соціально-психологічних та ситуаційних чинників активації злочинних думок і намірів у сфері інформаційної безпеки // Безпека інформації. — 2015. — Т. 21. — № 2 — С. 165—173.

References:

1. BSI Standards (2006), "BS 7799-3:2006 Information security management systems. Guidelines for information security risk management", available at: http://www.ganino.com/games/British%-20standard/BS/BS%2007799-3-2006.pdf (Accessed 10 Jan 2016).

2. ISO/IEC 27005 (2011), "Information security risk management", available at: http://www.iso-27001security.com/html/27005.html (Accessed 10 Jan 2016).

3. ISO/IEC TR 13335-3 (1998), "Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security", available at: http://shop.bsigroup.com/ProductDetail/?pid=000000000001496613 (Accessed 10 Jan 2016).

4. ISO/IEC TR 13335-4 (2000), "Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards", available at: http://shop.bsigroup.com/ProductDetail/?pid=000000000030107710 (Accessed 10 Jan 2016).

5. ISO/IEC 16085 (2006), "Systems and software engineering — Life cycle processes - Risk management", available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=40723 (Accessed 10 Jan 2016).

6. BSI Standards (2011), "BS 31100:2011 Risk management.Code of practice and guidance for the implementation of BS ISO 31000", available at: http://shop.bsigroup.com/ProductDetail/?pid=00-0000000030228064 (Accessed 10 Jan 2016).

7. AS/NZS 4360 (2004), "In the form of AS/NZS ISO 31000:2009 — Principles and Guidelines on Implementation", available at: https://www.google.-com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&-cd=4&ved=0ahUKEwjs48P-dw5zKAhUm83IKHSGnA3wQFg-gxMAM&url=http%3A%2F%2Fwww.ua.-ac.be%2Fdownload.aspx%3Fc%3D.ARGOSS-%26n%3D63180%26ct%3D61288%-26e%3D160543&usg=AFQjCNH8Yn-UgELxLnfGWI7BGA0SZwWh02g&sig2=-0dczb_TLGN6MGTmQU8wG9g&cad=rja (Accessed 10 Jan 2016).

8. NIST (2002), "Risk Management Guide for Information Technology Systems — Recommendations of the National Institute of Standards", available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (Accessed 10 Jan 2016).

9. Martsynkovskyi, D.A. Vladymyrtsev, A.V. and Martsynkovskyi, O.A. (2007), Rukovodstvo po ryskmenedzhmentu [Guide to Risk Management], Assotsyatsyia po sertyfykatsyy "Russkyi Rehystr" Beresta, Sankt-Peterburh, Russia.

10. Symono, S. (1999), "Risk analysis, risk management", JetInfo, vol. 1.

11. ISO/IEC 17799 (2005), "Information technology - Security techniques - Code of practice for information security management", available at: http://www.iso.-org/iso/ru/catalogue_detail?csnumber=39612 (Accessed 10 Jan 2016).

12. Oleksandrovich, G.Ya. Nesterov, S.A. and Petrenko S.A. (2003), "Automation of the company's risk assessment information", Zaschita informatsii. Konfident, vol. 2, pp. 78—81.

13. Simonov, S. (2003), "Technologies and tools for risk management", JetInfo, vol. 2.

14. Arhipov, A.E. (2011), "Application of economic and motivational relations for estimating the probability parameters of information risks", Zahist Informatsiyi, vol. 2 (51) , pp. 69—76.

15. Levchenko, E.G. and Rabchun, A.O. (2010), "Optimization tasks of management of information security", Suchasniy zahist Informatsyi, vol. 1, pp.16—23.

16. Gordon, L.A. and Loeb, M.P. (2002), "The Economics of Information Security Investment", ACM Transaction on Information and System Security, Vol.5, No4, pp. 438—457.

17. Willemson, J. (2010), "Extending the Gordon&Loeb Model for Information Security Investment", Fifth International Conference on Availability, Reliability, and Security (ARES2010), pp. 258—261.

18. Willemson, J. (2006), "On the Gordon & Loeb Model for InformationSecurity Investment", Proceedings of The FifthWorkshop on the Economics of Information Security (WEIS 2006), pp. 101—112.

19. Hausken, K. (2006), "Returns to Information Security Investment: The Effect of Alternative Information Security BreachFunctions on Optimal Investment and Sensitivity toVulnerability", Information Systems Frontiers, vol. 5, no. 8, pp. 338—349.

20. Huang, C.D. Hu, Q. and Behara, R.S. (2006), "Economics of Information Security Investment in the Case of Simultaneous Attacks", Proceedings of the Fifth Workshop on the Economics of Information Security. Cambridge, England.

21. Gordon, L. A. Loeb, M. P. Lucyshyn, W. and Zhou, L. (2014), "Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model", Journal of Information Security, Vol.6

22. Arkhypov, O. (2008), "Applications motivational-cost models to describe the probabilistic relationships in the "attack-defense"", Pravove, normativne ta metrologlchne zabezpechennya sistemi zahistu Informatsiyi v Ukrayini, vol. 1(16), pp. 57—61.

23. Arkhypov, O. (2012), "Features of the analysis of risks in the information and communication systems", Zahist Informatsiyi, vol.4 (57) , pp.18-27.

24. Arkhypov, O. (2015), "Application of economic and cost models for the evaluation of risks at the limit of investment in information security", Zahist Informatsiyi, vol. 17, no. 3, pp. 211—218.

25. Arkhypov, O. Skyba, A. and Khorina, O. (2015), "An extension of economic cost model of information risks indentification by social-psychological types of attacker", Information Security Research Journal, Vol 17, no. 1, pp. 60—72.

26. Androschuk, G.A. and Kraynev, P.P. (2000), Ekonomicheskaya bezopasnost predpriyatiya: zaschita kommercheskoy taynyi [Economic security of enterprise: protection of trade secrets], Izd. Dom "In Yure", Kyiv, Ukraine.

27. Arkhypov, O. (2015), Vstup do teorIYi rizikIv: Informatsiyni riziki [Introduction to the theory of risks: risks Information], Nats. Akad. SBU, Kyiv, Ukraine.

28. Skiba, A. and Horina, O.I. (2015), "Prediction of socio-psychological and situational factors activation criminal thoughts and intents of information security", Bezpeka Informatsiyi, vol. 21, no. 2, pp. 165—173.

Стаття надійшла до редакції 10.01.2016 р.