Методика оценки рисков информационной безопасности экономических информационных систем электронной коммерции

© 2014 Тищенко Евгений Николаевич
доктор экономических наук
© 2014 Капустина (Строкачева) Ольга Александровна
кандидат экономических наук, доцент
Ростовский государственный экономический университет (РИНХ)
344002, Ростов-на-Дону, ул. Б. Садовая, д. 69
E-mail: celt@inbox.ru, 0666@list.ru

Статья написана на основе материала, опубликованного авторами в[1], и посвящена изменениям, касаемым информационной безопасности, и анализу рисков экономических информационных систем в сфере электронной коммерции за последние несколько лет.

Ключевые слова: информационная безопасность, риски, электронная коммерция.

Безопасность на сегодняшний день является ключевым вопросом при внедрении и использовании систем электронной коммерции (ЭК). Под ЭК понимается технология, которая обеспечивает полный замкнутый цикл операций, включающий заказ товара (услуги), проведение платежей, участие в управлении доставкой товара (выполнения услуги). Эти операции проводятся с использованием электронных средств и информационных технологий и обеспечивают передачу прав собственности или прав пользования одним юридическим (физическим) лицом другому[2].

Объективно оценить текущее состояние информационной безопасности компании, а также ее адекватность поставленным целям и задачам бизнеса с целью увеличения эффективности и рентабельности экономической деятельности организации суть основные задачи аудита информационной безопасности. Поэтому под термином "анализ защищенности экономических информационных систем электронной коммерции" будем понимать системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности экономической системы в соответствии с определенными критериями и показателями безопасности[3].

Многообразие представленных на рынке средств и методов анализа защищенности экономических информационных систем электронной коммерции (ЭИСЭК), отсутствие математической основы и научного базиса позволили сделать вывод об актуальности исследуемого вопроса.

Трудно переоценить значимость обеспечения безопасности при пользовании ресурсами Интернета с персональных компьютеров или мобильных устройств. По опросам, Россия занимает первое место по количеству жертв киберпреступлений среди частных лиц. За 2013 г. общий ущерб от кибератак составил 1,48 млрд долл. За 2012 г. 85% пользователей Интернета в России подвергались вирусным или иным атакам[4].

В связи с вышеизложенным на сегодня аудит информационной безопасности (ИБ) экономических информационных систем (ЭИС) при ведении бизнеса с помощью интернет-технологий все еще актуален.

Целями проведения аудита безопасности систем ЭК являются:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
- оценка текущего уровня защищенности ЭИСЭК;
- локализация узких мест в системе защиты ЭИСЭК;
- оценка соответствия ЭИСЭК существующим стандартам в области информационной безопасности;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ЭИСЭК;
- разработка политик безопасности и других организационно-распорядительных документов по защите информации и участие в их внедрении в работу организации;
- участие в обучении пользователей и обслуживающего персонала ЭИСЭК вопросам обеспечения информационной безопасности;
- участие в разборе инцидентов, связанных с нарушением информационной безопасности.

Работы по аудиту безопасности ЭИСЭК включают в себя ряд последовательных этапов, которые в целом соответствуют этапам проведения комплексного ИТ-аудита автоматизированной системы, включающего в себя следующее:

- инициирование процедуры аудита;
- сбор информации аудита;
- анализ данных аудита;
- выработка рекомендаций;
- подготовка аудиторского отчета.

Подход к проведению аудита безопасности может базироваться на анализе рисков, опираться на использование стандартов информационной безопасности либо объединять оба эти подхода.

В настоящее время имеется большое разнообразие как методов анализа и управления рисками, так и реализующих их программных средств[5], которые за последние несколько лет изменились: CRAMM, RiskWatch, COBRA, Buddy System, КЭС, VS Risk, RTA, RSA Archer, Modulo Risk Manager, RM Studio, RA2 art of risk, Callio Secura 17799, Method Ware Proteus, РискМенеджер[6].

С точки зрения анализа рисков информационной безопасности к основным активам относятся: непосредственно информация, инфраструктура, персонал, имидж и репутация компании. Без инвентаризации активов на уровне бизнес-деятельности невозможно ответить на вопрос, что именно нужно защищать. Очень важно понять, какая информация обрабатывается в организации и где выполняется ее обработка.

В условиях крупной современной организации количество информационных активов может быть очень велико. Если деятельность организации, связанной с ЭК, автоматизирована при помощи ERP-системы, то можно говорить, что практически любому материальному объекту, использующемуся в данной деятельности, соответствует какой-либо информационный объект. Поэтому первоочередной задачей управления рисками становится определение наиболее значимых активов.

Решить указанную задачу невозможно без привлечения менеджеров основного направления деятельности организации как среднего, так и высшего звена. Оптимальна ситуация, когда высший менеджмент организации лично задает наиболее критичные направления деятельности, для которых крайне важно обеспечить информационную безопасность. Мнение высшего руководства по поводу приоритетов в обеспечении информационной безопасности очень важно и ценно в процессе анализа рисков, но в любом случае оно должно уточняться путем сбора сведений о критичности активов на среднем уровне управления компанией. При этом дальнейший анализ целесообразно проводить именно по обозначенным высшим менеджментом направлениям бизнес-деятельности. Полученная информация обрабатывается, агрегируется и передается высшему менеджменту для комплексной оценки ситуации.

Идентифицировать и локализовать информацию можно на основании описания бизнес-процессов, в рамках которых информация рассматривается как один из типов ресурсов. Формализованные описания бизнес-процессов служат хорошей стартовой точкой для инвентаризации активов. Если описаний нет, можно идентифицировать активы на основании сведений, полученных от сотрудников организации. После того как активы идентифицированы, необходимо определить их ценность.

Работа по определению ценности информационных активов в разрезе всей ЭИСЭК одновременно наиболее значима и сложна. Именно оценка информационных активов позволит начальнику отдела информационной безопасности выбрать основные направления деятельности по ее обеспечению.

Ценность актива выражается величиной потерь, которые понесет ЭИСЭК в случае нарушения безопасности актива. Но экономическая эффективность процесса управления информационной безопасностью во многом зависит именно от осознания того, что нужно защищать и какие усилия для этого потребуются, так как в большинстве случаев объем прилагаемых усилий прямо пропорционален объему затрачиваемых денег и операционных расходов. Управление рисками позволяет правильно их оценивать и оптимизировать, если это возможно.

Чтобы определить последствия нарушения безопасности, нужно либо иметь сведения о зафиксированных инцидентах аналогичного характера, либо провести сценарный анализ. В рамках сценарного анализа изучаются причинно-следственные связи между событиями нарушения безопасности активов и последствиями этих событий для бизнес-деятельности организации. Последствия сценариев должны оцениваться несколькими людьми итерационным или совещательным методом. Следует отметить, что разработка и оценка таких сценариев не может быть полностью оторвана от реальности. Всегда нужно помнить, что сценарий должен быть вероятным. Критерии и шкалы определения ценности индивидуальны для каждой организации. По результатам сценарного анализа можно получить информацию о ценности активов.

Если активы идентифицированы и определена их ценность, можно говорить о том, что цели обеспечения информационной безопасности частично установлены: определены объекты защиты и значимость поддержания их в состоянии информационной безопасности для организации[7]. Далее приведена модифицированная схема взаимосвязи управления рисками в ЭИСЭК (см. рисунок).

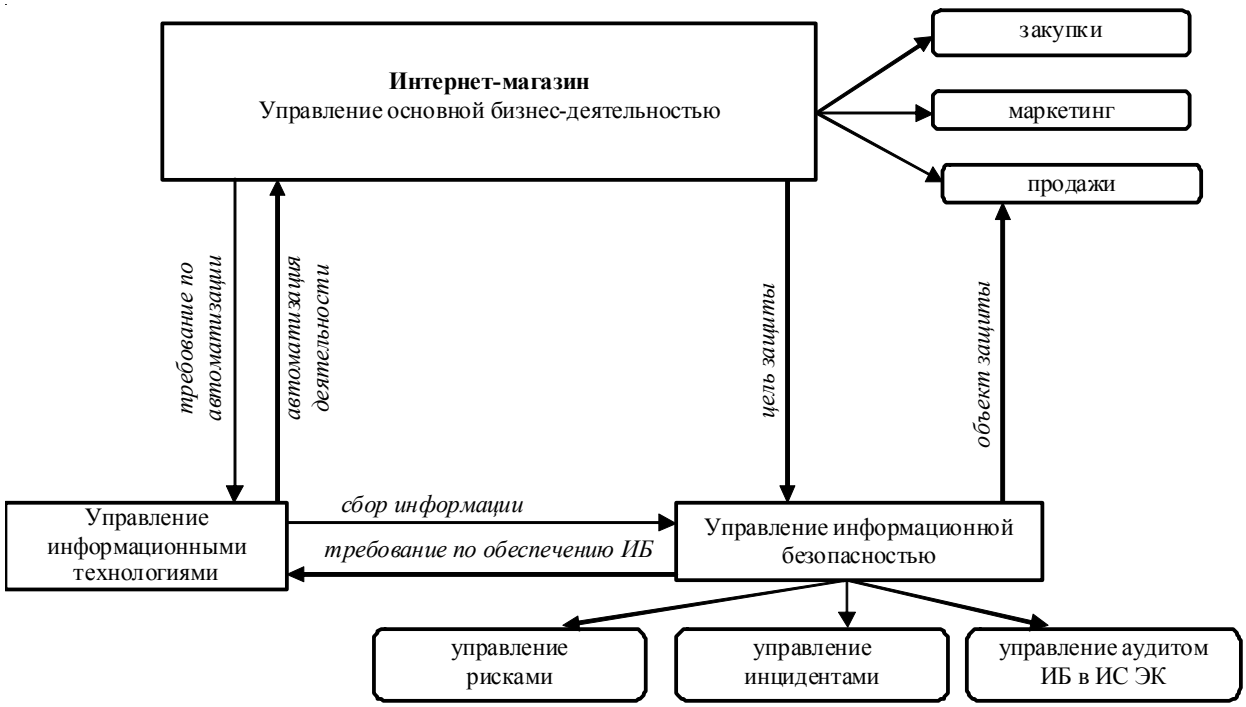

Рис. **Схема взаимосвязи управления рисками в ЭИСЭК**

Изучив существующие методики анализа рисков, авторы модифицировали методику, предложенную[8], путем применения ее в сфере ЭИСЭК. Было выделено поэтапное разделение процесса анализа рисков. Этапы алгоритма методики анализа ЭИСЭК рисков заключаются в следующем.

На начальным этапе оценки рисков необходимо получать данные оценки от большего количества экспертов. И для определения "вклада" ответов конкретного эксперта требуется определить "вес" каждого эксперта.

На данном этапе эксперт, выполняющий оценку рисков, должен представить данные о себе, чтобы сформировать вес Y_s (степень доверия к эксперту). Расчет веса *s*-го эксперта производится по следующей формуле:

$$Y_s = \left(\sum_{l=0}^{L} Y_s^l \right) / l \,, \qquad (1)$$

где Y_s^l - значение компонента веса, для всех компонентов используется шкала (от 0,1 до 1). Предполагается следующий набор компонентов: Y_s^0 - учет опыта работы в области ИБ; Y_s^1 - учет повышений квалификации в области ИБ; Y_s^2 - учет связи работы эксперта с управлением инфраструктурой информационных систем; Y_s^3 - учет валидности оценок экспертов в сфере информационной безопасности ЭИСЭК.

Эксперт, выполняющий оценку рисков, указывает классы компонентов, присутствующих в инфраструктуре организации.

В соответствии с классификацией перечисляются все *ресурсы* в организации, и эксперт указывает оценки стоимости *C*, *D*, *K*. В соответствии с этими характеристиками рассчитывается стоимость ресурсов H_p по следующей формуле:

$$H_p = (U_1 \cdot C + U_2 \cdot K) / (U_1 + U_2 + U_3), \qquad (2)$$

где U_1, U_2, U_3 - значения весовых коэффициентов, подстраиваемых для каждой организации (от 0,1 до 1);
C - оценка стоимости ущерба для организации при разрушении ресурса;
K - оценка стоимости ущерба для организации при осуществлении несанкционированного доступа к ресурсу. Все значения стоимостей эксперт оценивает в рублях.

Для оценки стоимости служб эксперту необходимо сравнить, на сколько значение стоимости данной службы (например, электронной почты) больше или меньше, чем стоимость уже учтенных им ресурсов. Таким образом, значение стоимости для каждой службы H_c будет равно:

$$H_c = \begin{cases} H_p \cdot g, \text{если } H_c \rangle H_p \\ \dfrac{H_p}{g}, \text{если } H_c \langle H_p \end{cases}, \qquad (3)$$

где *g* - значение коэффициента, на сколько стоимость службы больше (меньше) стоимости ресурса.

Для всех ресурсов и служб, заданных на предыдущем этапе, эксперты оценивают вероятность и ущерб от реализации каждой угрозы.

Получение данных о вероятностях и ущербе мы будем производить не прямыми методами оценки вероятности, а используя метод анализа иерархий, для определения суждений эксперта о значении вероятности одной угрозы относительно другой.

Значения вероятностей и ущерба от реализации угроз для данного ресурса могут быть представлены векторами $\vec{P}$ для вероятности и для ущерба. При наличии M угроз для данного ресурса эксперту необходимо оценить отношения

для вероятностей угроз по шкале значимости от 1 до 9 (1 - вероятность событий p_i и p_j одинаковы; 9 - вероятность p_i угрозы i "намного выше", чем вероятность p_j угрозы j), где i, j - меняются от 1 до M. После оценки всех пар отношений для данного ресурса можно сформировать матрицу парных сравнений $A=\left(a_{ij}\right)=\left(\frac{p_i}{p_j}\right)$ для значений отношений вероятностей угроз.

Для матрицы парных сравнений A вектор значений вероятностей $\vec{P}$ можно найти, решив следующее векторное уравнение:

, (4)

где λ_{max} - наибольшее собственное значение матрицы;

$\vec{P}$ - собственный вектор матрицы.

Для вычисления значений вектора сначала необходимо найти - наибольшее собственное значение матрицы А. Для этого необходимо получить ненулевое решение уравнения:

$$\left(A-\lambda E\right)\cdot\vec{P}=0,$$

где E - диагональная единичная матрица.

А для этого должен быть равен нулю. Так как определитель матрицы $A-\lambda E$ равен нулю, то для нахождения необходимо решить характеристическое уравнение данной матрицы. Это может быть сделано с использованием численных методов.

Далее при известном значении λ_{max} вектор вероятностей $\vec{P}$ следует искать, решая векторное уравнение (4). Для обеспечения единственности решения надо учитывать, что часто необходимо иметь нормализованное решение, и поэтому следует заменить одно из уравнений

системы (4) на уравнение

$$\sum_{k=1}^{n} p_k = 1.$$

Для проверки согласованности полученных результатов необходимо использовать индекс согласованности. Индекс согласованности будет выражать "близость к согласованности", т.е. степень отклонения суждений эксперта друг от друга. Индекс согласованности рассчитывается по следующей формуле:

$$ИС=\frac{\left(\lambda_{max-M}\right)}{\left(M-1\right)}, \quad (5)$$

где M - количество угроз для данного ресурса. Малое значение индекса согласованности (меньшее или равное 0,1) свидетельствует о приемлемой степени согласованности суждений эксперта. Значение индекса согласованности больше 0,1 служит основанием для пересмотра суждений эксперта.

Аналогичным образом происходит вычисление значений ущерба для всех ресурсов, служб и организации в целом.

Далее подсчитываются результаты оценки угроз и определяются необходимые меры защиты. Для вычисления величины значения риска W_i для i-го ресурса службы или организации в целом (i=0) следует воспользоваться методом взвешенной суммы для агрегирования данных субъективных оценок разных экспертов:

$$\mathrm{W_i}=\sum_{s=1}^{S}\left(w_m^s\cdot Y_s\cdot H_i^s\right)/S, \quad (6)$$

где S - количество экспертов, принимавших участие в оценке;

Y_s - вес эксперта, определяемый на нулевом этапе;

значение стоимости данного ресурса, указанное s-м экспертом;

w_m^s - значение риска для данного ресурса, определенное s-м экспертом, рассчитываемое по следующей формуле:

$$w_m^s=\sum_{j=1}^{M} v_j^s\cdot p_j^s, \quad (7)$$

где M - общее количество учтенных угроз для данного ресурса;

v_j^s - величина ущерба, который может быть нанесен компоненту системы, при реализации угрозы j;

p_j^s - вероятность реализации угрозы j за месяц.

После расчета значений рисков для компонентов (ресурсов и служб) системы выводится информация об общем риске для компонентов и рисках отдельных угроз и градация компонентов по степени уязвимости в соответствии с этим значением.

И завершающий шаг на основании справочника стандарта BSI: определяется рекомендованный список мер уменьшения рисков угроз информационной безопасности для каждого из компонентов системы и для системы в целом.

При проведении оценки рисков информационной безопасности между началом исследования системы и выпуском итогового отчета проходит существенный период времени. Это значительно уменьшает ценность некоторых данных и может приводить к снижению уровня решения задач информационной безопасности по обеспечению конфиденциальности, целостности или доступности информации.

В данной связи в последние годы активно разрабатывается концепция непрерывного аудита. Непрерывный аудит определяется как среда, позволяющая внутреннему или внешнему аудитору выносить суждения по значимым вопросам, основываясь на серии созданных одновременно или с небольшим промежутком отчетов. Следовательно, являются актуальными проблема получения количественных оценок параметров информационной системы и проблема управления рисками информационной безопасности в автоматизированной системе с учетом возможностей:

- агрегации разнородных данных;
- обучения в процессе работы и уточнения оценок, полученных на предыдущих этапах анализа;
- использования неточных данных;
- автоматизации большинства процессов принятия решений.

Таким образом, необходимо синтезировать подход к получению количественной оценки и управлению рисками информационной безопасности в автоматизированной системе, учитывая вышеуказанные возможности[9].

В целях решения указанных задач необходимо синтезировать автоматическую систему, позволяющую полностью или частично автоматизировать процесс описания среды функционирования и вывода значений рисков.

В задаче анализа рисков априорная вероятностная информация о реализации угроз может быть изменена после получения новых экспертных оценок или в результате наблюдения соответствующих событий, связанных с состояниями и подтверждающих или опровергающих априорную информацию. Многие статистические задачи, независимо от методов их решения, обладают общим свойством: до того как получен конкретный набор данных, в качестве потенциально приемлемых для изучаемой ситуации должны рассматриваться несколько вероятностных моделей. После того как получены данные, возникает выраженное в некотором виде знание об относительной приемлемости этих моделей. Одним из способов “пересмотра” относительной приемлемости вероятностных моделей является байесовский подход, основой которого выступает теорема Байеса. Практическое применение этого подхода затруднено отсутствием данных об условных вероятностях событий. В связи с этим особо актуально развитие существующих методик оценки рисков информационной безопасности, а также создание новых подходов, позволяющих обеспечить оценку риска информационной безопасности в реальных условиях эксплуатации автоматизированных систем.

---

[1] *Тищенко Е.Н., Строкачева О.А.* Модель аудита информационной безопасности систем электронной коммерции // Научная мысль Кавказа / Северо-кавказский научный центр высшей школы. 2006. № 14 (98). Приложение.

[2] *Волокитина А.В.* Электронная коммерция / под ред. Л.Д. Реймана. М., 2002.

[3] *Лукацкий А.В.* Обнаружение атак. 2-е изд., перераб. и доп. СПб., 2003.

[4] Информационная безопасность в Интернете. URL: http://www.garant.ru/infografika/510581.

[5] *Тищенко Е.Н., Строкачева О.А.* Указ. соч.

[6] См.: *Симонов С.* Технологии и инструментарий для управления рисками. URL: http://www.jetinfo.ru/2003/2/1/article1.2.20031103.html; Лаборатория системного анализа процессов информатизации ИСА РАН. URL: http://www.isprotection.da.ru; *Астахов А.* Анализ защищенности автоматизированных систем. URL: http://www.isaca.ru/security/Pubs/Pub1_AAM_SecEval.htm; *Бондаренко А.* Программное обеспечение для проведения оценки рисков. URL: http://www.securitylab.ru/blog/personal/secinsight/20280.php; Программные продукты для анализа рисков. URL: http://www.iso27000.ru/informacionnye-rubriki/upravlenie-riskami/programmnye-produkty-dlya-analiza-riskov.

[7] *Суханов А.* Анализ рисков в управлении информационной безопасностью. URL: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/analiz-riskov-v-upravlenii-informacionnoi-bezopasnostyu.

[8] *Лысов А.С.* Методические и программные средства анализа информационных рисков в деятельности органов государственного управления : дис. ... канд. техн. наук. Томск, 2008.

[9] *Атаманов А.* Вопросы анализа рисков ИБ при построении системы защиты конфиденциальной информации // Information Security / Информационная безопасность. 2012. № 1. URL: http://www.itsec.ru/articles2/pravo/voprosi-analiza-riskov-ib-pri-postroenii-sistemi.

Поступила в редакцию 04.06.2014 г.