УДК 519.866+004.056.5

А.А. Ткачев
ГВУЗ "Донецкий национальный технический университет" (Донецк)

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ ПРЕДПРИЯТИЯ С УЧЕТОМ ЭФФЕКТИВНОСТИ ЗАТРАТ НА ИХ СНИЖЕНИЕ

Рассмотрена сущность информационных рисков (ИР), основные направления их исследования на предприятиях, представлена классификация и характеристика источников возникновения ИР, предложена методика оценки и управления рисками предприятия с учетом эффективности затрат на их снижение.

Ключевые слова: *информационный риск, идентификация угроз, снижение экономического ущерба.*

За последние годы прогресс в сфере информационных технологий, превращение информации в производственный ресурс, колоссальный рост объемов информации обусловили формирование новой отрасли бизнеса – создание продуктов и оказание услуг по защите информации. Кроме того, наблюдается постоянный рост нарушений информационной безопасности в мире и растущая тяжесть их последствий, что обуславливает актуальность и практическую важность темы данной работы. Общее число нарушений ежегодно увеличивается более, чем на 100 %. По статистике правоохранительных органов, число выявленных преступлений в сфере компьютерной информации возрастает за год в среднем в 3-4 раза. Если коммерческая организация допускает утечку более 20 % важной внутренней информации, то она в 60 случаях из 100 банкротится. Порядка 93 % компаний, которые были лишены доступа к собственной информации на срок более 10 дней, покинули бизнес, причем половина из них заявила о своей несостоятельности немедленно [1].

Очевидно, что финансовые потери бизнеса, как крупного, так и малого, возрастают, поэтому необходим поиск и внедрение научно обоснованных и технологически оправданных методов управления информационными рисками (ИР).

Ранжирование по степени тяжести последствий потери конфиденциальности информации многими украинскими предприятиями показывает сходство украинской и международной практики в этой области: удар по репутации и потеря клиентов (79,2 %), прямые финансовые убытки (46 %), снижение конкурентоспособности (25,2 %) [2]. Расчет реальных убытков от реализации ИР достаточно сложен, поскольку речь идет об информации как нематериальном активе. При этом очевидно, что своевременное финансирование мероприятий по ее защите с целью минимизации ИР было бы для компаний значительно дешевле.

В исследованиях украинских и российских исследователей [1,3,4] освещены многочисленные проблемы использования информационных технологий в деятельности предприятий, механизмы и методы обеспечения информационной безопасности, изложены теоретические взгляды на инвестиции в мероприятия по защите информации, предложены методы оценки затрат компаний на информационную безопасность. Множество работ посвящено исследованию экономических рисков предприятий [5-7]. За рубежом изучались вопросы оценки ИР [8 и др.], информационной безопасности [9,10] и т.д. Вместе с тем, в этих трудах недостаточно изученными остаются вопросы управления ИР хозяйствующих субъектов.

Целью данной работы является исследование теоретической сущности ИР, источников их возникновения, разработка методического комплекса управления рисками предприятия с учетом экономической целесообразности затрат на их снижение.

ИР – ситуация, для которой характерна возможность получения убытков предприятием в результате применения информационных технологий, т.е. связанных с созданием, хранением, передачей, использованием информации с помощью средств связи.

Исследование ИР предприятия включает следующие этапы:

1) выявление перечня наиболее ценных ресурсов с обозначением уровня их конфиденциальности, целостности и доступности (проводится инвентаризация информационных ресурсов и

их распределение по категориям);

2) идентификация угроз, связанных с информационными ресурсами;

3) формирование моделей нарушителей и механизмов реализации угроз;

4) количественная оценка ИР и прогнозирование возможных финансовых потерь предприятия;

5) разработка мероприятий по предотвращению угроз или снижению вероятности их реализации.

С учетом разнообразия информационных ресурсов, хранящихся и обрабатываемых на предприятии, их различной ценности для предприятия и вероятных злоумышленников предлагается использование трех категорий ценности (полезности, стоимости) информационных ресурсов, характеризующих уровень их конфиденциальности, целостности и доступности:

$Ц_Б$=1 – категория информационных ресурсов с не очень важной информацией, которая не требует введения каких-либо ограничений на распространение и использование, однако даже потеря одного из свойств информации может нанести незначительный ущерб предприятию;

$Ц_Б$=2 – категория достаточно важной информации, потеря каждого из свойств которой приводит к нанесению значительного ущерба предприятию;

$Ц_Б$=3 – категория важнейшей информации, нарушение целостности и конфиденциальности которой нанесет предприятию максимальный ущерб.

Для типового предприятия информационные ресурсы по ценности можно разделить на категории следующим образом:

– не очень важная информация: информация о персональных данных сотрудников предприятия;

– важная информация: научно-техническая информация, данные финансового учета и управленческой отчетности, данные налогового и бухгалтерского учета, счета-фактуры, накладные, платежные поручения и другие расчетно-платежные документы, журналы учета входящей и исходящей корреспонденции, информация об основных средствах и нематериальных активах;

– самая важная информация: базы данных о клиентах и поставщиках предприятия, информация о перспективных разработках и бизнес-планы, кадровый, бухгалтерский и технический архивы предприятия, реестры контрактов и договоров, результаты маркетинговых исследований, электронная цифровая подпись, электронные ключи, пароли.

В рамках второго этапа исследования ИР предприятия осуществляется идентификация источников их возникновения. Источниками ИР являются любые потенциально возможные события, действия, процессы или явления, которые могут привести к нарушению конфиденциальности информации, ее потери или неправомерного использования, а значит, к реализации ИР.

Источники ИР можно классифицировать по определенным признакам:

– по отношению к предприятию: внутренние и внешние [5,6];

– по характеру нанесенного ущерба: источники, наносящие моральный или материальный ущерб;

– по вероятности появления: маловероятные, средней и высокой вероятности наступления;

– по причинам возникновения: случайная или преднамеренная утечка информации, техническая уязвимость предприятия, ошибки сотрудников, стихийные бедствия, преднамеренные действия сотрудников или третьих лиц и тому подобное.

Статистика свидетельствует [1,3], что в среднем 17 % всех источников ИР формируется за пределами предприятия (внешние источники), 1 % – угрозы со стороны случайных лиц и 82 % – внутренние источники рисков, т.е. от персонала организации. Злоумышленники рассчитывают, что пользователи будут устанавливать вредоносные программы или помогать им использовать бреши в системе защиты [9]. Наиболее опасными с точки зрения убытков и наиболее частыми считаются непреднамеренные ошибки штатных сотрудников (неверно введенные данные, ошибочное удаление информации, халатность, необразованность). Именно такие ошибки создают уязвимые места в системе защиты информации. В среднем, непреднамеренные ошибки приносят 60-65 % потерь, тогда как, например, на долю стихийных бедствий (ураганы, пожары, наводнения, перебой электроснабжения и др.) приходится около 13 % всех потерь от источников рисков.

Наиболее распространенными в настоящее время основными угрозами информационным ресурсам предприятия, обозначаемыми многими ведущими отечественными специалистами в области информационной безопасности [4], являются следующие:

$У_1$ – инфицирование компьютеров вирусами;

$У_2$ – заражение компьютерных и телефонных цифровых сетей вредоносными программами для скрытого несанкционированного доступа к информационным ресурсам;

$У_3$ – ошибочное введение информации;

$У_4$ – несанкционированное изменение ин-

формации;

$У_5$ – повреждение (порча, разрушение) фрагментов информационной системы;

$У_6$ – уничтожение информационных ресурсов;

$У_7$ – потеря переносных носителей информации (флэш-память и др.) с конфиденциальными данными;

$У_8$ – похищение (кража) носителей информации;

$У_9$ – несанкционированное чтение, копирование информации.

Следующий этап управления ИР предприятия заключается в выборе системы защиты его информационных ресурсов, для чего составляется модель возможных нарушителей с учетом заинтересованных персоналий, их мотивации, квалификации. Нарушитель – это лицо, которое может выполнить запрещенное действие с информационными ресурсами по ошибке, без злого умысла или осознанно для достижения корыстной цели или ради забавы, мести, удовлетворения своих амбиций, используя для этого все возможные методы и средства. Возможными участниками нарушений информационной безопасности предприятия, способными причинить его информационным ресурсам наибольший вред, являются: *A* – сотрудники; *B* – бывшие сотрудники; *C* – конкуренты; *D* – хакеры; *E* – преступники. Моделью нарушителя выступает инициатор нарушения в сочетании с его исполнителем. Так, модель нарушителя с условным обозначением *C-A* показывает, что несанкционированные действия осуществляются работающим сотрудником предприятия по заказу конкурентов.

Методология измерения ИР основывается на их стоимостной оценке. В этом и заключается основная сложность, поскольку такая оценка затруднена отсутствием материального наполнения информации как носителя рисков. Информационная безопасность охватывает все бизнес-процессы деятельности предприятий [11]. Такая кросс-операционность препятствует четкой классификации и анализу издержек, направленных на обеспечение информационной безопасности, т.е. на уменьшение ИР до требуемого уровня. При этом для такого объекта, как конфиденциальная информация, методики оценки стоимости фактически отсутствуют.

Кроме того, стоимость коммерческой информации субъективна. Она должна определяться с учетом конкретных условий, характеристик потребляющих ее систем, особенностей источника и получателя информации. Общие подходы к оценке стоимости информации: прямая выгода, которая может быть обеспечена в результате получения информации; прямые убытки, которые могут быть нанесены в результате утраты информации; минимальная стоимость затрат на восстановление информации. Совершенно ясно, что здесь использованы характеристики вероятности – ожидаемая (потенциальная) выгода и возможные (потенциальные) убытки. Кроме того, ценность информации является величиной, которая зависит от времени – она может определяться степенью недостатка информации и возможной или желаемой скоростью ее получения.

При оценке ИР предприятия наиболее целесообразным является расчет уровня риска потери информации как произведения полезности (ценности, стоимости) информационного ресурса на его уязвимость и вероятность реализации угрозы в отношении данного информационного ресурса [8,12]:

$$ИР = Ц_Б У В_Р,$$

где *ИР* – уровень ИР; $Ц_Б$ – балльная оценка ценности (полезности) информационного ресурса; *У* – уязвимость информационного ресурса; B_P – вероятность реализации ИР за определенный (расчетный) промежуток времени.

На этапе работы по управлению ИР, как правило, возможны следующие сценарии [7,13]:

1) принять риск – согласиться с возможными потерями (в случае низких рисков);

2) снизить риск – осуществить мероприятия по уменьшению его уровня (в случае среднего уровня рисков);

3) передать риск (например, страховой компании, которая компенсирует убыток в случае реализации риска) или трансформировать риск в другой, меньший по размеру, путем использования специальных механизмов и технологий;

4) отказаться от риска, т.е. ликвидировать его источник – информационный ресурс.

Относительно передачи риска страховой компании необходимо отметить, что в настоящее время отечественные страховые компании страхуют ИР, принимая на себя обязательства по возмещению убытков, связанных с утратой информационных ресурсов и электронных финансовых активов в результате следующих причин: сбоев информационных систем вследствие ошибок при их проектировании, разработке, создании, инсталляции, конфигурировании, обслуживании или эксплуатации; умышленных противоправных действий сотрудников компании; компьютерных атак против компании со стороны третьих лиц; действий компьютерных вирусов; хищений денежных средств и ценных бумаг с

использованием компьютерных сетей. Информация страхуется по стоимости восстановления (этот подход распространен во всем мире). Данный вид страхования ориентирован на компании, имеющие значительные объемы финансовой, экономической и технической информации, сложные информационные системы или осуществляющие часть своей деятельности с использованием автоматизированных систем, систем электронных расчетов или Интернет.

Передача ИР является внешним методом его нейтрализации.

Рассмотрение внутренних методов управления ИР на уровне предприятия позволяет предложить следующую их градацию:

1) административные методы – разработка политики в области управления ИР, принятие документированных управленческих решений руководством предприятия;

2) процедурные (организационные) методы – воздействие на персонал (разработка должностных инструкций, обучение персонала, требования к рабочим), меры физической защиты (охранно-пожарная система, защита территории, системы контроля и доступа), планирование и проведение восстановительных работ;

3) программно-технические методы – защита оборудования, программных средств и информационных ресурсов, которая реализуется с помощью сервисов безопасности (идентификация и аутентификация, разграничение доступа, протоколирование и аудит, шифрование, экранирование, обеспечение целостности, доступности и отказоустойчивости);

4) финансово-экономические методы – планирование, стоимостная оценка рисков, бюджетирование, стоимостная оценка эффективности расходов, оптимизация затрат, инвестиционный анализ IT-проектов, страхование.

Практика свидетельствует, что наибольшее количество мероприятий снижения уровня ИР относится к инженерно-техническому обеспечению информационной безопасности, заметно меньшее количество – к организационным мероприятиям.

Сочетания и упорядочения направлений исследования ИР позволили разработать методический комплекс управления рисками предприятия (рис. 1).

При бюджетировании затрат на управление ИР из множества мер защиты от рисков выбирают те действия, реализация которых позволит обеспечить оптимальный уровень затрат для поддержания достаточной защищенности ин-

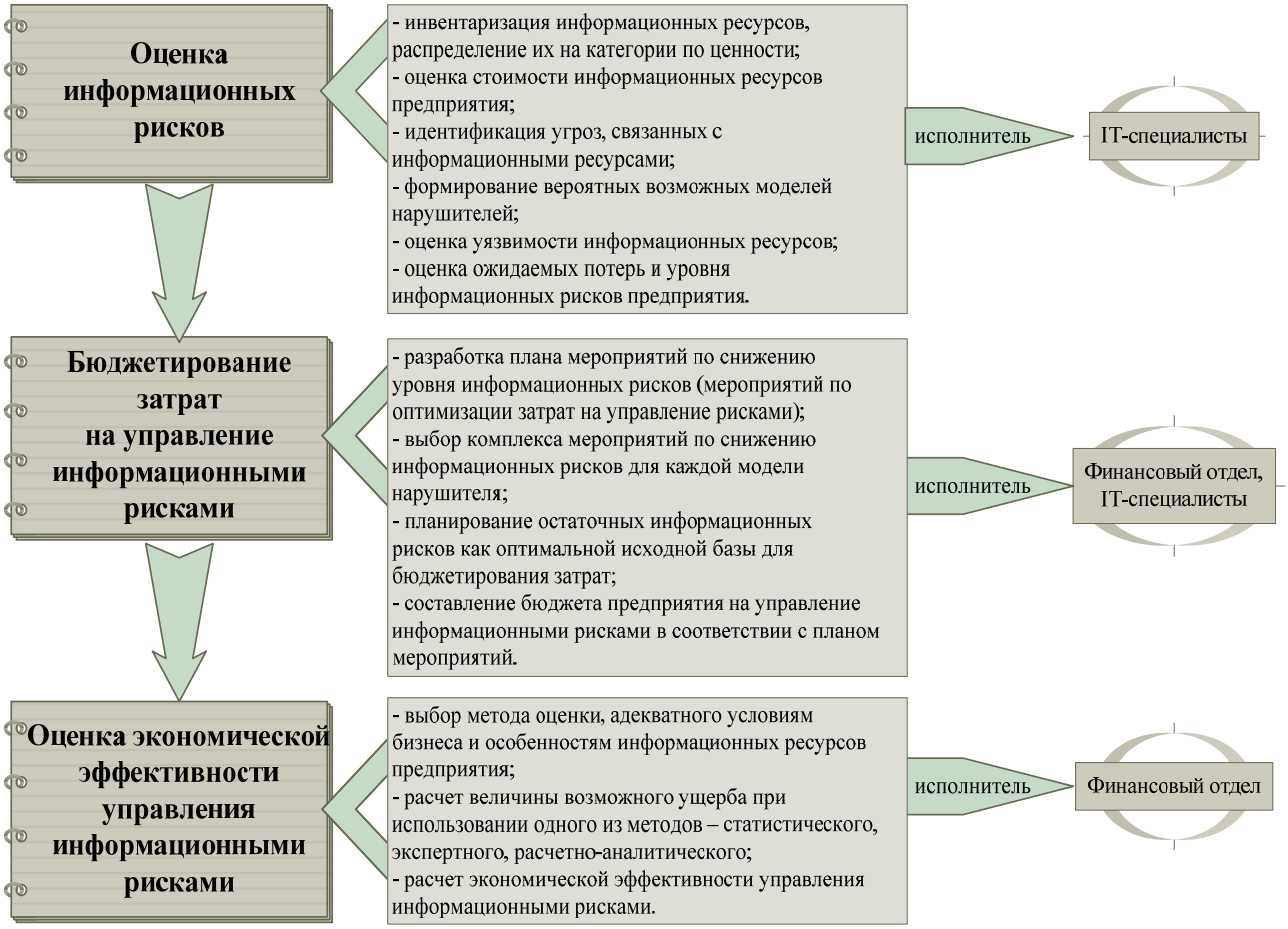

Рис. 1. Методика управления ИР предприятия

формационных ресурсов. Каждому из выбранных мероприятий характерны следующие уровни защиты информационных ресурсов: низкий, средний, высокий, которые могут быть реализованы путем соответствующего финансирования запланированных мероприятий по следующим вариантам: «дешевым», «бюджетным», «дорогим».

Заключительным этапом методики управления ИР предприятия является расчет экономической эффективности запланированных затрат на снижение рисков. Исходя из того, что все приемлемые меры безопасности необходимы для уменьшения среднестатистических убытков от реализации угроз по отношению к информационным ресурсам до приемлемой величины, предложено экономическую эффективность реализации мероприятий по снижению ИР определять по формуле:

$$Э = \frac{\Delta ЭУ - БЗ_{ИР}}{БЗ_{ИР}} \cdot 100\%,$$

где $Э$ – экономическая эффективность от реализации мер снижения ИР; $\Delta ЭУ$ – снижение ожидаемого экономического ущерба, что возможно за счет уменьшения суммарных остаточных рисков; $БЗ_{ИР}$ – бюджет затрат на управление ИР.

Снижение ожидаемого экономического ущерба, в свою очередь, можно рассчитать следующим образом:

$$\Delta ЭУ = ЭУ\left(1 - \frac{\sum\limits_i ИР_i^{ост}}{\sum\limits_i ИР_i^{нач}}\right),$$

где $ЭУ$ – ущерб от реализации угроз информационным ресурсам предприятия; i – индекс вида ИР; $ИР_i^{ост}$ – уровень i-го остаточного ИР; $ИР_i^{нач}$ – уровень i-го исходного (начального) ИР.

В вышеприведенных формулах определения $Э$ и $\Delta ЭУ$ для расчетов используется показатель уровня остаточного риска, что требует разъяснения сущности этого термина. Согласно работе [14], остаточным есть риск, который остается после обработки, приемлемый для предприятия риск. Под обработкой риска в данном случае понимается применение определенных мер по снижению его величины. Следует отметить, что среди всех выявленных рисков, обработке подвергаются лишь те, начальное значение которых выше порогового (целевого) значения, представляющего собой количественное выражение уровня безопасности информационных ресурсов, требуемого для каждого конкретного предприятия. Чем выше целевой уровень информационной безопасности, тем больше усилий и средств требуется на создание и сопровождение соответствующей системы управления информационной безопасностью [10].

Таким образом, показатель $\Delta ЭУ$ – это, по сути, экономия, достигнутая в результате внедрения мероприятий по снижению ИР. Его можно интерпретировать как доход от деятельности по управлению ИР.

При положительной экономической эффективности $Э$ можно говорить о прибыльности деятельности по управлению ИР предприятия. При этом главный результат заключается в сокращении потерь и содействии бесперебойному функционированию основного бизнеса предприятия с помощью финансового управления.

Выводы

Исследование сущности ИР и методики управления ими на предприятии позволяет констатировать следующее:

1) ИР – ситуация, для которой характерна возможность получения убытков предприятия в результате применения информационных технологий;

2) при оценке ИР обязательно учитывается ценность информационных ресурсов;

3) ИР оцениваются в денежном выражении и означают возможные убытки;

4) управление ИР позволяет повысить прибыль предприятия за счет управления затратами на их снижение, что предполагает планирование затрат, финансирование и оценку экономической эффективности от реализации мер снижения ИР.

Список литературы

1. Баутов А. Эффективность защиты информации / Открытые системы. – 2003. – №7-8. – С. 23-26.
2. Кучер В.А. Сутність та принципи формування антикризової програми розвитку промислового підприємства / Наук. пр. Донец. нац. техн. ун-ту; Редкол.: Дементьєв В.В. (голова) та інш. – Донецьк: ДонНТУ, 2011. – Т.2, №39. – С. 163-167. (серія: Економічна).
3. Информационные системы и технологии: приложения в экономике и управлении: учеб. пособие. Кн.6. / Под ред. Ю.Г. Лысенко. – Донецк: ООО «Юго-Восток, Лтд», 2004. – 377 с.
4. Скрипкин К.Г. Экономическая эффективность информационных систем. – М.: ДМК Пресс, 2010. – 256 с.
5. Донець Л.І. Економічні ризики та методи їх вимірювання: навч. посіб. – К.: Центр навч.

літ, 2006. – 312 с.
6. Ілляшенко С.М. Економічний ризик: навч. посіб. – К.: Центр навч. літ, 2004. – 220 с.
7. Бланк И.А. Финансовый менеджмент. – К.: Эльга, Ника-Центр, 2004. – 656 с.
8. Warren A.C. Engineering Safe and Secure Software Systems. – Boston: Artech House, 2013. – 326 p.
9. Годовой отчет Cisco по безопасности за 2015 год. – Сан-Хосе (США), Сингапур, Амстердам (Нидерланды): Cisco Systems. – 2015. – 53 с.
10. Miller D.R., Shon H. Security Information and Event Management (SIEM) Implementation. – New York (USA): Mc Graw Hill, 2011. – 465 p.
11. Bohme R. The Economics of Information Security and Privacy. – Berlin: Springer-Verlag, 2013. – 321 p.
12. Ольхович Е.А. Финансовые методы управления информационными рисками предприятия / Вестник РЭА. – 2008. – №1. – С. 12-16.
13. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IES 27002:2005, MOD). – К.: НБУ, 2010. – 149 с. – (Галузевий стандарт України).
14. ГСТУ СУІБ 1.0/ISO/IES 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IES 27001:2005, MOD). – К.: НБУ, 2010. – 49 с. – (Галузевий стандарт України).

A.A. Tkachev
Donetsk National Technical University (Donetsk)

INFORMATION RISKS MANAGEMENT AT AN ENTERPRISE IN VIEW OF COST-EFFECTIVENESS OF THEIR REDUCTION

Background. *In the last years, there has been a growing number of violations of information security and increasing severity of their consequences, which determines the topicality and practical importance of the given investigation.*
Materials and/or methods. *The theoretical basis of this research is presented by the scientific publications by native and foreign scientists on the evaluation of information risks and the provision of the industrial information security.*
Results. *The investigation of the essence of information risks and their control methods at the enterprise allows ascertaining that economic efficiency is by and large the economy attained as a result of the introduction of techniques aiming at information risks reduction. It can be interpreted as the income received from the information risk management activity. One can talk about profitability of the information risks management activity of an enterprise, given the economic efficiency is positive. Herein, the key result is to reduce losses and to ensure regular functioning of the core enterprise activity by means of the financial control.*
Conclusion. *Information risk is a situation that enables enterprise losses because of the information technology application. While assessing information risks, the value of information sources is taken into consideration. Information risks are estimated in money terms and imply possible losses. Information risks management means cost management of their reduction, which suggests cost planning, financing and evaluating their efficiency.*

Keywords: *information risk, threat identification, reduction of economic damage.*

Сведения об авторах
А.А. Ткачев
Телефон: +380 (50) 972-84-09
Эл. почта: tkachev.mail@yandex.ua

Статья поступила 08.12.2015 г.

Рецензент д.э.н., проф. В.А. Кучер