Korchenko Oleksandr, Dr Eng (Information security), professor, laureate of the State Prize of Ukraine in Science and Technology, Head of IT-Security Academic Department, National Aviation University, Visit-Professor at The University of Bielsko-Biala (Akademia Techniczno-Humanistyczna, Bielsko-Biała, Poland), Leading Researcher of the National Academy of SS of Ukraine.

Казмирчук Светлана Владимировна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: sv.kazmirchuk@gmail.com
Казмірчук Світлана Володимирівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Kazmirchuk Svitlana, PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University.

Иванченко Евгения Викторовна, кандидат технических наук, доцент, профессор кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: evivancenko@gmail.com
Іванченко Євгенія Вікторівна, кандидат технічних наук, доцент, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
Ivanchenko Eugenia, PhD in Eng., Professor of IT-Security Academic Department, National Aviation University.

DOI: 10.18372/2410-7840.19.11899
УДК 004.056.53

ПРИМЕНЕНИЕ РЕФЛЕКСИВНЫХ МОДЕЛЕЙ РИСКОВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В КИБЕРПРОСТРАНСТВЕ

Александр Архипов

Рассматриваются возможности и границы применения риск-ориентированного подхода (РОП) к построению и исследованию системы защиты информации организации (СЗИ). Введены четыре вербальных спецификации злоумышленника, описывающие различные аспекты его поведения и подготовки, социально-психологический контекст его действий, целевые установки этих действий, влияющие на выбор стратегии злоумышленника, методы и способы реализации информационных угроз. Соответственно введенным спецификациям сформированы рефлексивные модели рисков. Это математические модели, структура и параметры которых отражают (лат. reflexus) особенности злоумышленника, содержащиеся в его спецификации. Выполнено исследование рефлексивных моделей, которое в ряде случаев позволило определить предельные объёмы инвестиций в СЗИ, а также ограничения в применении РОП к построению СЗИ.
Ключевые слова: *риск, моделирование рисков, рефлексивные модели рисков, предельные объёмы инвестиций в СЗИ, риск-ориентированный подход.*

В основе большинства наиболее часто и успешно применяемых международных и отраслевых стандартов для систем менеджмента безопасности информации (СМБИ): ISO 27001, ISO 27005, СТО БР ИББС, NIST SP 800-30, COSO ERM-Integrated Framework и т.д., лежит риск-ориентированный подход (РОП), обеспечивающий получение определенных преимуществ в построении и эксплуатации СМБИ.

В частности, в отличие от директивного подхода к построению систем защиты информации (СЗИ), базирующегося на использовании рекомендованного перечня возможных угроз в отношении доступности, целостности и конфиденциальности информации, как правило в полном объёме привлекаемого для формирования системы услуг безопасности при построении СЗИ, РОП позволяет из огромного количества существующих угроз и уязвимостей информационных систем (ИС) выделить те, которые действительно актуальны для защиты информации в данной конкретной организации, что создает объективные предпосылки минимизации инвестиций в безопасность информации. Детальный анализ механизмов реализации выделенного ограниченного круга актуальных угроз дает возможность наилучшим образом выбрать методы и средства защиты,

реально соответствующие уровню гарантий защиты. Это позволяет сформировать объективные планы и оценить инвестиционные бюджеты на создание СЗИ и СМБИ. Найденные объемы инвестиций анализируется с точки зрения эффективности СЗИ, сопоставляются с общим бюджетом организации и т.п. По результатам анализа может осуществляется пересмотр первоначально введенных уровней гарантий защиты, внесение в них корректировок, повторное планирование и бюджетирование СЗИ, т.е. процедура анализа принимает итеративный характер.

Процедура выделения группы актуальных для защиты информации угроз, являющаяся завершающей стадией процесса оценивании рисков, получила название приоритизации [1] рисков, обусловленных реализациями возможных информационных угроз $t_i, i=\overline{1,n}$. Приоритизация предполагает определение для этих угроз частных рисков

$$r_i = p_{ti} q_i, \qquad (1)$$

где p_{ti} – количественная оценка вероятности реализации соответствующей информационной угрозы, а q_i – оценка потерь, причиненных этой угрозой, ранжирование рисков в полученной совокупности $\{r_i\}$ по убыванию своих значений и выделение из ранжированного ряда его левого фрагмента, содержащего существенные для организации риски. Угрозы, порождающие эти риски, и образуют группу искомых актуальных угроз. На базе группы существенных рисков (т.е. рисков актуальных угроз) формируется значение интегрального (обобщенного) риска $R = P_T Q$, характеризующего в общем возможные потери Q организации, являющиеся результатом совокупного действия всех анализируемых актуальных информационных угроз, P_T - вероятность возникновения этих потерь. Интегральный риск является универсальным показателем степени защищенности информации, позволяющим объективно оценивать уровень исходных угроз для информации, обрабатываемой в ИС организации, уровень остаточных угроз (после построения СЗИ), эффективность функционирования СЗИ. Для анализа эффективности СЗИ применяется показатель вида

$$E = (R_1 - R_T)/c = \Delta_R / c, \qquad (2)$$

где R_1 – исходное значение интегрального риска, характеризующее возможные потери организации из-за реализации актуальных информационных угроз в случае отсутствия СЗИ, R_T – остаточное значение интегрального риска организации, оценивающее возможные потери уже после ввода в действие СЗИ, Δ_R – величина возможных потерь, которые удалось предотвратить благодаря созданию в организации СЗИ.

Поскольку результаты оценивания рисков влияют на объем средств, инвестируемых в СЗИ, формирование понятного и прозрачного процесса анализа информационных рисков является важнейшим условием успешного функционирования СМБИ организации. Этим же объясняются жесткие требования к объективности и точности рассчитываемых оценок рисков.

К сожалению, практическое применение РОП для защиты от киберугроз сопряжено с рядом трудностей. Процедура нахождение интегрального риска в ряде случаев может оказаться достаточно простой. Например, при условии независимости и несовместности актуальных угроз и независимости наступивших в результате их реализации последствий, интегральному риску соответствует суммарный риск $R = \sum_{i=1}^{n} r_i$. Однако для организаций с достаточно сложной структурой, располагающих значительным объемом информационных ресурсов (ИР), интенсивно использующим в своей работе комплексные информационные технологии, вычисление интегрального риска в условиях возможного воздействия нескольких угроз, допускающих совместную реализацию с проявлением взаимосвязанных, взаимозависимых последствий, представляет нетривиальную задачу [2, 3]. Применение в подобных условиях суммарного риска в качестве оценки интегрального риска обычно дает существенно завышенное оценочное значение, способствуя необоснованному увеличению объема инвестиций в построение СЗИ. Кроме того, в формуле (1) при расчете частных рисков в качестве значений p_{ti}, q_i используются, как правило, экспертные оценки, что вносит в расчетные значения субъективные погрешности, снижающие надежность результатов последующего анализа. Еще одним негативным аспектом описанного выше процесса оценивания рисков является его длительность и трудоемкость, обуславливаемые, в частности, итеративным характером выбора структуры и комплектации СЗИ (с

учетом необходимости применения на каждой итерации показателя интегрального риска, не имеющего, как было отмечено выше, общей формализованной процедуры вычисления).

Недостатки описанного выше процесса оценивания рисков, получившего название детального оценивания рисков, стимулировали попытки применения более глобализированного подхода к рассмотрению информационных рисков организации, при котором технологическим аспектам оценивания рисков организации, в частности, детальному анализу угроз и уязвимостей ИС уделяется незначительное внимание, основной акцент сосредотачивается на обобщенных сценариях риска, степени зависимости бизнеса организации от состояния ее информационных активов, в частности, от общего уровня инвестиций организации в СЗИ. В стандартах [4, 5] этот подход, называемый оцениванием рисков высокого уровня, ориентирован в первую очередь на решение общестратегических аспектов обеспечение безопасности информации: организационных, экономических, а также базовых технических вопросов. В случае необходимости для обеспечения безопасности особо ценных активов дополнительно проводится процедура детального оценивания рисков, носящая в этом случае не итеративный характер и не требующая последующего вычисления интегрального риска через совокупность существенных частных рисков. Такой подход к анализу рисков получил название комбинированного [4]. Он гарантирует получения полного и технологически завершенного решения задачи построения СЗИ организации после проведения оценивания рисков высокого уровня.

Заметим, что цели и методы применения РОП для анализа и оценивания информационной безопасности организации однозначно не определены, многое зависит от свойств и особенностей самой организации. Интерес представляет обобщение известных практических результатов применения РОП для решения задач защиты информации, формализация процедур, в которых РОП является базовой методологией, оценивание перспектив РОП для защиты организаций от современных кибератак.

Применения РОП в процедуре оценивания рисков высокого уровня. Применим РОП для оценивания безопасности информации в организации с достаточно сложной территориально распределенной структурой, использующей для обмена данными Интернет, располагающей значительным распределенным информационным ресурсом I, массово и интенсивно применяющей в своей деятельности информационные технологии.

Предварительный анализ возможных угроз в отношении информационных ресурсов этой организации, выполненный с использованием приводимого в стандарте ИСО/ИЕК 27005 перечня угроз [5, Приложение С. Примеры типичных угроз] позволяет утверждать следующее:

1) из представленных в перечне 77 угроз лишь относительно пяти, связанных с воздействием явлений естественного характера (климатических, сейсмических, вулканических, метеорологических и наводнения), и еще четырех угроз случайного характера (отказы и сбои оборудования, сбои и ошибки программного обеспечения) можно сразу предположить возможность принятия эффективных решений по минимизации обусловленных ими рисков;

2) оставшиеся 69 угроз представляют собой реализации преднамеренных злоумышленных акций, нацеленных на информационные активы.

Последнее утверждение о преднамеренности и злоумышленности предпринимаемых действий говорит о том, источником угроз является человек – злоумышленник (нарушитель) или группа злоумышленников. С другой стороны, одна и та же угроза может быть реализована разными механизмами атак, базирующихся на использовании различных уязвимостей ИС организации, при этом степень успешности атаки (т.е. вероятностный параметр риска) и уровень возможных потерь организации напрямую зависят от потенциала атакующей стороны – компетентности, ресурсов и мотивации злоумышленника [6].

Очевидно, что применение в этой ситуации детального оценивания рисков потребует проведения продолжительной и кропотливой работы по исследованию уязвимостей и перебору реализуемых на их базе механизмов атак, выяснению массы недостающих сведений для вычисления частных рисков отдельных атак, «сворачиванию» их в риски угроз и т.д. в соответствии с изложенной выше процедурой детального оценивания. Ее промежуточным результатом будет вычисление значения R_1, пары значений R_T, Δ_R для предлагаемого варианта СЗИ, оценивание эффективности этого варианта СЗИ, внесения в него корректив и

изменений (в режиме возможной многоразовой итерации) и в конечном итоге определение приемлемой (в соответствии с принятой системой критериев) величины инвестиций c в СЗИ организации.

Принимая во внимание крайне высокие трудозатраты этой процедуры, актуальной является возможность решения поставленной задачи через оценивание рисков высокого уровня, исключая применение итеративной процедуры и не прибегая к предварительному вычислению частных рисков. Следует отметить, что подобные решения фактически были уже получены в работах [3, 7, 8], хотя постановка задачи там была несколько иной. В связи с этим в излагаемых ниже материалах ряд результатов будет приведен без выводов, лишь с ссылками на работы, их содержащие.

Используем для описания интегрального риска так называемую двухфакторную формулу:

$$R = P_T Q, \qquad (3)$$

где вероятность P_T возникновения потерь Q представлена произведением

$$P_T = P_t P_v, \qquad (4)$$

где P_t – вероятность мотивации злоумышленника (возникновения у него интереса к информационному ресурсу I организации, побуждающее к совершению каких-либо атакующих действий относительно этого ресурса), P_v – вероятность удачного использования злоумышленником для реализации своих атакующих действий уязвимостей ИС организации. Структуризация вероятности P_T удобна тем, что вероятность мотивации P_t фактически определяется только уровнем интереса атакующей стороны к информационному ресурсу организации, что делает целесообразным нахождение этой вероятности в виде отдельной экспертной оценки. Один из способов получения этой оценки – применение эвристической зависимости

$$P_t(g, D) = \frac{g - D}{g} = 1 - \frac{D}{g}, \qquad (5)$$

где g – ценность ресурса I для злоумышленника (атакующей стороны), D – обобщенные затраты на подготовку и реализацию атакующих действий злоумышленником, приведенные к денежной форме представления, $g - D$ – чистая прибыль злоумышленника в случае успешной реализации атаки. Очевидно, что чем больше g, тем ближе к 1 вероятность P_t. С уменьшением g, в случае $g \le D$ проведение атаки теряет смысл, если только интересы атакующего не выходят за рамки коммерческой выгоды. Следует также отметить, две особенности, важные для практического применения формулы (5):

1) параметры, входящие в выражение (5), определяются только интересами и мотивами поведения злоумышленника;

2) восприятие ценности одного и того же информационного ресурса I атакующей и защищающейся стороной в общем случае разное – «асимметричное» [3, 7]. Например, для владельца ресурса 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 ценность g «добытой» информации формируется на основе рыночной стоимости ресурса и количества потенциальных покупателей, желающих заполучить его в свою собственность, в итоге $g \ne q$.

Вероятность успешно атаки P_v определяется соотношением потенциалов атакующей и защищающейся сторон и может быть представлена эвристическим соотношением вида:

$$P_v(q, c, D) = \frac{\mu q}{\mu q + s\frac{c^2}{D}}, \qquad (6)$$

где c – общий объем инвестиций в СЗИ организации, $\mu = g / q$ – коэффициент асимметрии восприятии ценности информации сторонами атаки и защиты, 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. Величина коэффициента s зависит от отношения организации к вопросам безопасности информации и определяется уровнем зрелости организации в сфере менеджмента безопасности информации. Получить количественную (балльную) оценку уровня зрелости можно, применив изложенную в [1] методику самостоятельного оценивания уровня зрелости системы управления рисками в организации. Найденную по этой методике бальную оценку следует использовать в качестве искомого значения s. Максимально возможному значению s соответствует 85

баллов, высокий уровень зрелости организации характеризуется диапазоном 51 - 85 баллов.

Очевидно, что если информационный ресурс $\boldsymbol{I}$ не интересен для злоумышленника, то в этой ситуации $g \to 0$, коэффициент $\mu \to 0$ и вероятность успешной атаки $P_v \to 0$. Если наоборот, ресурс $\boldsymbol{I}$ не представляет ценности для организации-владельца, то инвестиции в СЗИ практически отсутствуют, т.е. $c = 0$, тогда $P_v = 1$. Наконец, если атакующая сторона проявляет к ресурсу $\boldsymbol{I}$ чрезвычайно высокий интерес и готова пойти для его получения на практически неограниченные затраты, в этом случае $D \to \infty$, $P_v = 1$.

Подстановка выражений (5), (6) в формулу (3) дает возможность построить формализованную обобщенную модель интегрального риска

$$R(c) = (1 - \frac{D}{g}) \frac{\mu q}{\mu q + s\frac{c^2}{D}} q, \qquad (7)$$

в которую величина c входит как один из параметров, а затем сформировать в общем виде зависимость предотвращенных потерь $\Delta_R(c)$ от уровня инвестиций c в СЗИ организации.

Для проведения исследований в рамках анализа рисков высокого уровня определим понятие эффективности СЗИ организации. Будем полагать, что обязательным для эффективной СЗИ является выполнение условия $\Delta_R(c) > c$. Тогда наиболее эффективной будем считать СЗИ, для которой разность $\Delta_R(c) - c = \Delta_c(c)$, представляющая «чистую прибыль», обусловленную построением СЗИ, кажется наибольшей. Эффективный объем инвестиций в этом случае составит [3, 7]:

$$c_{eff} = \arg\max_{c \in C} \Delta_c(c), \qquad (8)$$

где C – множество значений c, для которых $\Delta_R(c) > c$. К сожалению, использование обобщенной модели интегрального риска (8) не позволяет найти c_{eff} в явном виде в аналитической форме представления. Однако в ряде случаев, применяя более детальное описание возможностей и свойств атакующей стороны, мотивационно-экономических аспектов ее поведения, оказывается реальным получение аналитического решения оптимизационной задачи (8) и ряда дополняющих это решение сведений.

Рефлексивные модели рисков. Ниже будет рассмотрено четыре вербальных спецификации злоумышленника, отражающие различные аспекты поведения и подготовки атакующей стороны, социально-психологический контекст ее действий, существующие (часто директивно определяемые) целевые установки этих действий, во многом влияющие на выбор стратегии атаки, методы и способы реализации информационных угроз. Соответственно введенным спецификациям формируются рефлексивные (от лат. reflexus – отображение, отражение) модели рисков, каждой из которых присущи определенные особенности, зависящие от характеристик злоумышленника, содержащихся в его спецификации.

Спецификация 1 – скрипт кидди (script kiddie, newbies).

Атакующая сторона – неопытный одиночка/группа, не имеющий достаточной подготовки и знаний для написания эксплойта или сложной программы, использующий для атаки информационных систем и сетей скрипты или программы, разработанные другими, не понимающий механизма их действия, не способный к самостоятельной реализации эффективных атакующих решений, с достаточно скромными ресурсными возможностями (в частности финансовыми). Цель действий скрипт кидди – попытка произвести впечатление на друзей или получить похвалу от сообществ компьютерных энтузиастов.

Приведенную выше характеристику из Википедии можно дополнить еще одной цитатой [9]: «скрипт кидди … обычно не волнуют финансовые или политические соображения, они больше стремятся прославиться или «вызвать нарушение сервиса и породить хаос из спортивного интереса»».

По оценке А.В. Лукацкого [10], скрипт кидди составляют до 95% от общего числа злоумышленников, атакующих информационные и компьютерные системы, т.е. это наиболее распространенный тип нарушителя, необходимость защиты от которого является первоочередной задачей, решаемой при построении СЗИ. В частности, следует отметить, что реализуемые скрипт кидди «старые» угрозы (термин заимствован в [11] и подчеркивает несостоятельность скрипт кидди в плане разработки, подготовки и реализации новых оригинальных атакующих действий) могут нанести весьма значительный ущерб организации, если

она не уделяет должного внимания защите своей информации. Кроме того, необходимо учитывать, что сообщество скрипт кидди неоднородно, и те из них, кто получил неплохое базовое образование и научился учиться, составляют резерв для более продвинутых киберпреступников.

В целом будем полагать, что относительно скрипт кидди справедливо следующее итоговое заключении:

– атакующая активность скрипт кидди не носит целенаправленный характер, объектами их атак оказываются случайные компьютеры, в руки атакующего попадает разнородная случайная информация (хотя иногда и очень ценная). В связи с этим формула (5) неактуальна для скрипт кидди, его мотивация крайне неустойчива и носит спонтанный характер;

– скрипт кидди не в состоянии самостоятельно разрабатывать средства и новые механизмы атак, более того, не понимают механизма действия старых, основывая свои действия главным образом на применении переборного принципа в реализации угроз. Поэтому грамотно воплощенный в СЗИ организации базовый уровень защищенности, ориентированный на применение средств и способов защиты от уже известных «старых» угроз, достаточно эффективен для противодействия атакам скрипт кидди.

Этому заключению соответствует рефлексивная модель риска вида:

$$R(c) = P_t \frac{q}{q - sc} q\,, \qquad (9)$$

где вероятность удачного использования злоумышленником для реализации своих атакующих действий уязвимостей ИС организации определяется формулой

$$P_v = \frac{q}{q - sc}\,. \qquad (10)$$

Из (10) следует, что безопасность информации в организации в первую очередь зависит от внутренних параметров: суммы инвестиций c в СЗИ, уровня зрелости организации (определяется значением параметра s) и ценности q ее информационного ресурса. Рост значений параметров c и s ведет к падению значений вероятности (10).

Рассчитав для рефлексивной модели риска (9) величину предотвращенных потерь $\Delta_R(c)$ и, сопоставив ее с объемом c инвестиций в СЗИ, найдем «чистую прибыль» организации, обусловленную построением СЗИ:

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

Анализ выражения (11) позволяет определить [7] диапазон «разумных» инвестиций $0 \le c \le q(s-1)/s$, в пределах которого $\Delta_R(c) > c$, формулу для вычисления эффективного объема инвестиций

$$c_{eff} = \frac{q}{s}(\sqrt{P_t s} - 1), \qquad (12)$$

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

$$P_v(c_{eff}) = \frac{1}{\sqrt{P_t s}},$$

$$R_T(c_{eff}) = P_v(c_{eff}) P_t q = q\sqrt{\frac{P_t}{s}}\,. \qquad (13)$$

В пределах диапазона «разумных» инвестиций зависимость значений эффективного объема инвестиций c_{eff} от параметра s носит одноэкстремальный характер с максимумом, равным [3, 7] $\max[c_{eff}(s)] = 0{,}25 q P_t$. Очевидно, что наибольшей величина эффективных инвестиций в СЗИ окажется при P_t=1, при этом максимальный объем инвестиций в СЗИ составит $c_{eff\,\max} = 0{,}25q$, т.е. 25% стоимости ресурса q, который является объектом защиты, а для высокоэффективных защитных решений (например, $s = 60$) в соответствии с формулой (12) даже при P_t=1 объем инвестиций в СЗИ может оказаться на уровне 11-13% от стоимости защищаемого ресурса. Полученные результаты хорошо согласуется с эмпирическими оценками объема инвестиций, приведенными в ряде публикаций [12, 13], авторы которых акцентируют внимание на сумме в 15-20 % от стоимости активов ИС.

Следует отметить, что «под крышу» скрипт кидди – спонтанно действующий некреативный злоумышленник, воспроизводящий «старые» атаки - можно также подвести различные сетевые инфекции и черви, которые в основной своей массе, исключая разработки нулевого дня, успешно отсеиваются на базовом уровне защиты.

Спецификация 2 – злоумышленник-профессионал.

Атакующую сторону представляет профессионал или группа профессионалов, обладающая необходимыми знаниями, навыками и достаточным опытом, для которой хакинг – основная деятельность откровенно коммерческого характера. Злоумышленник-профессионал обычно располагает определенными финансово-экономическими ресурсами, но для него, тем не менее, сохраняет достаточную актуальность ограничение $D \le g$. Если стороны атаки и защиты примерно одинаково оценивают стоимость информационного ресурса $\boldsymbol{I}$, т.е. μ=1, рефлексивная модель риска для этого случая имеет вид:

$$R(c) = (1 - \frac{D}{g}) \frac{q}{q + s\frac{c^2}{D}} q . \qquad (14)$$

Исследование соотношения (14) для $D = 0$ позволяет оценить граничные значения диапазона разумных инвестиций [3, 7]: $0 \le c \le q$. С увеличением значений D, при $D \to 0{,}25sqP_t^2$, правая и левая границы диапазона сближаются, стягиваясь в точку $c = \frac{qP_t}{2}$ для $D = 0{,}25sqP_t^2$. В этом предельном случае наибольшая величина инвестиций в СЗИ составит $c_{eff\max} = 0{,}5q$, т.е. 50% стоимости ресурса q [3, 7]. Расходование этого объема инвестиций требует проведения анализа возможных угроз безопасности информации, выделения актуальных угроз с последующей реализацией системы защитных мероприятий в форме комплексной системы защиты информации (КСЗИ) в условиях оптимального распределения выделенных инвестиций.

Как уже отмечалось выше, атакующая сторона может вложить в организацию и проведение атаки значительные средства, сопоставимые по величине со значением q, но, как правило, выделяемый атакующий потенциал не превышает пределов экономической целесообразности. Однако в случае $\mu >> 1$, т.е. при существенной асимметрии восприятии ценности информации сторонами атаки и защиты, возникает ситуация, которую можно определить как долговременная (продолжительная) целевая атака. При этом атакующая сторона, предварительно уже выделившая на свои действия изрядные ресурсы для подготовки атаки, но еще не достигшая успеха, переходит к выжидательной тактике, сопровождаемой ведением постоянного контроля за качеством функционирования СЗИ атакуемой организации. Рано или поздно, при возникновении локального снижения уровня ее защищенности (появление даже кратковременной уязвимости), атакующая сторона проводит успешную атаку. Основным расходуемым ресурсом злоумышленника в этом случае является его время плюс затраты на осуществление мониторинга состояния защищенности объекта атаки.

С формальной точки зрения, если $\mu \ne 1$, то при $g \to \infty$ вероятность активации угрозы $P_t \to 1$, т.е. угроза существует постоянно и ее реализация произойдет как только представится удобный момент. При наличии инсайдера в атакуемой организации именно он может сообщить о наступлении этого момента, в частности, постараться создать его. Этому моменту будет соответствовать локальный всплеск вероятности P_v, которая, согласно введенному в [3] определению, представляет собой «терминальную» вероятность, величина которой изменяется во времени в соответствии с избранной тактикой атак. В свою очередь, правильный выбор стратегии защищающейся стороной, так называемая проактивная защита, основывающаяся на упреждающих защитных действиях, опирающихся на изучение поведения, тактики и стратегии атакующей стороны, т.е. использующая подходы и принципы рефлексивного управления [14, 15] – позволяет отсрочить наступление момента успешной реализации угрозы теоретически на неограниченно долгий период времени.

Таким образом, КСЗИ, построенная только в соответствии с требованиями действующих нормативных документов системы НД ТЗИ, не обеспечивает достаточных гарантий защиты от атак, реализуемых сегодня в киберпространстве – направленных целевых атак APT (Advanced Persistent Threat), динамических техник обхода AETs (Advanced Evasion Techniques), против которых применяемые сегодня комплексы защитных мероприятий малоэффективны. Перспективным может оказаться разработка проактивных систем защиты, использующих подходы и принципы рефлексивного управления.

Спецификация 3 – профессионал-исполнитель.

Атакующая сторона для достижения своих целей прибегает к услугам наемного исполнителя, обязанного при любых обстоятельствах выполнять свое работу. В частности, если его задание - реализации какой-либо угрозы информации, то профессионал-исполнитель сразу приступает непосредственно к поиску и эксплуатации уязвимости ИС организации, т.е. очевидно, что в этой ситуации $P_t = 1$. При этом в предыдущих спецификациях в ситуации атакующая сторона в своих действиях руководствуется принципом экономической целесообразности (разумной достаточности). Особенность же **Спецификации 3** состоит именно в том, что, в связи с особой важностью поставленной перед профессионалом-исполнителем задачи, ресурсные ограничения снимаются и, кроме того, он может рассчитывать на привлечение для поддержки своих действий различных дополнительных ресурсов: финансовых, технических, информационно-аналитических, оперативных и т.п. На практике это означает возможность реализации в рамках **Спецификации 3** очень высокозатратных атак ($D \to \infty$). Типичным примером подобной ситуации является выполнение особо важного задания сотрудником спецслужбы, являющимся профессионалом, подготовленным к осуществлению атакующих действий в киберпространстве [3, 7].

Рефлексивная модель риска для этого случая проста:

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

Из нее очевидно, что со снятием ресурсных ограничений ($D \to \infty$) вероятность $P_v \to 1$, т.е. успешная реализация угрозы атакующей стороной оказывается практически гарантированной и в итоге $R(c) \to q$. Это достигается за счет осуществления злоумышленником новых оригинальных атак, защиту от которых в рамках представленной в действующих руководствах по риск-менеджменту стандартной методологии РОП, базирующейся на исследовании и анализе имевших место ранее инцидентов в сфере безопасности, предусмотреть практически невозможно.

Спецификация 4 – хактивист.

Атакующая сторона – идейный хакер («киберактивист»), стремящийся перенести в киберпространство продвижения политических либо социальный идей (нередко достаточно сомнительного характера), организующий акции гражданского «электронного» неповиновения в киберпространстве, старающийся привлечь внимание власти и общественности (иногда в довольно жесткой форме) к тем или иным вопросам и проблемам современного общества путем синтеза социальной активности и хакерства. Наиболее характерными для хактивистов акциями являются виртуальные «сидячие забастовки» и блокады, бомбардировка электронной почты, WEB-хакинг и компьютерные взломы, компьютерные вирусы и черви [9]. В действиях хактивиста практически отсутствует коммерческая составляющая, его атакующий потенциал, в частности, ресурсное обеспечение, обычно ограничены, поэтому **Спецификация 4** для хактивиста, в зависимости от доступных для него ресурсов, может быть близка к **Спецификации 1** или **2**. Это позволяет предполагать, особенно при установлении принадлежности хактивистов к тому или иному протестному сообществу и учитывая групповой характер акции, ее тип, продолжительность, массовость, интенсивность и возможные последствия, что применение РОП в подобных ситуациях может быть достаточно эффективным.

Выводы. Исследование рефлексивных моделей риска, отражающих для ряда типовых ситуаций «атака-защита» характерные особенности поведения и действий атакующей стороны, представленные в рамках **Спецификаций 1, 2, 4** (скрипт кидди, злоумышленник-прфессионал, хактивист), позволяет осуществить анализ рисков высокого уровня, спрогнозировать оценки граничного объема инвестиций в СЗИ организации, провести приоритизацию рисков и выделение группы актуальных информационных угроз, обеспечив тем самым эффективное распределение средств, инвестируемых в СЗИ организации.

Анализ применение риск-ориентированного подхода (РОП) к построению СЗИ организации с использованием модели рисков, определяемой в рамках **Спецификации 2** для долговременных целевых атаки, приводит к выводу о невозможности обеспечения достаточных гарантий защиты от ряда атак (в частности, направленных целевых атак APT (Advanced Persistent Threat), динамических

техник обхода AETs (Advanced Evasion Techniques), реализуемых в киберпространстве.

Учитывая, что базовая методология РОП, представленная в стандартах риск-менеджмента безопасности информации, основывается на исследовании и анализе имевших место ранее инцидентов в сфере безопасности, успешное применение РОП для построения эффективной СЗИ, позволяющей отражать новые, непрогнозируемые по имеющейся предыстории атаки, не представляется возможным. В связи с этим применения РОП для построения СЗИ от атак злоумышленников, попадающих под **Спецификацию 3**, является бесполезным.

ЛИТЕРАТУРА

[1]. Руководство по управлению рисками безопасности. Группа разработки решений Майкрософт побезопасности и соответствию, регулятивным нормам и Центр Microsoft security center of excellence, [Электронный ресурс]. Режим доступа: http://infoeto.ru/download/ rukovodstvo-po-upravleniyu-riskami-bezopasnosti.doc [Дата доступа: липень 2017].

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

[3]. О. Архипов *Вступ до теорії ризиків: інформаційні ризики. Монографія.* К.: Нац. Академія СБУ, 2015, 248 с.

[4]. *ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 3. Методи керування захистом IT. (ISO/IEC TR 13335–3).* К.: Держспоживстандарт України, 2005, 76 с.

[5]. *ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).* К.: ДП «УкрНДНЦ», 2016.

[6]. *ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель*, 2008.

[7]. А. Архипов, "Применение экономико-стоимостных моделей информационных рисков для оценивания предельных объемов инвестиций в безопасность информации", *Захист інформації*, Том 17, №3, С. 211-218, 2015.

[8]. А. Архипов, "Экономические аспекты информационной безопасности", *Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту (ISDMCI'2016, Залізний порт, 2016 р.): Матеріали міжнародної наукової конференції*, 2016, С. 23-25.

[9]. Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" *Global Problem Solving Information Technology and Tools*, 1999. [Electronic resource]. Access mode: https://nautilus.org/global-problem-solving/ activism-hacktivism -and-cyberterrorism-the-internet-as-a-tool-for-influen cing-foreign-policy-2/. [Дата доступу: липень 2017].

[10]. А. Лукацкий, *Обнаружение атак.* СПб.: БХВ, Петербург, 2003, 608 с.

[11]. В. Платонов, *Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей.* М.: «Академия», 2006, 240 с.

[12]. Г. Андрощук, П. Крайнев, *Экономическая безопасность предприятия: защита коммерческой тайны.* К.: Изд. Дом «Ин Юре», 2000, 400 с.

[13]. С. Петренко, С. Симонов, *Управление информационными рисками. Экономически оправданная безопасность*, М.: Компания Ай Ти; ДМК Пресс, 2004, 348 с.

[14]. А. Архипов, "Применение рефлексивных моделей рисков при построении систем защиты информации", *Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту (ISDMCI'2017, Залізний порт, 2017 р.): Матеріали міжнародної наукової конференції*, 2016, С. 28-29.

[15]. Д. Новиков, А. Чхартишвили, *Рефлексивные игры.* М.: СИНТЕГ, 2003, 149 с.

REFERENCES

[1]. A guide to managing security risks. Microsoft Solution Development Group for Security and Compliance, Regulatory Standards and Microsoft Security Center of excellence. [Electronic resource]. Access mode: http://infoeto.ru/ download/rukovodstvo-po-upravleniyu-riskami-bezopasnosti.doc. [Date of access: july 2017]

[2]. O. Arkhypov, O. Muratov, *Criteria for determining possible harm to the national security of Ukraine in the event of disclosure of information protected by the state. Monography,* K.: Scientific-view. Department of the Security Service of Ukraine, 2011, 195 p.

[3]. O. Arkhypov, *Entry to the theory of risks: Information risks. Monography,* K.: Nat. Acad. SSU, 2015, 248 p.

[4]. *SSTU ISO / IEC TR 13335-3: 2003 Information technology. Information Technology Security Management (IT) Guidance. Part 3. IT Protection Management Methods. (ISO / IEC TR 13335-3)*, K.: Derzhspozhyvstandart of Ukraine, 2005. 76 p.

[5]. *SSTU ISO / IEC 27005: 2015 Information technologyю Security techniquesю Information security risk management (ISO / IEC 27005: 2011, IDT)*, K.: SE "UkrNDNTS", 2016.

[6]. *GOST R ISO / IEC 15408-1-2008. Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technology. Part 1. Introduction and the general model Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technology. Part 1. Introduction and the general model*, 2008.

[7]. A. Arkhypov, "The use of economic and cost models of information risks for assessing the limits of investment in information security", *Zahist Informatsii*, vol. 17, no. 3, pp. 211-218, 2015.

[8]. A. Arkhypov, "Economic aspects of information security", *Intellectual Systems for Decision Making and Problems of Computational Intelligence (ISDMCI'2016, Zaliznyy port, 2016)*, 2016, pp. 23-25.

[9]. Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" *Global Problem Solving Information Technology and Tools*, 1999. [Electronic resource]. Access mode: https://nautilus.org/global-problem-solving/ activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2. [Date of access: july 2017].

[10]. A. Lukatsky, *Detection of attacks*, St. Petersburg: BHV Petersburg, 2003, 608 p.

[11]. V. Platonov, *Software and hardware means for ensuring information security of computing networks*, Moscow: "Academy", 2006, 240 p.

[12]. G. Androshchuk, P. Krainev, *Economic security of the enterprise: protection of trade secrets*, K.: Ed. The house "In Yure", 2000, 400 p.

[13]. S. Petrenko, S. Simonov, *Information Risk Management. Economically justified safety,* M .: Company Ai Ti; DMK Press, 2004, 348 p.

[14]. A. Arkhypov, "The use of reflexive risk models in the construction of information security systems", *Intellectual Systems for Decision Making and Problems of Computational Intelligence (ISDMCI'2017, Zaliznyi port, 2017)*, 2017, pp. 28-29.

[15]. D. Novikov, A. Chkhartishvili, *Reflective games*, Moscow: SINTEG, 2003, 149 p.

ЗАСТОСУВАННЯ РЕФЛЕКСИВНИХ МОДЕЛЕЙ РИЗИКІВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ У КІБЕРПРОСТОРІ

Розглядаються можливості і межі застосування ризик-орієнтованого підходу (РОП) до побудови та дослідження системи захисту інформації організації (СЗІ). Введено чотири вербальних специфікації зловмисника, що описують різні аспекти його поведінки і підготовки, соціально-психологічний контекст його дій, цільові установки цих дій, що впливають на вибір стратегії зловмисника, методи і способи реалізації інформаційних загроз. Відповідно введеним специфікаціям сформовані рефлексивні моделі ризиків. Це математичні моделі, структура і параметри яких відображають (лат. Reflexus) особливості зловмисника, що містяться в його специфікації. Виконано дослідження рефлексивних моделей, яке в ряді випадків дозволило визначити граничні обсягами інвестицій в СЗІ, а також обмеження в застосуванні РОП до побудови СЗІ.

Ключові слова: ризик, моделювання ризиків, рефлексивні моделі ризиків, граничні обсягами інвестицій в СЗІ, ризик-орієнтований підхід.

APPLICATION OF REFLEXIVE RISK MODELS FOR PROTECTION OF INFORMATION IN THE CYBERSPACE

The possibilities and limits of the application of the risk-oriented approach (ROA) to the construction and research of the organization's information security system (ISS) are considered. Introduced four verbal specifications of the attacker, describing various aspects of his behavior and training, the socio-psychological context of his actions, the target settings of these actions, affecting the choice of the attacker's strategy, methods and ways to implement information threats. Accordingly the introduced specifications formed reflexive risk models. These are mathematical models whose structure and parameters reflect (*latin.* reflexus) the characteristics of the attacker contained in its specification. A study of reflexive models has been carried out, which in a number of cases has made it possible to determine the limits of investment in the GIS, as well as limitations in the application of the RRP to the construction of the GIS.

Keywords: risk, risk modeling, reflexive risk models, maximum volumes of investments in ISS, risk-oriented approach.

Архипов Александр Евгеньевич, доктор технических наук, профессор кафедры информационной безопасности НТУУ «КПИ».
E-mail: sonet0515@gmail.com.

Архипов Олександр Євгенійович, доктор технічних наук, професор кафедри інформаційної безпеки НТУУ «КПІ».

Arkhypov Oleksandr, Professor, Doctor of Sciences in Eng., professor of the Department of Information Defense of National Technical University of Ukraine "Kyiv Polytechnic Institute".