УДК 004.942

Евсеев С.П.

Харьковский национальный экономический университет имени Семена Кузнеца

ОЦЕНКА ЭФФЕКТИВНОСТИ ИНВЕСТИЦИЙ В БЕЗОПАСНОСТЬ ОРГАНИЗАЦИЙ БАНКОВСКОГО СЕКТОРА НА ОСНОВЕ СИНЕРГЕТИЧЕСКОЙ МОДЕЛИ УГРОЗ

В статье проводится анализ методов оценки эффективности инвестирования в мероприятия информационной безопасности (ИБ). Предлагается комплексный показатель оценки эффективности инвестирования в безопасность банковской информации (ББИн) организаций банковского сектора (ОБС) на основе синергетической модели оценки ББИн и классификатора угроз в автоматизированных банковских системах (АБС) и формальное описание математической модели оценки эффективности инвестиций в Б БИн..

Ключевые слова: автоматизированные банковские системы, методы оценки эффективности инвестиций ИБ, комплексный показатель оценки эффективности безопасности банковской информации.

Введение. Развитие организаций банковского сектора (ОБС) тесно связано с интенсивным развитием как информационных технологий компьютерной системы Интернет, так и ее информационных ресурсов. ОБС относятся к критически важным инфраструктурам, имеющим ключевое значение для общественного порядка, экономической стабильности и национальной безопасности государств, ее защита затрагивает вопросы национальной безопасности, и потому входит в компетенцию государства [1]. Информационные технологии автоматизированных банковских систем (АБС) являются неотъемлемой частью бизнес-процессов ОБС, в которых для обеспечения непрерывной и безопасной обработки и циркуляции банковской информации (БИн) используется система защиты информации (СЗИ) на основе технических средств защиты информации (ТСЗИ). Принимая решения о финансировании на создание и поддержание на всех этапах жизненного цикла СЗИ ОБС стремятся существенно уменьшить материальный ущерб в процессе своей деятельности, затраты на обеспечение режима информационной безопасности (ИБ) составляют до 30 % всех затрат на информационную систему (ИС) [2 – 7]. Однако лишь 10% предприятий осуществляют эффективное инвестирование ИБ, 40% – подвергаются большим количествам рисков нарушения ИБ. Таким образом, проблема эффективного инвестирования ИБ предприятия еще не решена, что подтверждается анализом опубликованных работ и существующих подходов [12, 13].

Одним из основных вопросов ОБС является оценка эффективности принятия мер по обеспечению безопасности информационных активов БИн для получения максимальной прибыли. Оценка эффективности инвестиций в ИБ в настоящее время является актуальной проблемой, т.к. для оценки инвестиций в ИБ предприятия (ОБС) необходимо соотносить затраты на ИС и получаемые преимущества от использования ТСЗИ с точки зрения финансовой и организационной перспектив [3].

Целью статьи является анализ основных методов оценки инвестиций в ИБ предприятия, разработка метода оптимизации инвестиций в безопасность БИн ОБС на основе комплексного подхода оценки эффективности инвестиций в ББИн.

1. Анализ последних исследований [2 – 9] показал, что в рыночных условиях любое предприятие сосредоточено на поддержании конкурентоспособности. Непрерывный оборот информационного актива, связь между информационными ресурсами, эффективное функционирование информационных систем, в которых они обрабатываются, влияют на конечные финансовые показатели компании [12, 13].

Принято считать, что затраты на обеспечение информационной безопасности (ИБ) компании эффективны, если они обеспечивают выполнение требований государственных нормативных документов и стандартов, а также концепции ИБ.

Такое понимание связано с тем, что для объективной оценки экономического эффекта ИБ нет универсальных методов. Отсутствие обоснованных и общепринятых методов оценки

 © Евсеев С. П., 2017

инвестиций в ББИн зачастую создает ситуацию противоречия между предполагаемыми результатами, полученными при внедрении ТСЗИ в АБС ОБС и задачами оптимизации расходов, ограничивающими инвестиционные возможности ОБС.

Сложность оценки эффективности мероприятий по ББИн в АБС ОБС обусловлена целым рядом обстоятельств. В соответствии с теорией оценки эффективности систем, качество любого объекта, в том числе и СЗИ, проявляется лишь в процессе его использования по назначению (целевое функционирование), поэтому объективной является оценка по эффективности применения [9, 12,13]. Проведенный анализ методов оценки эффективности инвестиций показал [2 – 9, 12, 13], что условно они подразделяются на три группы: финансовые (традиционные, количественные), качественные (эвристические) и вероятностного характера. Общая классификация методов оценки инвестиций представлена на рис.1.

Под *экономическим эффектом* обычно понимают превышение стоимостных оценок конечных результатов соответствующих мероприятий над совокупными затратами ресурсов на их проведение за расчетный период [2, 7, 8].

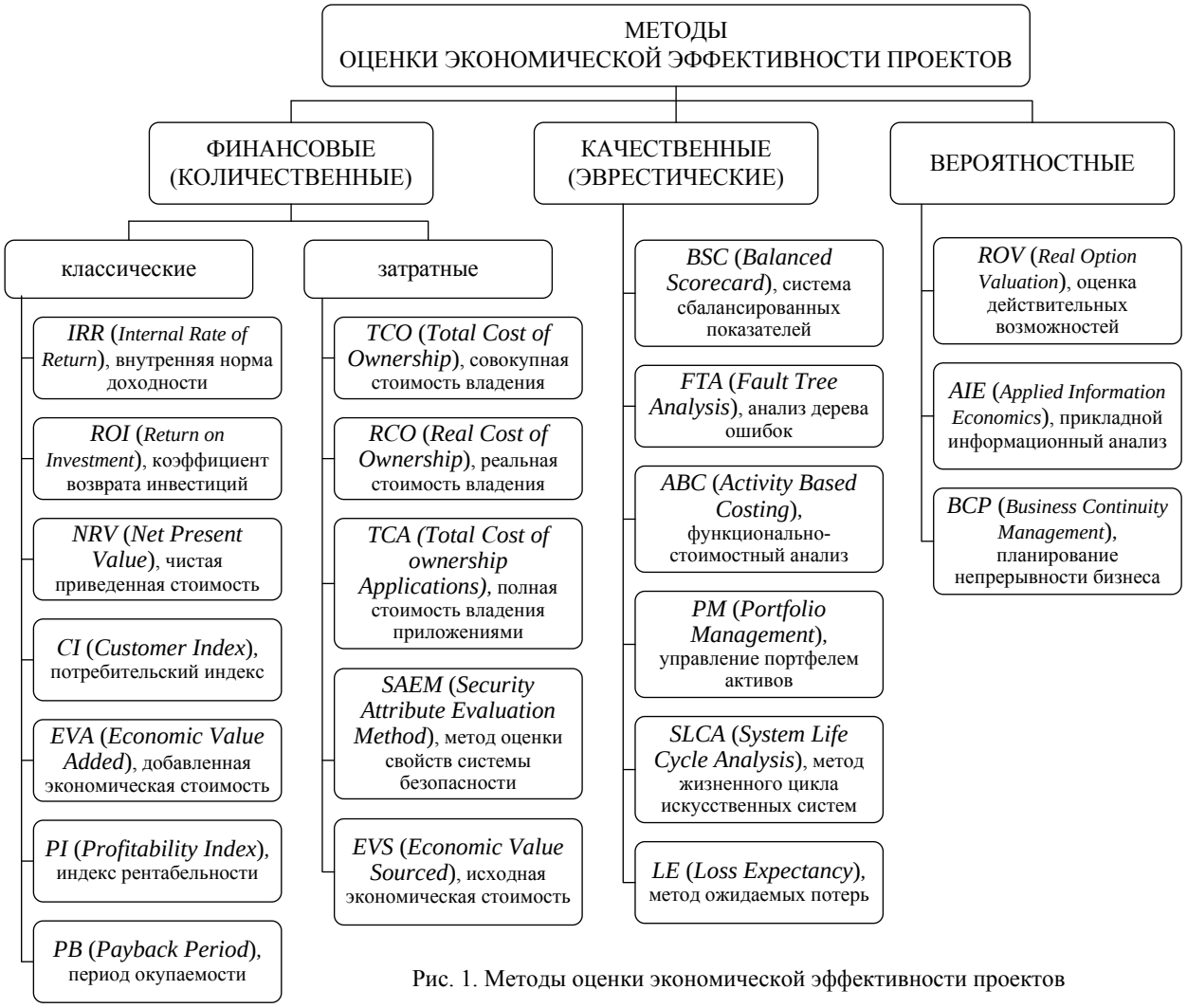

Рис. 1. Методы оценки экономической эффективности проектов

Для оценки экономической составляющей эффективности ИТ-проектов в мировой практике наиболее часто используют основные показатели финансовой группы: коэффициент рентабельности инвестиций (*ROI*), чистая приведенная стоимость (*NPV*), внутренняя норма рентабельности (*IRR*), период окупаемости (*Payback Period*), экономическая привлекательность (*EVA*), сбалансированная система показателей (*BSC*), совокупная стоимость владения (*TCO*) и т.п. Однако при попытке оценить чистую прибыль от реализации проекта по ИБ возникают существенные затруднения, т.к. методы изначально предназначены для анализа финансовых инвестиционных инструментов, учитывают преимущественно прямые затраты и их прямые эффекты и просто не учитывают в своих математических моделях важные нефинансовые параметры и эффекты при реализации проекта ИБ. Данная группа методов не позволяет адекватно оценить реальный

экономический эффект реализации проекта комплекса средств защиты информации (КСЗИ) [3, 6, 12, 13]. Затратные методы оценки (см. рис. 1) можно применить только в динамике. При этом отсутствие статистических данных в силу конфиденциальности БИн, не позволяет инвестору провести обоснованный расчет рисков АБС. Данная группа методов предполагает сравнение оцениваемого проекта с уже реализованными, при этом методы фактически не могут найти широкого применения в условиях жесткой конкурентной среды и с учетом действующих в компаниях ОБС режимов конфиденциальности. Более того, такой анализ путем сравнения проекта КСЗИ – соответственно раскрытия его состава – с проектами иных ОБС (конкурентов) и третьих лиц парадоксален и противоречит основной цели самого проекта [5].

Группа эвристических методов предлагает комплексный подход к оценке, однако имеет свои недостатки при оценке проектов КСЗИ ОБС. Так, метод сбалансированной системы показателей *BSC* (рис. 1) направлен на разработку стратегии управления на основе стратегических карт, группирующих цели и показатели по категориям: финансы, клиенты, процессы, развитие. Однако применение метода не предполагает создания стратегического плана развития ОБС и не требует отказа от традиционных инструментов планирования и контроля [7]. Метод *FTA* базируется на двух связанных предположениях о том, что компоненты системы разрушаются случайным образом в соответствии с известными вероятностями разрушений, и на самом низком уровне дерева составляющие отказа независимы друг от друга. Основными недостатками метода являются: неопределенность оценок вероятностей базисных событий влияет на оценку вероятности возникновения конечного события; в некоторых ситуациях начальные события не связаны между собой, и порой трудно установить, учтены ли все важные пути к конечному событию [4]. Методы *LE, PM, SLCA* основаны сравнении потерь от нарушений политики безопасности, с которыми может столкнуться ОБС, и инвестициями в безопасность ОБС. Методы опираются на результаты анализа экспертных групп ОБС на основании которых строятся модели “Как есть” и “Как будет”. Результаты работы экспертной группы в значительной степени субъективны и не дают объективной оценки сформулированных рисков. Эти недостатки характерны для всей группы эмпирических методов оценки.

Группа вероятностных методов оценки (рис. 1) предлагает заблаговременное внедрение специфических систем управления/менеджмента качеством(а) (СМК) в компании, требует значительных затрат финансовых, трудовых и временных ресурсов, направлена не столько на оценку отдельных проектов, сколько на общее управление деятельностью предприятия и подходят только для дорогостоящих длительных проектов [5].

Таким образом, проведенный анализ методов оценок эффективности инвестиций ИБ показал, что формирование объективной оценки эффективности инвестиций в МС крайне трудоемкий процесс, и как правило оценка мероприятий ББИн ОБС сводится к нахождению категорий:

ROI, “*Return on Investment*”, коэффициент возврата инвестиций;

TCO, “*Total Cost of Ownership*”, совокупная стоимость владения;

PB, “*Payback Period*” период окупаемости.

2. Разработка комплексного показателя эффективности инвестиций на основе синергетической модели угроз. Для оценки затрат на ББИн в ОБС воспользуемся подходом, предложенным в работах [3, 12, 13]. Специфика подхода основывается на предложенных автором моделях угроз и нарушителя на основе синергетического подхода, классификатора угроз в АБС [10, 11], и сводится к расчету рисков нарушения Б БИн в АБС, позволяющего оценить непрерывность функционирования бизнес-процессов (информационных процессов) в АБС и коэффициента внутренней нормы рентабельности инвестиций.

Представление ББИн как информационного процесса, а не продукта, даёт возможность интерпретировать безопасность информационных активов как многофункциональный процесс управления рисками нарушения режима безопасности ОБС. В результате управления рисками можно достичь баланса информационных рисков для деятельности ОБС, снижая потенциальные угрозы, направленные на вычислительные средства, обрабатывающие информационные ресурсы. Результатами баланса рисков информационных активов является выбор эффективного метода управления, который позволяет максимально точно определить параметры безопасности БИн, и получение максимальной прибыли от вложенных средств на построение СЗИ в АБС [13].

Формальное описание модели оценки инвестиций в Б БИн ОБС можно представить [3, 10 – 14]:

$$W_{ABS}^{effinv} = \begin{Bmatrix} I_{O^{ABS}}, \Delta^{ABS}, \{DF^{ABS}\}, rang^{ABS}, \{SZ^{ABS}\}, d^{ABS}, D^{ABS} \\ ROI^{ABS}, NPV^{ABS}, ROSI^{ABS}, r^{ABS}, CV^{ABS}, OU^{ABS} \end{Bmatrix}$$

где $I_{O^{ABS}}$ – значимость информационного актива;

Δ^{ABS} – признак эффективности затрат;

$\{DF^{ABS}\}$ – множество источников угроз безопасности БИн АБС [10];

$rang^{ABS}$ – ранг процесса разработки СЗИ;

$\{SZ^{ABS}\}$ – множество СЗИ [10];

d^{ABS} – приведенная стоимость денежного потока;

ROI^{ABS} – коэффициент возврата инвестиций;

NPV^{ABS} – чистая приведенная стоимость;

$ROSI^{ABS}$ – рентабельность инвестиций в СЗИ;

r^{ABS} – коэффициент рентабельности в ББИн;

CV^{ABS} – степень риска в единицу среднего дохода;

D^{ABS} – доход от использования СЗИ;

OU^{ABS} – оценка дохода от использования СЗИ.

Значимость информационного актива оценим за формулой:

$$I_{O^{ABS}} = \frac{E_{BIn}^{ABS}}{Y_{BIn}^{ABS}}, \quad (1)$$

где E_{BIn}^{ABS} – стоимость информационного ресурса (ИР БИн) БИн; Y_{BIn}^{ABS} – капитал, вложенный в эксплуатацию этого ИР БИн.

Признак эффективности затрат Δ^{ABS} можно оценить по формуле:

$$\Delta^{ABS} = \frac{e}{b}, \quad (2)$$

где e – ожидаемый экономический эффект; b – расходы на разработку СЗИ.

Если ОБС взвешивает целесообразность реализации того или иного проекта, то, в простейшем случае она может рассчитать чистую приведенную стоимость NPV^{ABS} прибыли и затрат, которые принесет проект и сравнит их. Другими словами, прибыль от инвестиций должна превосходить затраты, а уровень доходности ОБС устанавливает самостоятельно [3].

$$ROI^{ABS} = NPV_{inv}^{ABS} - NPV_{zt}^{ABS}, \quad (3)$$

где NPV_{inv}^{ABS} – прибыль от инвестиций в СЗИ АБС;

NPV_{zt}^{ABS} – затраты в СЗИ АБС;

ROI^{ABS} – доходность инвестиций в СЗИ АБС.

Такой же подход применим для оценки целесообразности в ББИн. Основное отличие – инвестиции в ББИн не приносят прибыль, а лишь гипотетически предотвращают затраты. Таким образом, ТСЗИ АБС ОБС должны предотвратить затраты на большую сумму, чем средства, затраченные на их разработку и внедрение в СЗИ АБС, что и будет говорить о рентабельности инвестиций в ТСЗИ ($ROSI^{ABS}$) [3]:

$$ROSI^{ABS} = NPV_{zbtszi}^{ABS} - NPV_{zvtszi}^{ABS}, \quad (4)$$

где NPV_{zbtszi}^{ABS} – затраты на устранение компрометации безопасности без внедренных ТСЗИ;

NPV_{zvtszi}^{ABS} – затраты на устранение компрометации безопасности с внедренными ТСЗИ.

При этом чистая приведенная стоимость NPV^{ABS} рассчитывается по формуле:

$$NPV_{zbtszi}^{ABS} = \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i}, \; NPV_{zvtszi}^{ABS} = C_{sz} + \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i}, \quad (5)$$

где N – число интервалов инвестирования;

ALE_i – ожидаемые потери в i-м периоде;

r – ставка дисконтирования;

C_{sz} – стоимость средств защиты.

Для получения синергетического эффекта повышения уровня защищенности БИн необходимо учитывать комплексирование угроз:

$$DF^{ABS} = \{V^{NS}\} \cup \{V^{AS}\}, \quad (6)$$

где $\{V^{AS}\} = \{V^{ASBI}\} \cap \{V^{ASIB}\} \cap \{V^{ASKBr}\}$, в котором V^{NS} – класс естественных источников угроз, $V^{AS} = \{V^{ASIB}, V^{ASBI}, V^{ASKBr}\}$ – класс антропогенных угроз, где V^{ASIB} – множество угроз информационной безопасности, V^{ASBI} – множество угроз безопасности информации, V^{ASKBr} – множество угроз кибербезопасности. Каждый элемент из множества угроз $DF_i \in \{DF^{ABS}\}$, может быть представлен следующим вектором значений DF_i *(p,u,risk)*, где p – вероятность реализации угрозы, u – потенциальный ущерб, *risk* – риск, выраженный в качественной форме и принимающий одно из двух состояний T_{risk}={допустимый, недопустимый}={α_{r1},α_{r2}}.

При оценке риска БИн применим методику расчета *Annual loss expectancy – ALE,* то есть ожидаемых потерь в каждый период оценки:

$$ALE^{ABS} = \sum_{i=1}^{n} I\left(O_{DF}^{ABS}\right) F_i, \quad (7)$$

где $\{O_{DF}^{ABS}\}$ – множество угроз;

$I\left(O_{DF}^{ABS}\right)$ – стоимостные последствия реализации угрозы;

ALE^{ABS} – ожидаемый урон от реализации;

F_i – частота (возможность) реализации угрозы.

Затраты на разработку СЗИ ОБС определяются *рангом*. Оценка ранга разработки СЗИ ОБС $rang^{ABS}$ производится по формуле:

$$rang^{ABS} = \frac{SUM \times p}{s_{OPZ}^{ABS}}, \quad (8)$$

где *SUM* – ожидаемая прибыль от внедрения СЗИ в АБС ОБС;

p – вероятность успеха использования СЗИ;

s_{OPZ}^{ABS} – расходы на разработку, внедрение и поддержания уровня защищенности СЗИ.

Приведенная стоимость денежного потока d^{ABS} оценивается по формуле:

$$d^{ABS} = D_r + ROI^{ABS}, \quad (9)$$

где D_r – коэффициент дисконтирования;

ROI^{ABS} – доходность инвестиций в СЗИ АБС.

Коэффициент рентабельности инвестиций в Б БИн r^{ABS} вычисляется по формуле:

$$r^{ABS} = \sum_{t=1}^{T} \frac{CF_t}{\left(1 + ROSI^{ABS}\right)}, \quad (10)$$

где *t* – начало временного периода;

CF_t – денежный поток в период времени *t*;

$ROSI^{ABS}$ – доход от реализации проекта;

T – конец временного периода.

Оценку степени риска в единицу среднего дохода CV^{ABS} получим, используя формулу:

$$CV^{ABS} = \frac{\sigma(E)}{M(E)}, \quad (11)$$

где $\sigma(E)$ – среднеквадратическое отклонение затрат на реализацию СЗИ ОБС;

$M(E)$ – математическое ожидание на реализацию СЗИ ОБС.

Доход D^{ABS} от использования СЗИ можно оценить по формуле:

$$D^{ABS} = Cost_1 P_D - Cost_2(1 - P_D), \quad (12)$$

где P_D – вероятность получения дохода;

$(1 - P_D)$ – вероятность получения убытков;

$Cost_1, Cost_2$ – единицы стоимости информационного актива.

Предложенная модель базируется на оценке инвестиций в ББИн ОБС и на дисконтировании будущих денежных поступлений и расходов. Таким образом, данная модель учитывает изменение инвестиций в ББИн ОБС с течением времени.

Описательной характеристикой изменения инвестиционного потока является его *интенсивность l(t)* – среднее число изменений, произошедших в потоке в единицу времени [13]. Интенсивность позволяет оценить интервалы времени $\Delta t_{[i-q]}$ между изменениями, произошедшими в потоке, используя формулу [13]:

$$\Delta t_{[i-q]}(t) = \frac{K}{l(t)}, \quad (13)$$

где K – суммарное количество изменений инвестиций;

l(t) – интенсивность инвестиционного потока;

$i, q \in [1; n]$ – порядковые номера изменений; $i \geq q$.

Изменения процессов инвестирования в Б БИн ОБС описываются в виде конечного автомата H^{ABS}, состояния которого описывает формула [13]:

$$H^{ABS} = \left\langle S^I, value, \Pi, S_0^I \right\rangle, \quad (14)$$

где S^I – конечное состояние инвестиций;

$value$ – значение изменений инвестиций;

Π – функция переходов инвестиций из состояния *k* в состояние *j*;

S_0^I – начальное состояние инвестиций.

Функция переходов инвестиций Π из состояния *k* в состояние *j* оценивается по формуле:

$$\Pi = S^I \times value \rightarrow S^I. \quad (15)$$

Оценку потенциального ущерба U^{ABS} информационного актива получим из формулы:

$$U^{ABS} = p_{rj} u_j, \quad (16)$$

где p_{rj} – вероятность реализации хотя бы одной угрозы *j*-му активу;

u_j – ценность *j*-го актива.

Расчет вероятности реализации хотя бы одной угрозы для каждого актива выполняется по формуле:

$$p_{rj} = 1 - \prod_{i=1}^{m} \left(1 - pr_{ij}\right), \quad (17)$$

Таким образом, оценка общего ожидаемого ущерба OU^{ABS} состоит из потенциальных ущербов и определяется по формуле:

$$OU^{ABS} = \sum_{j=1}^{n} U^{ABS}. \quad (18)$$

Каждому параметру присваиваются весовые категории по правилу Фишберна [14], основанном на том, что изменение весовых коэффициентов критериев подчиняется убывающей арифметической прогрессии. При этом первый критерий (i = 1), расположен первым в строго упорядоченном по важности ранжированном ряду критериев i = 1, 2, ..., *n*, является наиболее важным и имеет наибольший весовой коэффициент. Данное правило задается формулой:

$$w_i = \frac{2(N - n + 1)}{N(N + 1)}, \quad (19)$$

где w_i – весовой коэффициент Фишберна для критерия оценки эффективности инвестиций в ББИн ОБС;

N – общее количество параметров интегрального критерия оценки эффективности инвестиций в Б БИн ОБС;

n – порядковый номер параметра, i – количество параметров в интегральном критерии оценки.

Согласно формулы Фишберна имеем:

$$w_1 = \frac{2 \times N}{N(N+1)},\ w_N = \frac{2}{N(N+1)},\ \gamma = \frac{w_1}{w_N} = N, \quad (20)$$

где γ – кратность отличия весовых коэффициентов друг от друга.

Таким образом, формируем систему весовых коэффициентов Фишберна W_{Φ}^{ABS}, с условиями:

$$w_i \in [0;1],\ W_{\Phi}^{ABS} = \sum_{i=1}^{N} w_i, \quad (21)$$

где $i \in [1;N]$.

В качестве оптимизационных мер в работах [12, 13] предлагается использовать оценку совокупной стоимости затрат на ликвидацию последствий реализации угрозы и иных причин вывода из строя ТСЗИ, и суммарные выплаты источникам финансирования.

Оценка совокупной стоимости затрат M^{ABS} ликвидации последствий реализации угрозы и иных причин вывода из строя ТСЗИ производится по формуле:

$$M^{ABS} = \sum_{i=1}^{m} C_i, \quad (22)$$

где C_i – стоимость і-й меры; m – общее число принятых мер.

Оценка суммарных выплат c_i источников финансирования формируется по формуле:

$$c_i = \sum_{i=1}^{n} A_{i,j}, \quad (23)$$

где c_i – суммарные выплаты j-му источнику финансирования;

$A_{i,j}$ – выплаты j-му источнику финансирования;

$i, j = 1...n$; n – число источников финансирования.

Предложенная модель эффективности инвестиций в ББИн ОБС решает задачу повышения эффективности инвестиций путем минимизации затрат на Б БИн ОБС.

Минимизация затрат на Б БИн ОБС производится оптимизационным процессом, который отражает следующая формула:

$$\min\left(E_1^{ABS} b_1 + E_2^{ABS} b_2 + \ldots + E_j^{ABS} b_n\right), \quad (24)$$

где E_j^{ABS} – j-й критерий оптимизации, $j = 1...n$, n – количество критериев;

b_n – признак использования j-го источника финансирования,

$$b_n = \begin{cases} 1, \text{если источник финансиров ания использован,} \\ 0, \text{если источник финансиров ания не использован} \end{cases}. \quad (25)$$

В рамках предложенной модели эффективности инвестиций в ББИн ОБС оцениваются следующие параметры – совокупная стоимость затрат ликвидации последствий реализации угрозы, или иных причин вывода из строя систем защиты информации, и суммарные выплаты источников финансирования, для того, чтобы определить допустимые уровни рисков нарушения информационной безопасности ОБС. При этом обеспечивается минимизация ущерба, а затраты на безопасность БИн ОБС являются эффективными, так как прибыль, полученная от внедрения СЗИ, больше чем вложенный капитал [13].

Обобщив параметры, используемые в рамках предложенной модели, определим интегральный критерий эффективности инвестиций в ББИн ОБС, используя формулу:

$$W_{ABS}^{effinv} = \sum_{i=1}^{N} w_i M^{ABS}. \quad \ldots(26)$$

Таким образом, модель эффективности инвестиций в Б БИн ОБС может находится в разных состояниях S^{ABS}, которые можно описать в виде следующего множества:

$$S^{ABS} = \left\{S_1^{ABS}, S_2^{ABS}, \ldots, S_m^{ABS}\right\}, \quad (27)$$

где S^{ABS} – множество возможных состояний модели;

S_1^{ABS} – начальное состояние модели;

S_m^{ABS} – конечное состояние модели.

Выводы. Таким образом, проведенные исследования показали, что оценка эффективности инвестиций в ИБ предприятия крайне трудоемкий процесс, и как правило оценка мероприятий ББИн ОБС сводится к нахождению категорий: *ROI, TCO, PB*. Такой подход не учитывает синергетику угроз БИн в АБС, и не позволяет оптимизировать инвестиционную политику ОБС. Предложенная модель эффективности инвестиций в ББИн ОБС полностью формализована, ориентирована на использование в ОБС с централизованным документооборотом, позволяет производить комплексную оценку затрат на Б БИн ОБС, определить интервалы времени между изменениями инвестиций в безопасность БИн, и обеспечивает повышение эффективности инвестиций в Б БИн ОБС.

Перспективным направлением дальнейших исследований является реализация предложенного комплексного показателя оценки эффективности инвестирования в ББИн организаций банковского

сектора на основе синергетической модели оценки ББИн и классификатора угроз в автоматизированных банковских системах с целью практической оценки оптимизационного процесса инвестиций в ББИн.

Список литературы

1. Леоненко Г.П. Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины / Г.П. Леоненко, А.Ю. Юдин // Information Technology and Security". № 1(3). 2013. С. 44 – 48.

2. Синяк А.А. Анализ методов оценки эффективности затрат в информационную безопасность / А.А. Синяк, Н.Е. Губенко // ИУС и КМ. Секция 4. Web-технологии и ИБ. – 2012. – С. 444 – 446.

3 Первадчук В.П. Оценка эффективности инвестирования в информационную безопасность предприятия на основе нечетких множеств / В.П. Первадчук, В.А. Белецкий // Вестник ИжГТУ. – 2011. – № 1(49). – С. 51 – 53.

4. Зубарева Е.В. Методы оценки инвестиций в информационную безопасность предприятия / Е.В. Зубарева, А.А. Бабенко// – [Электронный ресурс]. – Режим доступа к ресурсу: www.volsu.ru/download.php?id=000028639-1.pdf

5. Хомяков К.Г. Оценка эффективности инвестиций в комплексные системы защиты информации компаний нефтегазового комплекса для принятия взвешенного инвестиционного решения / К.Г. Хомяков, Л.В. Каницкая // Экономика. Фундаментальные исследования. – 2015. – Вып. № 2. – С. 5173 – 5177.

6. Ажмухамедов И.М. Оценка экономической эффективности мер по обеспечению информационной безопасности // И.М. Ажмухамедов, Т.Б. Ханжина // Вестник АГТУ. Сер.: Экономика. – 2011. – Вып. № 1. – С. 185 – 190.

7. Петренко С.А. Оценка затрат на кибербезопасность // Труды ИСА РАН. – 2006. – Т.27. – С. 235 – 265.

8. Никита Кожокару Эффективность инвестиций в области информационной безопасности // – [Электронный ресурс]. – Режим доступа к ресурсу: http://www.securitylab.ru/bitrix/exturl.php?goto=http://1.bp.blogspot.com/-7Lhsq9eFw7U/VhZrMFnOLJI/AAAAAAAAHqk/AHT9E2u8R9E/s1600/risk-taxanomy.bmp

9. Ефимов Е.Н. Оценка эффективности мероприятий информационной безопасности в условиях неопределенности / Е.Н. Ефимов, Г.М. Лапицкая // Бизнес-Информатика. Математические методы и алгоритмы решения задач бизнес -информатики. – 2015. – Вып. №1(31). – С. 51 – 57.

10. Евсеев С.П. Синергетическая модель оценки безопасности банковской информации // Науково-технічний журнал "Інформаційна безпека". № 4. Сєвєродонецьк. – 2016. – С. 43 – 58.

11. Евсеев С.П. Науково-технічний журнал "Інформаційна безпека". № 17. Сєвєродонецьк. – 2017. – С. 58 – 69.

12. Жаринова С.С. Оптимизация инвестиций в информационную безопасность предприятия / С.С. Жаринова, А.А. Бабенко // ГУ-УНПК: Информационные системы и технологии – 2014. – Вып. 3 (83). С. 114 – 123.

13. Жаринова С.С. Модель эффективности инвестиций в информационную безопасность предприятия / С.С. Жаринова, А.А. Бабенко // – [Электронный ресурс]. – Режим доступа к ресурсу: www.volsu.ru/download.php?id=000026221-1.pdf.

14. Постников В. М. Методы выбора весовых коэффициентов локальных критериев / Постников В. М., Спиридонов С. Б.// Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл № ФС 77 – 48211.– 2016. Вып. № 3. – С.267 – 287.

Надійшло до редколегії 24.02.2017

Рецензент: д-р фіз-мат. наук проф. С. Є. Остапов Чернівецький національний університет імені Юрія Федьковича, Чернівці.

ОЦІНКА ЕФЕКТИВНОСТІ ІНВЕСТИЦІЙ В БЕЗПЕКУ ОРГАНІЗАЦІЙ БАНКІВСЬКОГО СЕКТОРА НА ОСНОВІ СИНЕРГЕТИЧНОЇ МОДЕЛІ ЗАГРОЗ

С.П. Євсеєв

У статті проводиться аналіз методів оцінки ефективності інвестування у заходи інформаційної безпеки (ІБ). Пропонується комплексний показник оцінки ефективності інвестування в безпеку банківської інформації (ББІн) організацій банківського сектора (ОБС) на основі синергетичної моделі оцінки ББІн і класифікатора загроз в автоматизованих банківських системах (АБС).

***Ключові слова**: автоматизовані банківські системи, методи оцінки ефективності інвестицій ІБ, комплексний показник оцінки ефективності безпеки банківської інформації.*

EVALUATION OF THE EFFECTIVENESS OF INVESTMENTS IN THE BANKING SECTOR SECURITY ORGANIZATIONS BASED ON SYNERGETIC MODEL THREATS

S. Yevseiev

The article analyzes the methods of evaluating the effectiveness of investment in information security events (IB). A complex indicator of evaluating the effectiveness of investment in the safety of bank information (BBIn) banking organizations (CBOs) based on synergetic model BBIn assessment classifier and threat in automated banking systems (ABS).

***Keywords**: automated banking systems, methods for evaluating the effectiveness of information security investments, complex index of evaluating the effectiveness of the security of banking information.*