УДК 004.056.53

ПРИМЕНЕНИЕ ЭКОНОМИКО-СТОИМОСТНЫХ МОДЕЛЕЙ ИНФОРМАЦИОННЫХ РИСКОВ ДЛЯ ОЦЕНИВАНИЯ ПРЕДЕЛЬНЫХ ОБЪЕМОВ ИНВЕСТИЦИЙ В БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

Александр Архипов

Рассмотривается проблема определения максимального размера инвестиций в систему защиты информации. Осуществлен анализ публикаций, содержащих материалы, связанные с исследованием и развитием подхода Гордона-Лоеба, в котором обосновывается предельный объем инвестиций в безопасность информации. Показано, что данный подход не позволяет получить однозначный ответ: субъективный формально-аппроксимативных способ задания модели, на которой базируется получаемое решение, порождает множественность возможных моделей и, как следствие, - множественность решений. Предложен подход к решению задачи определения объема инвестиций в систему защиты информации, основанный на исследовании модели информационных рисков. Формирование ее структуры и параметров базируется на использовании сведений о реальных механизмах развития и реализации информационных угроз, в частности, на экономико-стоимостной модели, используемой для оценивания вероятности успешной реализации атак уязвимостей информационной системы. По результатам исследования получена оценка максимального объема инвестиций в систему защиты информации, составляющая 25% стоимости защищаемого информационного ресурса (или потерь, обусловленных реализацией угрозы относительно этого ресурса). Отмечено, что при применении в системе защиты информации высокоэффективных решений уровень инвестирования может быть уменьшен до 11-13%. Рассмотрены перспективы применения в исследованиях моделей, основывающихся на мотивационных и ресурсных отношениях, характерных для ситуации «атака-защита» в информационной сфере.

***Ключевые слова**: риск, моделирование рисков, экономико-стоимостные модели, диапазон разумных инвестиции.*

Введение и постановка задачи. По данным О. Лукацкого, бизнес-консультанта Cisco по безопасности, 78% организаций на мероприятия, связанные с безопасностью информации, тратят не более 15% от их ИТ-бюджета, еще 11% организаций – от 16 до 20 %, и только 7% организаций – от 21 до 28% [1]. Следует отметить, что статистики, подобные приведенной выше, носят очевидный эмпирический характер и отражают стихийно сложившуюся к текущему моменту ситуацию с инвестированием в сферу защиты информации. К сожалению, эти статистики часто служат базой для формирования рекомендаций по оцениванию уровня инвестиций в построение систем защиты информации (СЗИ) в рамках так называемого «практического подхода» [2], придавая оттенок обоснованности фактически ничем не подтвержденным рекомендациям. Именно этим объясняется пристальное внимание к опубликованной в 2002 статье американских исследователей в области экономики Лоуренса Гордона и Мартина Лоеба [3], в которой ими предпринята попытка теоретико-методологического обоснования предельного объема инвестиций в безопасность информации. Появление этой статьи вызвало широкий резонанс в научных и профессиональных кругах: многочисленные отзывы и комментарии как положительного, так и критического характера, замечания, предложения, дополнения [4–6].

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) [5, 6], в которых несколько изменена и расширена исходная система аксиом Гордона-Лоеба, других модификаций положений подхода Гордона-Лоеба. При этом изменялась и величина оптимального объе-

ма инвестиций в СЗИ: в статье [5] она достигает 100% от величины максимально возможных потерь, а в новой статье Гордона и Лоеба [7], 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 существенный 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.

В этой ситуации интерес представляют модели, предложенные для исследования экономико-мотивационно отношений, характерных для ситуации «атака-защита» в информационной сфере [8, 9].

Применение экономико-стоимостных моделей для оценивания объема инвестиций в безопасность информации. Рассмотрим ситуацию, возникающую при реализации атакующей стороной А (злоумышленник) угрозы *T* относительно некоторого информационного ресурса *I*, принадлежит стороне В. Полагаем, что *D* – общая стоимость расходов атакующей стороны А на реализацию угрозы *T*, *g* – полученный при этом «выигрыш», величина которого обусловливается ценностью ресурса *I* для злоумышленника. Ущерб, понесенный в этой ситуации стороной В (владелец ресурса *I*), то есть стоимость ресурса с точки зрения его владельца, оценивается им как *q*, а общая стоимость реализованного комплекса защитных мероприятий равна *c*.

В общем случае вероятность реализации угрозы *T* относительно некоторого информационного ресурса *I* [2] – это произведение

$$P_T = P_t P_v, \qquad (1)$$

где P_t – вероятность активации (возникновения) угрозы относительно информационного ресурса *I*, P_v – вероятность удачного использования Злоумышленник уязвимостей информационной системы (ИС), содержащей этот ресурс *I*.

Значение вероятности P_v зависит от уровня защищенности ИС, который в свою очередь обусловлен объемом инвестиций *c* в систему защиты информации (СЗИ), что с определенным приближением можно учесть соотношением [8, 9]:

$$P_v = \frac{q}{q + sc}, \qquad (2)$$

где *s* – коэффициент, который определяет уровень эффективности инвестиций *c* в СЗИ: чем больше значение *s*, тем ниже, при условии одного и того же объема *c* инвестиций, величина вероятности P_v. Из формулы (2) очевидно, что при отсутствии ценной информации в ИС (т.е. *q*=0) вероятность $P_v = 0$. Когда ценность *q* ресурса *I* высока или очень высока, однако расходы на создание и функционирование СЗИ низкие, т.е. *q*>>*sc*, вероятность $P_v \to 1$. Если владелец ресурса *I* объективно учитывает его ценность *q* и уделяет его защите соответствующее внимание, значения *q* и *sc* могут оказаться соразмерными, но при этом всегда будет выполняться условие $0 < P_v < 1$. В общем случае значения вероятности P_v при *q*=*const* растут с падением уровня инвестиций *c* в СЗИ и наоборот, уменьшаются с ростом объема инвестиций.

Формулы (1), (2) позволяют построить оптимизационную процедуру, из которой можно будет сделать выводы о эффективности и целесообразности инвестиций в СЗИ организации. Для этого предположим [9], что при нулевых инвестициях в СЗИ организации P_v=1 и выходной информационный риск составляет $R_1 = P_t q$. Инвестирование в СЗИ средств в размере *c* приводит (при условии рационального расходования этих средств для целей защиты) к тому, что вероятность успешного использования уязвимости становится меньше 1, то есть P_v<1. Остаточный риск в этом случае будет равен $R_T = P_t P_v q$, величина потерь, которые удалось предотвратить – $R_1 - R_T = P_t q - P_t P_v q = (1 - P_v) P_t q$, а соответствующая «прибыль» -

$$\Delta_R = R_1 - R_T - c = (1 - P_v) P_t q - c. \qquad (3)$$

Заменяя P_v в формуле (3) его развернутым выражением (2), получаем:

$$-c+\frac{sc}{q+sc}P_t q=\Delta_R, \quad (4)$$

Из анализа выражения (4) 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: $0<c<q(s-1)/s$ – так называемым диапазоном «разумных» инвестиций. Из приведенное условия, исключая c, получаем неравенство: $0<q\ (s-1)/s$, требование соблюдение которого накладывает ограничения на возможные значения коэффициента s: $s>1$.

Исследуя соотношения (4) на экстремум (считая, что Δ_R является функцией переменной c), получаем равенство:

$$\frac{d\Delta_R}{dc}=\frac{s(q+sc)-s^2c}{(q+sc)^2}P_t q-1=0, \quad (5)$$

из условия выполнения которого определяем [9] объем инвестиций c_{eff}, обеспечивающий получение наибольшего значения Δ_R (по терминологии Гордона-Лоеба c_{eff} – оптимальный объем инвестиций):

$$c_{eff}=\frac{q}{s}(\sqrt{P_t s}-1), \quad (6)$$

а также формулы для расчета значение вероятности P_v и риска R в условиях оптимального объема инвестиций:

$$P_v(c_{eff})=\frac{1}{\sqrt{P_t s}},\ R_T(c_{eff})=P_v(c_{eff})P_t q=q\sqrt{\frac{P_t}{s}}. \quad (7)$$

Анализ формулы (6) дает возможность оценить максимальный объем оптимальных инвестиций в СЗИ. Исследуя на экстремум зависимость (6) как функцию переменной s, получаем:

$$\frac{dc_{eff}(s)}{ds}=q(s^{-2}-\frac{1}{2}s^{-3/2}\sqrt{P_t})=0. \quad (8)$$

Из равенства (8) находим, что своего экстремума функция $c_{eff}(s)$ достигает при значении $s=4/P_t$. Этому значению переменной s соответствует максимум функции $c_{eff}(s)$:

$$\max[c_{eff}(s)]=c_{eff}(4/P_t)=0{,}25qP_t. \quad (9)$$

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 $s\geq 10\div 45$ [8, 9], 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_T 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 $R_T(c_{eff})$, 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 (2) 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:

$$P_v = \frac{g}{g + sc}. \qquad (10)$$

При одинаковом понимании ценности информации сторонами А и В $g = q$. Тогда оценки, получаемые с использованием формул (2), (10), 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 [12]. 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, (2) или (10), отдать предпочтение?

Предположим, что $g \neq q$, причем защищающейся стороне В известна оценка g. Тогда, с учетом формулы (10) получаем для соотношения (4) новую форму представления:

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

а итоговые выражения (6), (9) преобразуются к виду:

$$c_{eff} = \frac{q}{s}\sqrt{P_t s} - \frac{g}{s}, \qquad (12)$$

$$\max[c_{eff}(s)] = c_{eff}(4g^2 / P_t q^2) = 0{,}25 q^2 P_t / g. \qquad (13)$$

Наибольшей величина оптимальных инвестиций в СЗИ окажется при $P_t = 1$ и составит $c_{eff\,\max} = 0{,}25 q^2 / g$. Анализ последнего выражения, а также сопоставление исходных формул (2), (6), (9), 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 $g = q$, ведут к занижению значения вероятности P_v и недостаточному инвестированию в СЗИ (все показатели занижены в g / q раз), 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 (10) и получаемыми на ее основе соотношениями (11) – (13), 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 (9), учитывая при этом сделанное выше замечание о нестабильности и неустойчивости получаемых оценочных значений g.

В связи с неоднозначностью получаемых выше решений представляет интерес возможность применения других моделей, описывающих вероятностные параметры риска, альтернативных рассмотренным.

Учет мотивационных и ресурсных аспектов ситуации «атака-защита» при моделировании действий атакующей стороны. Постановка и способы решения задачи защиты информации в организации могут варьироваться в очень широких пределах, в зависимости от отношения организации к вопросам информационной безопасности (ИБ). Основным фактором, который определяет характер этих отношений, является степень (уровень) зрелости организации в аспекте ИБ [2]. Учет этого фактора в формуле

(2) осуществляется выбором значения коэффициента эффективности инвестиций *s*: более высокому уровню зрелости организации соответствует большее значение *s*. Однако величина коэффициент эффективности инвестиций *s* зависит не только от поведения защищающейся стороны В, но и от усилий и целеустремленности действий атакующей стороны А. Поэтому адекватное задание значения *s* оказывается очень сложной задачей. Упростить ее решение можно, используя основные факторы, определяющие потенциал атакующей стороны, непосредственно для вычисления вероятностных параметров P_t и P_v оценки риска. В частности, учет мотивационных аспектов в действиях атакующей стороны А позволяет для оценивания вероятности активации (возникновения) угрозы P_t относительно информационного ресурса *I* использовать соотношение [8, 9]:

$$P_t = \frac{g - D}{g} = 1 - \frac{D}{g}. \qquad (14)$$

Применимость предложенной формулы для описания ситуации «атака-защита» поясняется следующим образом: чистая прибыль злоумышленника в случае успешной реализации угрозы *T* составляет *g* - *D*. Если ценность *g* ресурса *I* для атакующей стороны А значительная, в частности, если *g*>>*D*, можно предположить, что злоумышленник попытается использовать любые шансы для реализации этой угрозы. Напротив, для малых значений *g* экономические мотивы возникновения угрозы *T* практически отсутствуют: при *g*=*D* атака становится нецелесообразной, в этом случае $P_t = 0$, а для *g*<*D* попытка реализации угрозы *T* теряет всякий экономический смысл.

Для вероятности P_v учет ресурсных возможностей атакующей стороны А осуществляется путем умножения значения инвестиций *c* в знаменателе формулы (2) на мультипликатор c/D, позволяющий учесть инвестиции *D,* вносимые стороной А в реализацию атаки [10, 11]:

$$P_v(c, D) = \frac{q}{q + s\dfrac{c^2}{D}}. \qquad (15)$$

Очевидно, что рост расходов *D* обусловливает увеличение вероятности P_v. Использование формул (14), (15) для вычисления риска приводит к выражению вида:

$$R_T = P_t \frac{q}{q + s\dfrac{c^2}{D}} q = \left(1 - \frac{D}{g}\right)\frac{q^2 D}{qD + sc^2}. \qquad (16)$$

К сожалению, подстановка найденного риска (16) в выражение (3) для последующего построением оптимизационной процедуры, аналогичной рассмотренной выше (выражения (5), (6)), не позволяет получить решение в явном виде. Зависимость $R_1 - R_t = (1 - P_v)P_t q$ после подстановки в нее выражения (16) приобретает логистический характер, а анализ неравенства $\Delta_R = R_1 - R_t - c \geq 0$ дает возможность лишь определить диапазон разумных инвестиций:

$$\frac{qP_t}{2}\left(1 - \sqrt{1 - \frac{4D}{sqP_t^2}}\right) \leq c \leq \frac{qP_t}{2}\left(1 + \sqrt{1 - \frac{4D}{sqP_t^2}}\right). \qquad (17)$$

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

$$D \leq 0{,}25sqP_t^2, \qquad (18)$$

накладываемое на объем инвестиций атакующей стороны А. Кроме того, необходимость применения формулы (14) для оценивания вероятности активации (возникновения) угрозы *T* вводит характерное ограничение $g \geq D$, которое, как показывает практика, является более слабым по сравнению с условием (16). Исследование соотношения (16) для $D = 0$ позволяет оценить граничные значения диапазона разумных инвестиций:

$$0 \leq c \leq q. \qquad (19)$$

С увеличением значений D, при $D \to 0{,}25sqP_t^2$ правая и левая границы диапазона (17) сближаются, стягиваясь в точку $c = \dfrac{qP_t}{2}$ для $D = 0{,}25sqP_t^2$, т.е. в этом предельном случае наибольшая величина оптимальных инвестиций в СЗИ составит $c_{eff\,\max} = 0{,}5q$.

Отметим, что наличие двух приведенных выше ограничений $D \leq 0{,}25sgP_t^2$ и $g \geq D$ характерно для ситуации, когда атакующая сторона А в своих действиях руководствуется исключительно принципом экономической целесообразности (разумной достаточности).

Однако, как показано в [10, 11], при определенных обстоятельствах принцип экономической

целесообразности может не выполняться. Это касается ситуации, в которой атакующая сторона для достижения своих целей прибегает к услугам наемного исполнителя, который при любых обстоятельствах должен выполнять поставленную перед ним задачу (т. е. для него вероятность активации угрозы $P_t \equiv 1$ и, соответственно, $P_T \equiv P_v$). Типичным примером подобной ситуации является выполнение задачи сотрудником спецслужбы, являющимся профессионалом, подготовленным к осуществлению атакующих действий в киберпространстве. В зависимости от важности поставленной перед ним цели, такой «злоумышленник-исполнитель» во многих случаях может рассчитывать на привлечение для поддержки своих действий определенных дополнительных ресурсов: финансовых, технических, информационно-аналитических, оперативных. На практике это означает, что в случае «злоумышленника-исполнителя» существует большая вероятность реализации им высокозатратных атак. В частности, если $D \to \infty$, то $P_v \to 1$, т.е. в этой ситуации, если защищающаяся сторона В, создавая свою СЗИ, исходит из принципа разумной достаточности, основываясь исключительно на собственных («внутренних») представлениях о ценности q защищаемого ресурса *I*, успешная реализация угрозы атакующей стороной А оказывается практически гарантированной.

Выводы. В статье рассмотрен подход к определению предельного объема инвестиций в систему защиты информации (СЗИ), лишенный недостатков, присущих подходу Гордона-Лоеба, обусловленных применением субъективного формально-аппроксимативного способа формирования модели защищенности информационных ресурсов.

Предложен способ оценивания предельного объема инвестиций в безопасность информации, основанный на анализе модели информационных рисков, структура и параметры которой базируются на использовании сведений о реальных механизмах развития и реализации информационных угроз и рисков, в том числе на моделях экономико-стоимостных, мотивационных и экономико-ресурсных отношений, характерных для ситуации «атака-защита» в информационной сфере.

По результатам анализа предложенной экономико-стоимостной модели информационных рисков оценен максимальный объем инвестиций в СЗИ, равный 25% стоимости защищаемого информационного ресурса.

ЛИТЕРАТУРА

[1]. Лукацкий А. В. Процент безопасности [Электронный ресурс]. – 2013. – Режим доступа: http://www.it-world.ru/safety/58323.html

[2]. Петренко С. А Управление информационными рисками / С. А. Петренко, С. В. Симонов. – М.: Компания АйТи, ДМК Пресс, 2004. – 384 с.

[3]. Gordon L.A., Loeb M.P. The Economics of Information Security Investment // ACM Transaction on Information and System Security – 2002. – Vol.5. – No4. – pp. 438-457.

[4]. Hausken K. Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability // Information Systems Frontiers. – 2006. – No. 5(8). – pp. 338-349.

[5]. Willemson J. On the Gordon & Loeb Model for Information Security Investment // Proceedings of The Fifth Workshop on the Economics of Information Security (WEIS 2006), 2006. pp.101-112

[6]. Willemson J. Extending the Gordon&Loeb Model for Information Security Investment // Fifth International Conference on Availability, Reliability, and Security (ARES 2010), 2010. pp 258-261.

[7]. Gordon, L.A., and Loeb, M.P. and Lucyshyn, W. and 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, 2015, vol. 6, pp.24-30

[8]. Архипов А.Е. Применения мотивационно-стоимостных моделей для описания вероятностных соотношений в системе «атака-защита»/ А.Е. Архипов, С.А. Архипова //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – 2008. – вип. 1(16). – С. 57-61.

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

[10]. Архипов О.Є. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О.Є. Архипов, А.В. Скиба // Захист інформації. – 2013. – Том15, №4. – С.366-375.

[11]. Архипов А.Е. Применение затратно-стоимостных моделей для оценивания вероятностных параметров информационных рисков / А.Е.Архипов, С.А.Архипова, А.В. Скиба // Інформаційна безпека. – 2013. – №2(10). – С.11-18.

[12]. Архипов О. Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою: моногр. / О.Є. Архипов, О.Є. Муратов. – К: Наук.-вид. відділ НА СБ України, 2011. – 195 с.

REFERENCES

[1]. Lukackij, A. V. (2014), “Percentage of security” available at: http://www.it-world.ru/ safety/ 58323. html. (Accessed 10.08.2014). 2.

[2]. Petrenko S. A. Information Risk Management / S.A. Petrenko, S.V. Simonov, M.: IT Co., DMK Press, 2004, 384 p.
[3]. Gordon, L.A. and Loeb, M.P. (2002), "The Economics of Information Security Investment", ACM Transaction on Information and System Security, vol. 5, no. 4. pp. 438-457.
[4]. Hausken, K. (2006), "Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability", Information Systems Frontiers, vol. 5(8), pp 338-349.
[5]. Willemson, J. (2006) "On the Gordon & Loeb Model for Information Security Investment", The Fifth Workshop on the Economics of Information Security (WEIS 2006), Cambridge, UK, pp. 101-112.
[6]. Willemson, J. (2010) "Extending the Gordon&Loeb Model for Information Security Investment", Fifth International Conference on Availability, Reliability, and Security (ARES 2010), Krakov, pp 258-261.
[7]. Gordon, L.A., and Loeb, M.P. and Lucyshyn, W. and Zhou, L. (2015) "Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model," Journal of Information Security, vol 6, pp. 24-30.
[8]. Arkhypov, A. Ye. and Arhipova, S.A. (2008) "Application of motivational-cost models to describe the probabilistic relationships in the attack-defense system", Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini, vol. 1(16), pp.57-61.
[9]. Arkhypov, A. Ye. (2011) "Application of economic and motivational relations for estimating the probability parameters of information risks", Zakhyst informatsii, vol. 2(51), pp.69-76.
[10]. Arkhypov, A. Ye. and Skyba, A.V. (2013), "Information risks: methods and techniques of research, risk models and methods for their identification", Zakhyst informatsii, vol. 15(4), pp.366-375.
[11]. Arkhypov, A. Ye. and Arhipova, S.A. and Skyba, A.V. (2013), "Use of cost-cost models to estimate the probability parameters of information risks", Information security, vol. 2(10), pp.1-18.
[12]. Arkhypov, A. Ye. Criteria for possible damage to the national security of Ukraine in case of disclosure of information protected by the state, monogram. / A. Ye. Arkhypov, A. Ye. Muratov., K: Research and Publishing Department of NA S S U, 2011., 195 p.

ЗАСТОСУВАННЯ ЕКОНОМІКО-ВАРТІСНИХ МОДЕЛЕЙ ІНФОРМАЦІЙНИХ РИЗИКІВ ДЛЯ ОЦІНЮВАННЯ ГРАНИЧНОГО ОБСЯГУ ІНВЕСТИЦІЙ В БЕЗПЕКУ ІНФОРМАЦІЇ

Розглядається проблема визначення максимального розміру інвестицій в систему захисту інформації. Здійснено аналіз публікацій, що містять матеріали, пов'язані з дослідженням та розвитком підходу Гордона-Лоеба, в якому обґрунтовується граничний обсяг інвестицій у безпеку інформації. Показано, що даний підхід не дозволяє отримати однозначну відповідь: суб'єктивний формально-апроксимативних спосіб завдання моделі, на якій базується одержуване рішення, породжує множинність можливих моделей і, як наслідок, - множинність рішень. Запропоновано підхід до вирішення завдання визначення обсягу інвестицій в систему захисту інформації, заснований на дослідженні моделі інформаційних ризиків. Формування її структури і параметрів базується на використанні відомостей про реальні механізми розвитку та реалізації інформаційних загроз, зокрема, на економіко-вартісній моделі, що використовується для оцінювання ймовірності успішної реалізації атак вразливостей інформаційної системи. За результатами дослідження отримана оцінка максимального обсягу інвестицій в систему захисту інформації, яка дорівнює 25% вартості інформаційного ресурсу,який підлягає захисту (або втрат, зумовлених реалізацією загрози щодо цього ресурсу). Відзначено, що при застосуванні в системі захисту інформації високоефективних рішень рівень інвестування може бути зменшений до 11-13%. Розглянуто перспективи застосування в дослідженнях моделей, які ґрунтуються на мотиваційних та ресурсних відносинах, характерних для ситуації «атака-захист» в інформаційній сфері.

Ключові слова: ризик, моделювання ризиків, економіко-вартісні моделі, діапазон розумних инвестиции.

APPLICATION OF ECONOMIC-COST MODEL OF INFORMATION RISKS FOR EVALUATION LIMITEB VOLUME OF INVESTMENT IN INFORMATION SECURITY

The article analyzes the problem of determination of the maximum amount of investment in information security. It is studied the approach of Gordon-Loeb, which justified the limit investment in information security. It is analyzed the publications containing materials related to the exposure and the development of this approach. It is shown that this approach does not ensure univocal answer. The reason for this is a subjective formal-approximation way of defining of a model, which is basis for the solution. This way gives multiplicity of possible models and, as the resulting, multiplicity of solutions. It is offered an approach to solving the problem of determining the amount of investment in the system of protection of information, which is based on study of the model of information risks. Formation of its structure and parameters are based on the use of information about the actual mechanisms of the development and implementation of information threats. It is applied economic-cost model, which is used to estimate the probability of successful implementation of the attack of information system vulnerability. The paper proposes the estimation of the maximum amount of investment in information security. This investment amounts to 25% of the value of the protected information resource (or losses aris-

ing from the implementation of the threat to this resource). It is noted that the in the case of application of high-performance technology/decisions in the system of information security level of investment may be reduced to 11-13%. It is considered the prospects of application of models based on motivational and resource relations which are characteristic to of the situation "attack-defense" in the information sphere.

Index terms: risk, risk modeling, economic and cost models, the range of reasonable investment.

Архипов Александр Евгеньевич, доктор технических наук, професор кафедры информационной безопасности НТУУ «КПИ».
E-mail: sonet0515@gmail.com.
Архипов Олександр Євгенович, доктор технічних наук, професор кафедри інформаційної безпеки НТУУ «КПІ».
Oleksandr Arkhipov, Dr. Sci. Tech., Professor at the Department of Information Defence at National University of Ukraine «Kyiv Polytechnic Institute».

УДК 004.056.5

МЕТОДОЛОГІЯ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ. ПОРІВНЯЛЬНИЙ АНАЛІЗ ОСНОВНИХ ТЕРМІНІВ ТА ВИЗНАЧЕНЬ

Олександр Юдін, Сергій Бучик

У статті здійснено порівняльний аналіз основних термінів та визначень згідно керівних документів з питань захисту інформаційних ресурсів та введених авторами в попередніх дослідженнях. До таких термінів та визначень авторами віднесено та розглядаються в статті: державні інформаційні ресурси, загроза державним інформаційним ресурсам, національні інформаційні ресурси, національні електронні інформаційні ресурси, система національних інформаційних ресурсів, система державних інформаційних ресурсів, державні електронні інформаційні ресурси, реєстр електронних державних інформаційних ресурсів, депозитарій електронних державних інформаційних ресурсів, атака на державні інформаційні ресурси, метод подвійної трійки захисту, загрози нормативно-правового спрямування, загрози організаційного спрямування, загрози інженерно-технічного спрямування, ідентифікатор об'єкта. Запропоновано ці терміни та визначення покласти в основу стандарту або нормативного документу технічного захисту інформації щодо термінології в галузі захисту державних інформаційних ресурсів.

***Ключові слова**: державні інформаційні ресурси, загроза державним інформаційним ресурсам, національні інформаційні ресурси, національні електронні інформаційні ресурси, система національних інформаційних ресурсів, система державних інформаційних ресурсів, державні електронні інформаційні ресурси, реєстр електронних державних інформаційних ресурсів, депозитарій електронних державних інформаційних ресурсів, атака на державні інформаційні ресурси, метод подвійної трійки захисту, загрози нормативно-правового спрямування, загрози організаційного спрямування, загрози інженерно-технічного спрямування, ідентифікатор об'єкта.*

Актуальність дослідження. Актуальність статті обумовлюється вимогами сьогодення, а саме необхідністю забезпечення інформаційної безпеки, кібербезпеки та безпеки інформаційних ресурсів держави в цілому. Як зазначено в Указі Президента України №287/2015 Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», одним із пріоритетів забезпечення інформаційної безпеки є «створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; розробка і реалізація скоординованої інформаційної політики органів державної влади». Що стосується основних пріоритетних напрямків забезпечення кібербезпеки і безпеки інформаційних ресурсів, то до них відповідно тематики статті можна віднести забезпечення захисту «державних інформаційних ресурсів, систем електронного врядування … з урахуванням практики держав – членів НАТО та ЄС».

Аналіз останніх досліджень та публікацій. Авторами визначалось, що з одного боку в Україні на концептуальному та нормативному рівні не визначено перелік і класифікацію загроз інформаційним ресурсам держави, з іншого боку не розроблено нормативно-правового документу та стандарту щодо поняття державних інформаційних ресурсів, його складових та відповідної їм моделі загроз [1, 2]. Також в роботах [1, 2, 3, 4, 5] авторами введено або уточнено ряд понять, які відносяться до методології захисту ДІР. Таким чином виникає необхідність узагальнення всієї термінології, яка введена або уточнена авторами в попере-