Published in the Russian Federation
Sochi Journal of Economy
Has been issued since 2007.
ISSN: 1996-9005
Vol. 40, Is. 2, pp. 117-126, 2016

www.vestnik.sutr.ru

UDC 338.14 + 004.056

The Model of Information Security Audit in the Information Systems of E-Commerce Type of B2E

Vladlena S. Oladko

Volgograd State University, Russian Federation
400062, Volgograd region, Volgograd, University Avenue, 100
PhD (Engineering), Assistant Professor, Volgograd State University
E-mail: oladko.vs@yandex.ru

Abstract

The actual problem of information security in the electronic systems is considered in the article. The main functions and areas of application of e-commerce systems are indicated. Classification of e-commerce model is presented. One of the most popular models – B2E model allocated. The main categories of data that are processed in the B2E e-commerce systems and the risks that arise as a result of information security threats are investigated. The need for data protection in e-commerce systems, B2E is shown. It was concluded that the role of information security audit in the process of maintenance of protection and control system of the current state of security. The methodology of information security audit in the B2E offered. Formal audit model based on the use of security profile, risk assessment and the initial security system developed.

Keywords: e-commerce, risk, damage, information security, threat, audit, security profile, protection system.

Введение

Электронная коммерция является современной, стремительно растущей и активно развивающейся отраслью экономики. По данным [1], наиболее активно электронная коммерция применяется в таких отраслях как: высокотехнологичное производство; управление бизнес-процессами; финансовый сервис; оптовая и розничная торговля; гостиничный бизнес и туризм; телекоммуникации; государственные услуги и закупки; реклама и маркетинг; транспорт. Так по данным Synovate Comcon, в настоящий момент 58 % пользователей рунета прибегают к услугам электронной коммерции

Анализ источников [1, 2] показывает, что подобная популярность в первую очередь связана:

–с существенным сокращением затрат на проведение маркетинга и торговых операций (транзакционных издержек);

–с решением проблемы расстояний;

–созданием условий для прямых контактных отношений с взаимодействующими сторонами;

–с возможностью совершения покупок с мобильных устройств;

–с предоставлением конкурентных преимуществ на мировом рынке для малых и средних предприятий;

– повышением прозрачности рынков: покупатели и продавцы практически мгновенно могут получать информацию о ценах на продукцию, условиях поставки, предлагаемых конкурирующими фирмами.

Однако, вместе с увеличением темпов роста электронной коммерции увеличивается также число компьютерных преступлений и инцидентов информационной безопасности в данной сфере. Анализ [3, 4] позволяет сделать вывод о том, что число активных угроз с 2010 к 2016 году увеличилось в 2 раза и экономический ущерб от подобных инцидентов колеблется в диапазоне от 250 тысяч до 60 млн. рублей. Следовательно, для предотвращения или снижения тяжести от подобных последствий необходимо предпринимать меры по защите от угроз информационной безопасности. Согласно законодательству Российской Федерации [5] данные меры могут носить организационный, технический и программно-аппаратный характер и реализовываться в виде единой системы защиты информации (СЗИ) на предприятии. Состав, функции и сложность СЗИ будет завесить от типа обрабатываемой информации, требований регуляторов (ФСБ России, ФСТЭК России, Роскомнадзор, Банк России и др.) к минимальному уровню защищенности и финансовых возможностей предприятия. Целью СЗИ является противодействие актуальным угрозам, снижение рисков информационной безопасности и обеспечение требуемого уровня защищенности на протяжении всего периода существования СЗИ на предприятии. Как правило, задачи контроля рисков и уровня защищенности решаются в рамках аудита информационной безопасности, который проводится на периодической основе и может быть как внутренним, осуществляемым самим предприятием, так и внешним, осуществляемым специализированными организациями и подразделениями регуляторов. При этом актуально решение задач, связанных с разработкой методики и инструментальных средств проведения внутреннего аудита информационной безопасности в системах электронной коммерции. Это обусловлено тем, что в настоящее время в документах, регламентирующих защиту информации в электронной коммерции не существует обязательных к исполнению, четких правил проведения аудита информационной безопасности и методик расчета рисков и уровня защищенности.

Материалы и методы

Для написания данной статьи были использованы материалы научной, учебной литературы, законодательство Российской Федерации, статистические данные, собранные из печатных и электронных источников информации.

В качестве основных методов исследования при выполнении работы были использованы: метод описания, системного анализа, аналогии и обобщения, а также элементы теории множеств и логики нечетких высказываний.

Проблемы безопасности информации в системах электронной коммерции вида B2E

В настоящее время существуют различные модели организации систем электронной коммерции, при классификации которых учитывается область применения, архитектура и принципы функционирования, см. рис. 1. По данным [6] наибольшая доля систем электронной коммерции приходится на модели вида B2E – 48 %, поэтому именно они будут рассматриваться в данной работе.

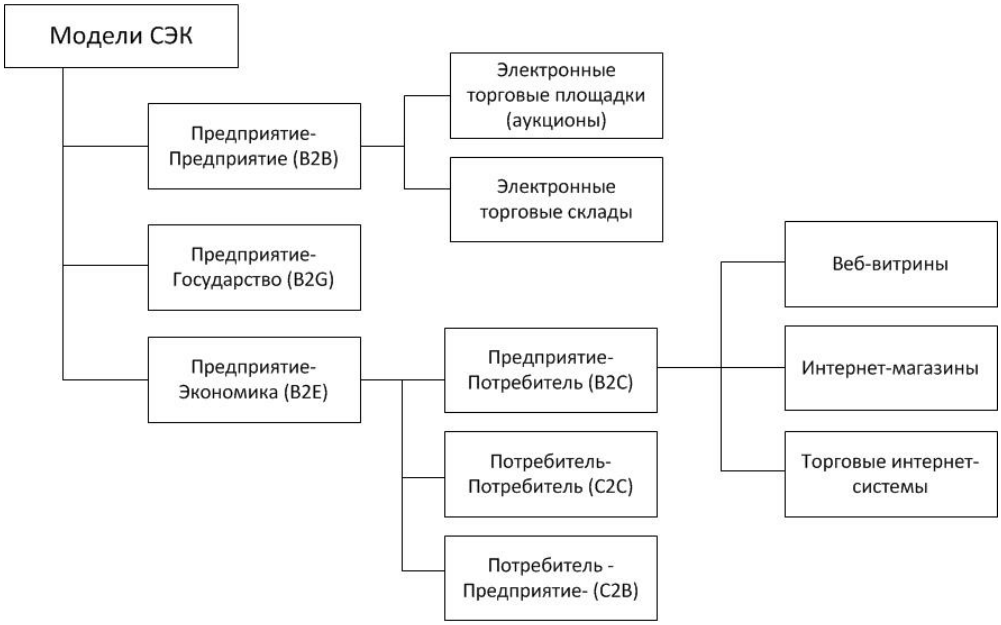

Рис. 1. Классификация моделей электронной коммерции.

Модель электронной коммерции B2E (Business-to-Employee) – бизнес-модель, включающая электронный обмен данными между организацией и ее сотрудниками. Представляет собой внутрикорпоративную систему электронного бизнеса, позволяющую организовывать работу персонала организации и вести совместную бизнес-деятельность сотрудников, отдельных структур или подразделений. При организации взаимодействия используются ресурсы внутрикорпоративной сети организации и глобальной сети интернет. Основными подсистемами информационной системы электронной коммерции (ИСЭК) модели B2E (см. рис. 2) являются:

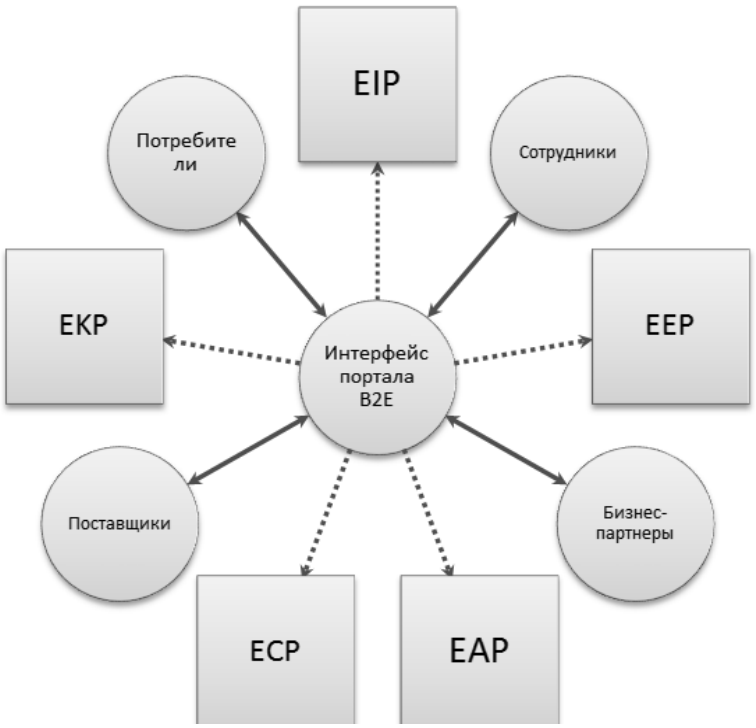

Рис. 2. Архитектура ИСЭК модели B2E

–EIP (Enterprise Information Portal) – корпоративный информационный портал.

–EEP - (Enterprise Expertise Portals) – корпоративный экспертный портал, обеспечивающий связь между пользователями на основе их знаний.

–EAP (Enterprise Application Portal) – корпоративный портал приложений.

–ECP (Enterprise Collaboration Portal) – корпоративный портал совместной работы, автоматизирует бизнес-процессы.

–EKP (Enterprise Knowledge Portal) – корпоративный портал управления знаниями. Охватывает все перечисленные выше порталы.

Образуя единое пространство, выделенные подсистемы ИСЭК обеспечивают выполнение следующих функций:

–обеспечение непрерывного взаимодействия сотрудников организации, поставщиков, финансовых организаций, потребителей, партнеров с соответствующим разграничением доступа;

–обеспечение доступа к корпоративной информации, в том числе к приказам, новостям, нормативно-справочным данным;

–обработка, хранение и передача информации;

–автоматизация бизнес-процессов;

–управление транзакциями;

–управление и обеспечение коллективной работы;

–осуществление переводов и платежей;

–построение системы управления знаниями организации.

–интеграция приложений, превращение портала в единую точку доступа ко всем корпоративным системам и ресурсам.

При выполнении каждой функции используются данные, сервисы и информационные ресурсы ИСЭК, безопасность которых может быть нарушена в результате деструктивных воздействий случайного характера и/или деятельности злоумышленника. В результате подобных нарушений, по данным [3], в 58 % случаях, для организаций владельцев ИСЭК, наблюдается отрицательный экономический эффект, связанный с ростом финансовых издержек, нарушением непрерывности деятельности, потере репутации, клиентов и конкурентоспособности на рынке услуг. Поэтому для обеспечения стабильной работы информационной инфраструктуры ИСЭК, непрерывности бизнес-процессов, конфиденциальности, доступности и целостности информации необходимо применять средства защиты информации. При этом выбор состава средств защиты информации будет зависть от ряда факторов [7]:

–требования регуляторов к уровню защищенности категории обрабатываемой в ИСЭК информации;

–финансовые возможности организации владельца ИСЭК;

–стоимость защищаемой информации и информационной инфраструктуры;

–уровень рисков, связанных с воздействием угроз и дестабилизирующих факторов.

В таблице 1 представлено описание типовых ресурсов, подлежащих защите в ИСЭК и возможные риски, вязанные с успешной реализацией угроз информационной безопасности.

Таблица 1. Ресурсы и активы, подлежащие защите в ИСЭК

Ресурсы и активы	Категория ценности	Виды рисков
платежные данные	конфиденциальная информация	Финансовые потери, снижение репутации, отзыв лицензии регуляторами
финансовые средства и их электронные заместители	конфиденциальная информация	Финансовые потери, снижение репутации, отзыв лицензии регуляторами
данные о транзакциях	конфиденциальная информация	Финансовые потери, снижение репутации, наложение регуляторами штрафа за нарушение

персональные и идентификационные данные пользователей и сотрудников	персональные данные	Финансовые потери, снижение репутации, наложение регуляторами штрафа за нарушение
коммерческая тайна компании	коммерческая тайна	Финансовые потери, снижение репутации, предупреждение от регуляторов
бизнес-процессы	информация для служебного пользования, конфиденциальная информация и коммерческая тайна	Финансовые потери, падение конкурентоспособности, снижение репутации, предупреждение от регуляторов
информационная инфраструктура и критичные сервисы	для служебного пользования, конфиденциальная информация и коммерческая тайна	Финансовые потери, снижение репутации, падение конкурентоспособности, предупреждение от регуляторов

Применение специализированных технических, программных и аппаратных средств защиты регламентируется регуляторами в области безопасности информационных технологий и платежных систем. А для контроля над эффективностью средств, используемых в рамках единой системы защиты ИСЭК необходимо на периодической основе осуществлять мониторинг и аудит состояния безопасности и проводить оценку степени выполнения организацией требований по защите.

Формализованная модель проведения аудита информационной безопасности

В данной работе автором предлагается модель проведения аудита информационной безопасности, которая учитывает специфику ИСЭК (см. рис.3) и использует в процессе оценки соответствия системы уровню безопасности базис в виде профиля защиты, который сравнивается с «эталоном».

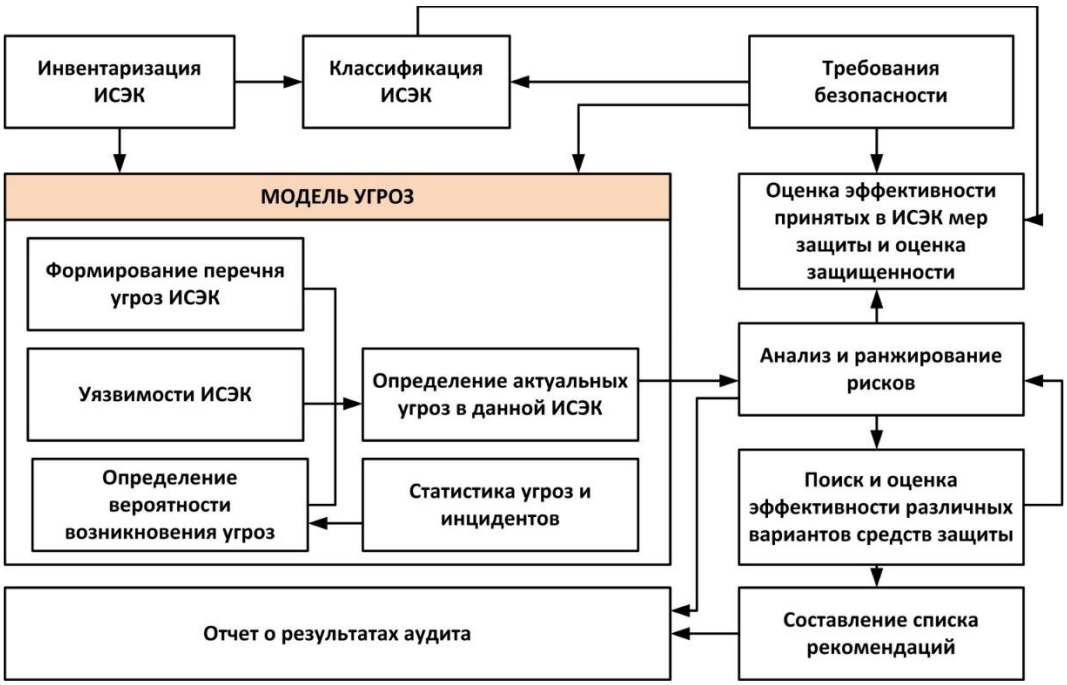

Рис. 3. Модель аудита информационной безопасности в ИСЭК B2E

В общем виде процесс проведения аудита информационной безопасности согласно данной модели можно описать тремя основными этапами, каждый из которых включает последовательность из нескольких шагов.

Этап 1. Сбор данных, о системе подлежащий аудиту информационной безопасности.

1. Ввод систематизация и хранение необходимой информации об организации, ее структуре, типе данных и процессах обработки данных, средствах вычислительной техники, информационных системах и принятых мерах по защите информации.

2. Выделение объектов защиты и классификация ИСЭК.

3. Идентификация и оценка параметров угроз информационной безопасности. На этом шаге формируется перечни угроз информационной безопасности, уязвимостей присущих ИСЭК, вероятностей проявления угроз, составляется модель потенциального злоумышленника и модель угроз.

Этап 2. Оценка состояния системы.

1. Анализ рисков.
2. Оценка эффективности принятых мер защиты.
3. Оценка защищенности.

Этап 3. Формирование отчета и выдача рекомендаций.

1. Выдача заключения о степени соответствия проверяемой организации критериям аудита ИБ. Составление протоколов несоответствия.
2. Априорная оценка эффективности различных вариантов построения системы защиты. Анализ рисков. Выдача рекомендаций.

На основе разработанной выше модели проведения аудита информационной безопасности в ИСЭК было разработано формализованное описание аудита ИСЭК, в основе которой лежит теория множеств и логика нечетких высказываний. В соответствие с данным математическим аппаратом общую модель аудита информационной безопасности в ИСЭК можно представить в виде следующего множества, см. формулу 1.

$$M_{AISPD} = \{Pisec, \{RIS\}, MT, MC, Risk, RPT\}, \quad (1)$$

где *Pisec* –профиль проверяемой ИСЭК, составляется на основе собранных характеристик; *{RIS}* – множество требований к защите ИСЭК различных классов, на основе которых составляется «эталонный» профиль системы; *MT* – модель угроз в аудируемой ИСЭК; *MC* – модель нарушителя в ИСЭК; *Risk* – риски в ИСЭК; *RPT* – сформированный отчет о результатах проведения аудита ИСЭК;

Реальный профиль ИСЭК формируется на основе результатов сбора информации об аудируемой ИСЭК, результатах ее классификации, а так же средств и мер защиты информации, имеющихся в данной ИСЭК, описывается следующим кортежем:

$$Pisec=\{\{O\}, \{SP\}, \{SS\}, Class, ILP\}, \quad (2)$$

где *{O}* – множество объектов ИСЭК, $o_i \in \{O\}, i = 1..n$, где n общее количество объектов; *{SP}* – множество характеристик ИСЭК; {SS} – множество средств и методов защите, реализованных в ИСЭК; *Class* – класс ИСЭК; *ILP* – уровень исходной защищенности в ИСЭК представляет собой обобщенный показатель, зависящий от технических и эксплуатационных характеристик, применяется при составлении модели актуальных угроз МТ и в соответствии с [9] описывается множеством базовых значений $ILP=\{высокий, средний, низкий\}=\{Y_{11}, Y_{12}, Y_{13}\}=\{0, 5, 10\}$.

Множество, описывающее модель угроз задается следующим образом:

$$MT=\{\{T\}, \{AT\}\}, \quad (3)$$

где *{T}*- множество возможных угроз для ИСЭК, полученное в результате сбора данных о ИСЭК. Каждая потенциальная угроза $T_j \in \{T\}, j = 1..m$, где m – количество угроз, характеризуется следующим кортежем (4):

$$T_i = \{PT, RT, DT\} \quad (4),$$

где *PT*- частота (вероятность) реализации угрозы, определяется экспертным путем, характеризует, насколько вероятным является реализация конкретной угрозы безопасности для данной ИСЭК в складывающихся условиях обстановки. Описывается множеством базовых значений $PTY = \{маловероятно, низкая\ вероятность, средняя\ вероятность, высокая\ вероятность\}=\{0, 2, 5, 10\}$; *RT* - реализуемость угрозы, описывается множеством базовых значений $RTY= \{низкая, средняя, высокая, очень\ высокая\}=\{Y_{31}, Y_{32}, Y_{33}, Y_{34}\}$. На основании [8] коэффициент реализуемости угрозы RT_i будет определяться

соотношением (5).

$$RT = \frac{ILP + PT}{20}, \quad (5)$$

$$Если\ 0 \le RT \le 0.3,\ RT_j = Y_{31}$$
$$Если\ 0.3 < RT \le 0.6,\ RT_j = Y_{32}$$
$$Если\ 0.6 < RT \le 0.8,\ RT_j = Y_{33}$$
$$Если\ 0.8 < RT,\ RT_j = Y_{34}$$

DT- показатель опасности для каждой угрозы, формируется экспертным путем, характеризуется множеством базовых значений *DTY={низкая, средняя, высокая} = {Y_{41}, Y_{42}, Y_{43}}*.

{AT}- множество актуальных угроз для ИСЭК, является подмножеством потенциальных угроз $\{AT\} \subseteq \{T\}$. Каждая актуальная угроза $AT_k \in \{AT\}, k = 1..d$, где d – число актуальных угроз, d≤ m, отбирается в соответствии с [9], по следующему правилу, описанному в соответствии с системой нечетких высказываний $\widetilde{L^1}$:

$$\widetilde{L^1} = \begin{cases} \widetilde{L_1^{(1)}}: < \text{ЕСЛИ}\ \ E_{13}\ \text{ТО А} > \\ \widetilde{L_2^{(1)}}: < \text{ЕСЛИ}\ E_{22}\ \text{ИЛИ}\ E_{23}\ \text{ТО А} > \\ \widetilde{L_3^{(1)}}: < \text{ЕСЛИ}\ \ E_{31}\ \text{ИЛИ}\ E_{32}\ \text{ИЛИ}\ E_{33}\ \ \text{ТО А} > \\ \widetilde{L_4^{(1)}}: < \text{ЕСЛИ}\ \ E_{41}\ \text{ИЛИ}\ E_{42}\ \text{ИЛИ}\ E_{43}\ \ \text{ТО А} > \end{cases} \quad (8)$$

Eij – высказывание вида*: <RT есть Y_{3i} и DT есть Y_{4j}>*

А – высказывание вида: *<{AT}={AT}+T_i> (<T_i включается в {AT}>)*

Модель злоумышленника описывается следующим кортежем:

$$MC = \{TC, AT\}, \quad (9)$$

где ТС – множество злоумышленников различного типа. Каждый тип злоумышленника может реализовать для ИСЭК различные виды и количество актуальных угроз из множества {АТ}.

Для расчета риска нарушения информационной безопасности в ИСЭК в количественной (денежной форме) используется методика, основанная на методики расчета риска описанной в РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» [10]. Оценка риска нарушения ИБ в ИСЭК (Risk) проводится в количественной форме на основе количественных оценок:

–*P* – стоимость информации, обрабатываемой в ИСЭК выраженная в количественной денежной форме, вводится непосредственно оператором ИСЭК и определяется экспертным путем;

–*RT* – коэффициент реализуемости угрозы, выраженный в количественной форме.

И в зависимости от коэффициента реализуемости угрозы рассчитывается по следующему правилу, описанному формулой (10):

$$Risk(T_j) = \begin{cases} 0, \text{если RT}_j \le 0.3 \\ [0.01\text{P}; 0.2\text{P}], \text{если } 0.3 < \text{RT}_j \le 0.6 \\ [0.21\text{P}; 0.5\text{P}], \text{если } 0.6 < \text{RT} \le 0.8 \\ [0.51\text{P}; \text{P}], \text{если RT} > 0.8 \end{cases} \quad (10)$$

Рассчитанные для каждой угрозы риски, в соответствие с [11] можно разделить на 4 основных класса:

1) риск отсутствует (Risk=0);
2) риск низкий и является допустимым ($Risk \in [0.1P; 0.2P]$);
3) риск средний и является недопустимым ($Risk \in [0.21P; 0.5P]$);
4) риск высокий и является недопустимым ($Risk \in [0.21P; 0.5P]$).

После того как была произведена оценка риска и его классификация для каждой актуальной угрозы, необходимо провести его обработку. Стратегии поведения относительно каждого риска, в зависимости от его класса выбираются следующим образом, см. таблицу 2.

Таблица 2. Стратегии обработки риска

№ п/п	Уровень риска	Способ обработки
1	Отсутствует или низкий	Принимается
2	Средний	Минимизируется за счет его страхования, передачи на аутсорсинг или отказа от использования ресурса
3	Высокий	Минимизируется за счет внедрения контрмер и дополнительных средств защиты

Множество рассматриваемых средств защиты информации в ИСЭК фиксировано и представляет собой *{SS} = {T, S},* где T - Категория к которой относится средства защиты информации, S – название средства защиты информации. Перечень средств защиты информации, используемой в дальнейшем при разработке программной модели составлен на основе данных Государственного реестра сертифицированных средств защиты информации.

В модели определены следующие типы связей:

–*MP* – имеется средство защиты, данный вид связи указывает, что для существующей актуальной угрозы в ИСЭК имеется средство противодействующее данной угрозе;

–*NMP* – нет средства защиты, данный вид связи показывает, что для существующей актуальной угрозы в СЗИ ИСЭК нет средства осуществляющего защиту от данной угрозы.

Отношение R^{TSS} задающее связи между средствами защиты информации в ИСЭК {SS} и множеством актуальных для данной ИСЭК угроз - {AT} представлено в виде матрицы:

$$R^{TSS} = \left|r_{ij}^{TSS}\right|, \text{ где}$$

r_{ij}^{TSS} - отображает наличие и тип связи между i-ой актуальной угрозой и j-ым средством защиты.

При этом $i \in \{AT\}$, а $j \in \{SS\}$, $r_{ij}^{TSS} \in \{MP, NMP\}$, MP, NMP - наличие связи типа определенного типа между i-ой актуальной угрозой и j-ым средством защиты.

Для элементов данной матрицы верно следующее:

$$r_{ij}^{TSS} = \begin{cases} MP, \text{если } i \text{ угроза закрывается } j \text{ средством защиты} \\ NMP, \text{если } i \text{ угроза не закрывается } j \text{ средством защиты} \end{cases}$$

Если для всех значений i=k, $r_{kj}^{TSS} = NMP$, то делается вывод о том, что в ИСЭК нет защиты от данной угрозы, и для повышения уровня защищенности ИСЭК необходимо в СЗИ ИСЭК добавить средство защиты от данного незакрытого вида угроз. Полученные данные помещаются в отчет о результатах аудита информационной безопасности (RPT) и выносятся в рекомендации.

Таким образом, в процессе проведения аудита происходит сопоставление реального профиля *Пisec* с множеством требований *{RIS}* которые предъявляются к защите информации в ИСЭК в зависимости от ее класса, типа ценных ресурсов, технико-эксплуатационных характеристик, уровня исходной защищенности и множества актуальных угроз. По результатам проведенного сравнения выявляются возможные несоответствия, оцениваются риски и выносятся рекомендации по управлению рисками и снижению негативного экономического эффекта.

Заключение

В системах электронной коммерции обрабатываются большие объёмы данных различной категории доступа, которые в соответствии с требованиями регуляторов в области информационной безопасности и платежных систем подлежат обязательной защите. Аудит информационной безопасности является одним из этапов реализации стратегии защиты информации в системе электронной коммерции. Аудит информационной безопасности проводится регулярной основе в соответствии с выбранной моделью. В данной работе предлагается модель проведения аудита информационной безопасности для систем электронной коммерции вида B2E. Разработанная модель, построена на анализе профиля защиты ИСЭК B2E и объединяет в себе несколько подходов к проведению аудита. Модель была автоматизирована и представлена в виде программного комплекса, который может быть использован лицом ответственным за информационную безопасность в качестве инструментального средства проведения внутреннего аудита информационной безопасности.

Примечания

1. Власова А.С. Электронная коммерция// Современные тенденции в экономике и управлении: новый взгляд. 2014. №26. С. 37-43.

2. Старцев М.В. Электронная коммерция как способ интенсификации бизнес-процессов // Социально-экономические явления и процессы. 2011. № 5–6. С.212 -215.

3. Абдеева З.Р. Проблемы безопасности электронной коммерции в сети интернет//Проблемы современной экономики. 2012. №1. С. 172-175.

4. Оладько В.С. Защита информации в системах электронной коммерции // Вестник УрФО. Безопасность в информационной сфере. 2015. № 3 (17). С. 17-22.

5. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 13.07.2015) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 10.01.2016) // Консультант Плюс.URL: http://www.consultant.ru/document /cons_ doc_LAW_61798/ (дата обращения 23.06.2016).

6. Вольфсон М. За прошлый год глобальный e-commerce вырос на 20%// E-business. URL: http://el-business.ucoz.ru/news/za_proshlyj_god_globalnyj_e_commerce_vyros_na_20 /2015-03-14-167 (дата обращения 21.06.2016).

7. Аткина В.С., Оладько А.Ю. Модель оценки безопасности систем электронной коммерции // Вестник компьютерных и информационных технологий. 2015. № 3 (129). С. 33-37.

8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год // ФСТЭК России. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380 (дата обращения 25.06.2016).

9. Аткина В.С. Применение карты рисков для оценки деструктивного воздействия существенной среды на информационную систему // Безопасность информационных технологий. 2013. № 4. С. 21-26.

10. Методика оценки рисков нарушения информационной безопасности // Обеспечение информационной безопасности организаций банковской системы Российской Федерации. URL: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf (дата обращения 25.06.2016).

11. Mikova S.Yu., Oladko V.S. The risk assessment of the implementation of network attacks on information infrastructure on the example of tourism enterprises// Sochi Journal of Economy. 2016. Vol. 39. Issue 1. P. 42-50.

References

1. Vlasova A.S. Elektronnaya kommertsiya // Sovremennye tendentsii v ekonomike i upravlenii: novyi vzglyad. 2014. №26. S. 37-43.

2. Startsev M.V. Elektronnaya kommertsiya kak sposob intensifikatsii biznes-protsessov// Sotsial'no-ekonomicheskie yavleniya i protsessy. 2011. № 5-6. S.212 -215.

3. Abdeeva Z.R. Problemy bezopasnosti elektronnoi kommertsii v seti internet // Problemy sovremennoi ekonomiki. 2012. №1. S. 172-175.

4. Olad'ko V.S. Zashchita informatsii v sistemakh elektronnoi kommertsii // Vestnik

UrFO. Bezopasnost' v informatsionnoi sfere. 2015. № 3 (17). S. 17-22.

5. Federal'nyi zakon ot 27.07.2006 N 149-FZ (red. ot 13.07.2015) "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" (s izm. i dop., vstup. v silu s 10.01.2016)//Konsul'tant Plyus.URL: http://www.consultant.ru/document/cons_ doc_LAW _61798/ (data obrashcheniya 23.06.2016).

6. Vol'fson M. Za proshlyi god global'nyi e-commerce vyros na 20%// E-business. URL: http://el-business.ucoz.ru/news/za_proshlyj_god_globalnyj_e_commerce_vyros_na_20/2015-03-14-167 (data obrashcheniya 21.06.2016).

7. Atkina V.S., Olad'ko A.Yu. Model' otsenki bezopasnosti sistem elektronnoi kommertsii // Vestnik komp'yuternykh i informatsionnykh tekhnologii. 2015. № 3 (129). S. 33-37.

8. Metodika opredeleniya aktual'nykh ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh. FSTEK Rossii, 2008 god // FSTEK Rossii. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380 (data obrashcheniya 25.06.2016).

9. Atkina V.S. Primenenie karty riskov dlya otsenki destruktivnogo vozdeistviya sushchestvennoi sredy na informatsionnuyu sistemu // Bezopasnost' informatsionnykh tekhnologii. 2013. № 4. S. 21-26.

10. Metodika otsenki riskov narusheniya informatsionnoi bezopasnosti//Obespechenie informatsionnoi bezopasnosti organizatsii bankovskoi sistemy Rossiiskoi Federatsii. URL: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf (data obrashcheniya 25.06.2016).

11. Mikova S.Yu., Oladko V.S. The risk assessment of the implementation of network attacks on information infrastructure on the example of tourism enterprises// Sochi Journal of Economy.2016. Vol. 39. Issue 1. P. 42-50.

УДК 338.14 + 004.056

Модель аудита информационной безопасности в информационных системах электронной коммерции вида B2E

Владлена Сергеевна Оладько

Волгоградский государственный университет, Российская Федерация
400062 г. Волгоград, пр-т Университетский, 100
Кандидат технических наук
E-mail: oladko.vs@yandex.ru

Аннотация. В статье рассмотрена актуальная проблема обеспечения информационной безопасности в системах электронной коммерции. Обозначены основные функции и области применения систем электронной коммерции. Представлена схема классификации моделей электронной коммерции, выделена одна из наиболее популярных моделей – модель B2E. Рассмотрены основные категории данных, обрабатываемых в системах электронной коммерции B2E и риски, которые возникают при воздействии угроз информационной безопасности. Показана необходимость применения системы защиты информации в системах электронной коммерции B2E. Сделан вывод о роли аудита информационной безопасности в процессе сопровождения системы защиты и контроля состояния текущей защищенности. Предложена методика проведения аудита информационной безопасности в системах электронной коммерции B2E. Разработана формализованная модель аудита, основанная на использовании профиля защиты, оценки рисков и расчете исходной защищенности системы.

Ключевые слова: электронная коммерция; риск, ущерб; информационная безопасность; угроза; аудит; профиль защиты, система защиты.