ИНФОРМАТИКА И ПРОГРАММИРОВАНИЕ

УДК 004.056; 004.4
DOI: 10.17223/19988605/33/6

В.С. Оладько

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ СИСТЕМ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Рассматриваются задача оценки уровня защищенности информации и ресурсов в системах электронной коммерции; основные модели и ресурсы систем электронной коммерции. Выделены типовые угрозы и механизмы защиты в системах электронной коммерции. Предложен подход к оценке уровня защищённости в системах электронной коммерции вида B2B и B2E. Разработан программный комплекс, реализующий предложенный подход. Проведены экспериментальные исследования.
Ключевые слова: электронный заместитель; риск; платежная система; угроза.

В настоящее время одной из наиболее активно развивающихся отраслей экономики и информационных технологий является электронная коммерция. По данным Synovate Comcon, в настоящий момент 58% пользователей Рунета прибегают к услугам электронной коммерции. При этом с каждым годом увеличивается число инцидентов, связанных с хищением денежных средств и нарушением информационной безопасности в системах электронной коммерции (СЭК); по данным [1], ущерб от подобных инцидентов колеблется в диапазоне от 250 тысяч до 60 млн руб. Следовательно, актуальным направлением являются исследования, связанные с анализом защищенности СЭК от угроз различной природы и синтезом наиболее эффективной системы защиты.

1. Проблемы безопасности системы электронной коммерции

В соответствии с [2] электронная коммерция – это форма коммерческой деятельности, осуществляемая полностью или частично в виртуальной среде, при которой информационные или транзакционные взаимодействия происходит на основе применения информационно-коммуникационных технологий. Анализ источников [2, 3] показывает, что наиболее востребована электронная коммерция в следующих отраслях:

– высокотехнологичное производство;
– финансовый сервис;
– розничная торговля;
– телекоммуникации;
– оптовая торговля;
– государственные услуги и закупки;
– транспорт.

В связи с этим в СЭК обрабатывается и храниться большое количество данных различной категории: платежные данные, электронные деньги, данные о транзакциях, а также персональные и идентификационные данные пользователей. В зависимости от способа функционирования и области использования СЭК реализуются с помощью следующих моделей, представленных в виде схемы на рис. 1. При этом наиболее распространёнными являются СЭК вида B2B и B2E, на долю которых, по данным [4], приходится 35 и 48% соответственно. Именно эти виды СЭК и будут рассматриваться автором в данной работе.

В связи с распределённой архитектурой СЭК, наличием подключения к глобальным сетям типа Интернет, круглосуточной доступностью сервисов и данных, а также большого количества пользователей-клиентов в процессе своего функционирования система подвергается ряду угроз и деструктивных воздействий как случайного характера, так и инициированных злоумышленником.

Основными источниками угроз СЭК являются:

1) непреднамеренные угрозы, вызванные стихийными бедствиями и техногенными катастрофами случайного характера, в ходе которых может быть нарушена непрерывность бизнес-процессов СЭК, доступность данных и сервисов, целостность данных;

2) ошибки пользователей и обслуживающего персонала СЭК;

3) преднамеренные действия злоумышленника, направленные на нарушение таких составляющих информационной безопасности, как доступность, целостность и конфиденциальность информации, циркулирующей в СЭК.

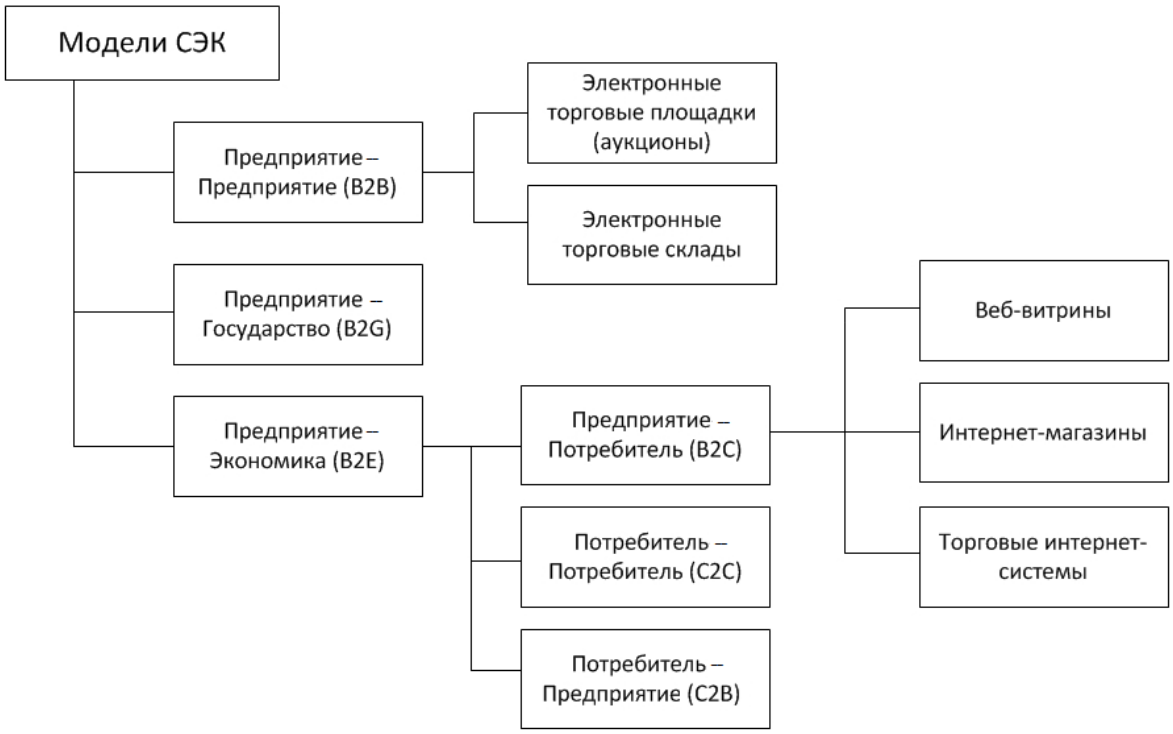

Рис. 1. Классификация моделей электронной коммерции

Согласно данным [5, 6] наибольшую опасность представляет собой класс угроз, связанных с действиями злоумышленников, поскольку именно этот класс несет наибольшие финансовые и репутационные риски. При этом главным объектом воздействий злоумышленника в СЭК являются финансовые средства, их электронные заместители, платежные данные и информация о транзакциях. По отношению к данным объектам злоумышленник преследует следующие цели:

– получение доступа к финансовым средствам и реквизитам для последующего использования;

– похищение финансовых средств и электронных заместителей;

– внедрение фальшивых финансовых средств;

– нарушение доступности сервисов СЭК и непрерывности бизнес-процессов;

– несанкционированный доступ к идентификационным данным пользователей СЭК;

– мошенничество, фишинг;

– несанкционированная модификация платежных данных, реквизитов и идентификационных данных.

Для эффективного противодействия большому числу угроз безопасности СЭК и обеспечения безопасности всех участников электронных платежей должны применяться различные средства и методы

защиты, правила применения и состав которых описываются в стандартах и рекомендациях регулирующих органов. Анализ литературных источников [7–11] показывает, что в качестве основных регулирующих органов в области безопасности платежных систем и СЭК в Российской Федерации выступают ЦБ РФ, ФСТЭК России и ФСБ России, которые, в соответствии с ФЗ № 161-ФЗ, образуют три уровня регулирования (рис. 2).

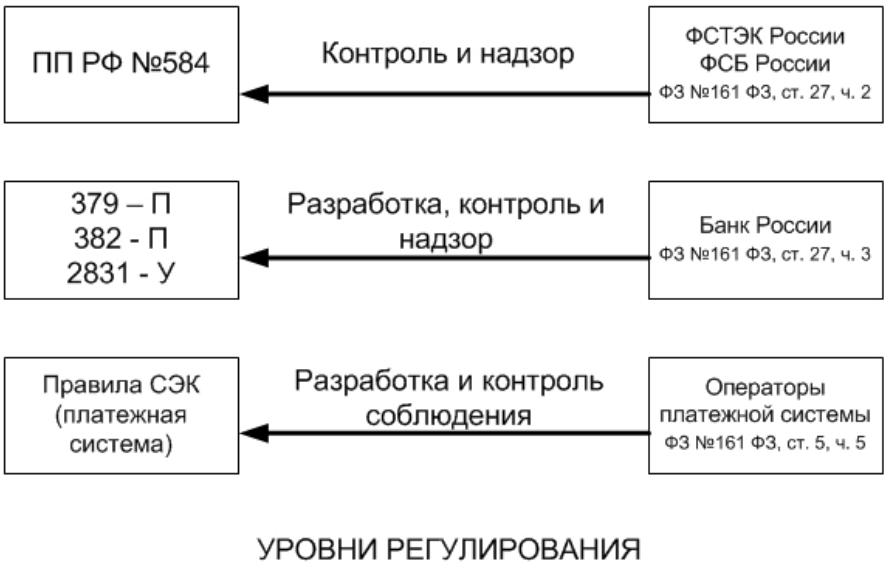

Рис. 2. Уровни регулирования безопасности в СЭК (область платежных систем)

В соответствии с требованиями регуляторов в СЭК должны применяться организационные и технические меры по защите информации. Данные меры по защите информации, с учетом использования в СЭК сетей общего пользования, должны предусматривать применение криптографических средств защиты информации, средств межсетевого экранирования, антивирусной защиты, обнаружения вторжений и анализа защищенности.

При этом средства анализа защищенности актуально применять на различных этапах жизненного цикла СЭК:

– на этапах проектирования и разработки системы защиты СЭК для выбора наиболее рационального и эффективного состава средств защиты;

– на этапе сопровождения с целью регулярного мониторинга и аудита безопасности СЭК и проверки соответствия системы защиты установленным регуляторами требованиям.

Таким образом, для исследования уровня защищенности СЭК и выбора наиболее рационального состава средств защиты информации в СЭК, позволяющих снизить риски от потенциальных угроз в пределах допустимого, актуально разработать процедуру оценки защищенности СЭК и автоматизировать ее с помощью программного комплекса.

2. Процедура оценки защищенности СЭК

Анализ литературных источников [5, 12, 13] показывает, что защищенность системы и риск нарушения информационной безопасности – два понятия, тесно связанных между собой. В частности, в работе [12] риск определяется как вероятный ущерб, который зависит от защищенности системы. Таким образом, риск – это экономический эквивалент защищенности системы от реализации возможных угроз. Следовательно, при проведении оценки защищенности СЭК целесообразно в качестве базового показателя использовать величину общего риска от реализации актуальных для СЭК угроз безопасности. А поскольку анализ рисков связан с оптимизационной задачей, заключающейся в поиске баланса между вложениями в систему защиты информации и возможным ущербом, то при оценке защищенности и выработке корректирующих рекомендаций будет решаться задача поиска наиболее рационального состава средств защиты, применение которого на практике позволит не только снизить общий уровень

риска, но и повысить защищенность СЭК. В данной работе будет использоваться качественный подход к оценке защищенности, в соответствии с которым защищенность СЭК будет оцениваться шкалой разбитой на три уровня: L = {низкий, средний, высокий}. Правила определения принадлежности защищенности СЭК к одному из трех уровней описаны автором в работе [14]. Таким образом, процедура оценки качественного уровня защищенности СЭК описывается в виде следующей последовательности шагов:

– составление модели СЭК с указанием объектов защиты, используемых средств защиты и пользователей СЭК;

– составление модели угроз и оценка рисков;

– оценка защищенности СЭК на основе данных об используемых средствах защиты и рисках от реализации актуальных угроз;

– формирование отчета о результатах оценки защищённости и выдача рекомендаций по реконфигурации системы защиты СЭК в случае необходимости.

На рис. 3 в нотации IDEF0 представлена разработанная функциональная модель оценки защищенности СЭК.

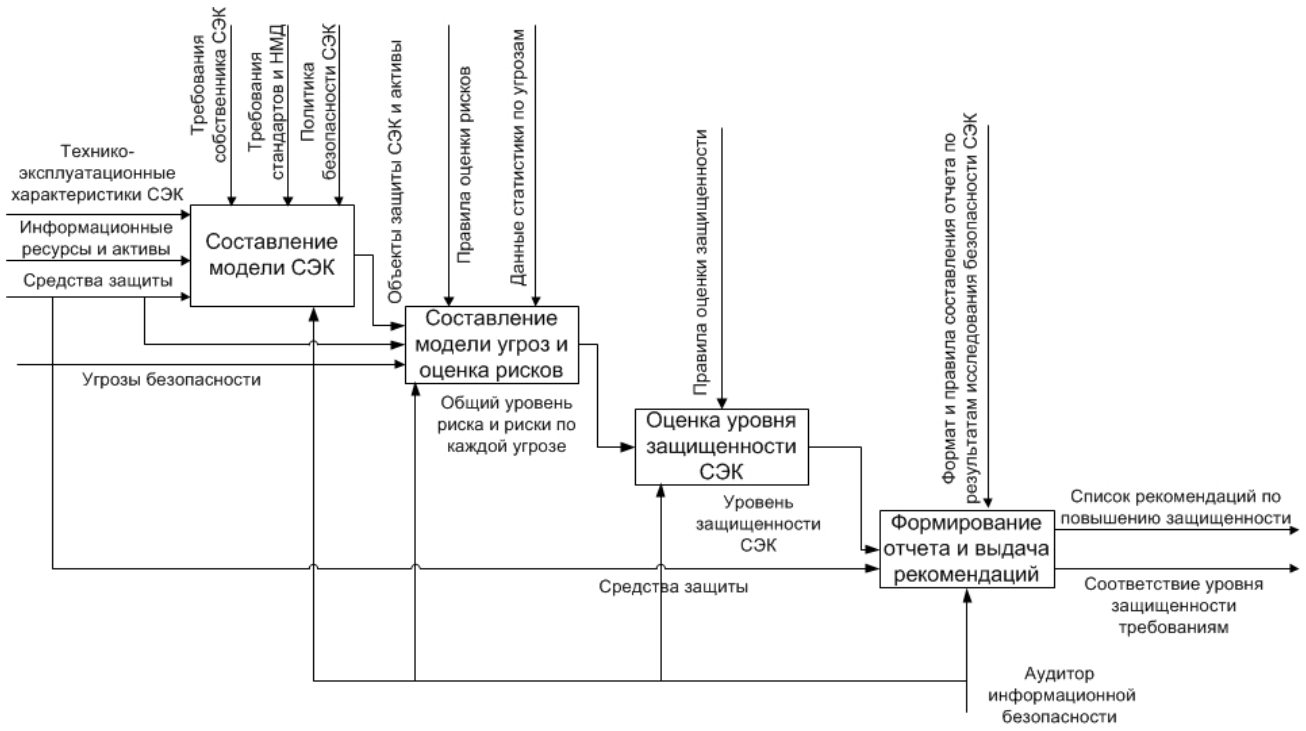

Рис. 3. Функциональная контекстная диаграмма оценки защищенности СЭК в нотации IDEF0

Входными данными являются:

– вид и технико-эксплуатационные характеристики СЭК;

– информационные ресурсы, активы СЭК и платежные данные;

– используемые средства и механизмы защиты;

– список угроз для СЭК;

– список злоумышленников;

– требования к допустимому уровню риска и уровню защищенности СЭК.

Выходными данными являются:

– оцененный уровень защищенности СЭК;

– соответствие или несоответствие оцененного уровня защищенности СЭК требованиям безопасности;

– список рекомендаций по повышению защищенности СЭК.

3. Программный комплекс оценки уровня защищенности СЭК

Для автоматизации описанных выше функций был разработан программный комплекс, архитектура которого представлена на рис. 4. В архитектуре схожие функции были объединены в отдельные модули с целью обеспечения их более эффективного выполнения.

Рис. 4. Архитектура программного комплекса оценки защищенности СЭК

Модуль сбора данных об СЭК предназначен для сбора информации о технико-эксплуатационных характеристиках СЭК, ее активах и объектах, которые подлежат защите; ввода требований к защищенности СЭК и уровню допустимого риска. Информация вводится ответственным за информационную безопасность в СЭК лицом.

Модуль выбора средств защиты предназначен для выбора из списка возможных средств и механизмов защиты, которые используются в исследуемой СЭК для обеспечения безопасности.

Модуль выбора угроз и оценки рисков СЭК предназначен для составления модели угроз для СЭК, установки для каждой угрозы вероятности реализации и потенциального ущерба и расчета риска по каждой угрозе и общего риска.

Модуль оценки защищенности предназначен для оценки уровня защищенности СЭК.

Модуль формирования рекомендаций и отчета обеспечивает взаимодействие между другими модулями и на основании данных об уровне защищенности СЭК вырабатывает комплекс мероприятий – рекомендаций по защите от каждой из актуальных угроз, определяет соответствие между рассчитанным уровнем защищенности и допустимым и выносит решение о защищенности или незащищённости СЭК. И если СЭК имеет низкую защищенность, то выводит список рекомендуемых средств и механизмов защиты. Отчет о результате оценки выводится на экран, а также может быть сохранен в формате .docx.

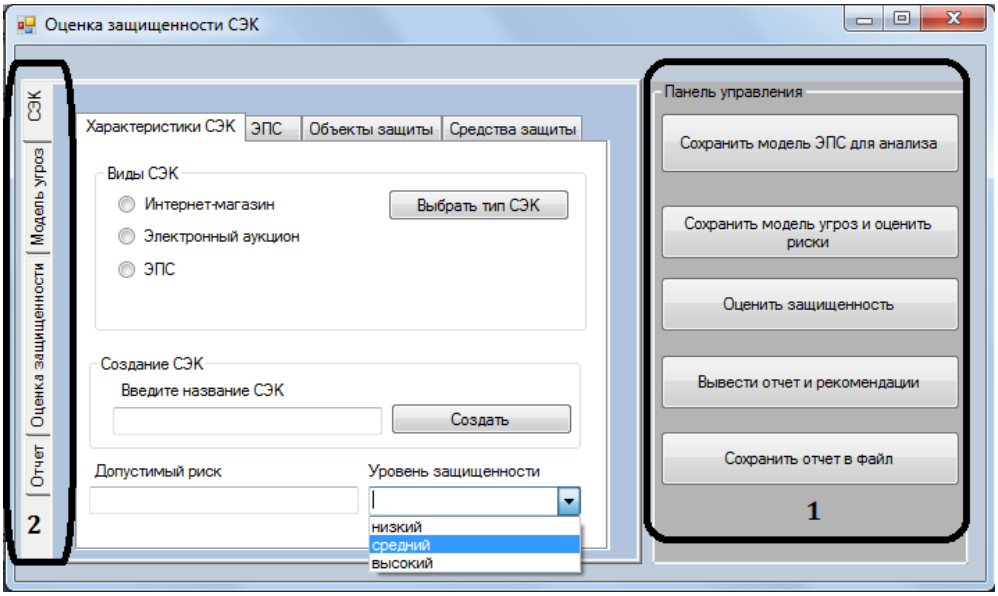

Рис. 5. Пользовательский интерфейс программного комплекса оценки защищенности СЭК (экранная копия)

Пользовательский интерфейс имеет графический вид и предназначен для ввода данных, вывода результатов и организации взаимодействия пользователя с программой. Состоит из блока управления программным комплексом (рис. 5, область *1*) и четырёх функциональных вкладок (рис. 5, область *2*), реализующих основные задачи оценки защищенности СЭК: составление модели СЭК, составление модели угроз для исследуемой СЭК, оценки защищенности СЭК и вывода отчета о результатах оценки защищенности на экран.

Разработанный программный комплекс предназначен для специалиста по информационной безопасности и/или другого ответственного за защиту информации в СЭК лица. Может использоваться в качестве вспомогательного средства при проведении внутреннего аудита информационной безопасности СЭК.

4. Экспериментальные исследования

Эксперименты направлены на исследование результатов оценки защищенности и возможности использования, предложенных моделью рекомендаций для повышения общего уровня защищенности СЭК и снижения рисков. В рамках данных экспериментов было проведено исследование защищенности 10 тестовых СЭК, результаты которых представлены в виде гистограммы на рис. 6.

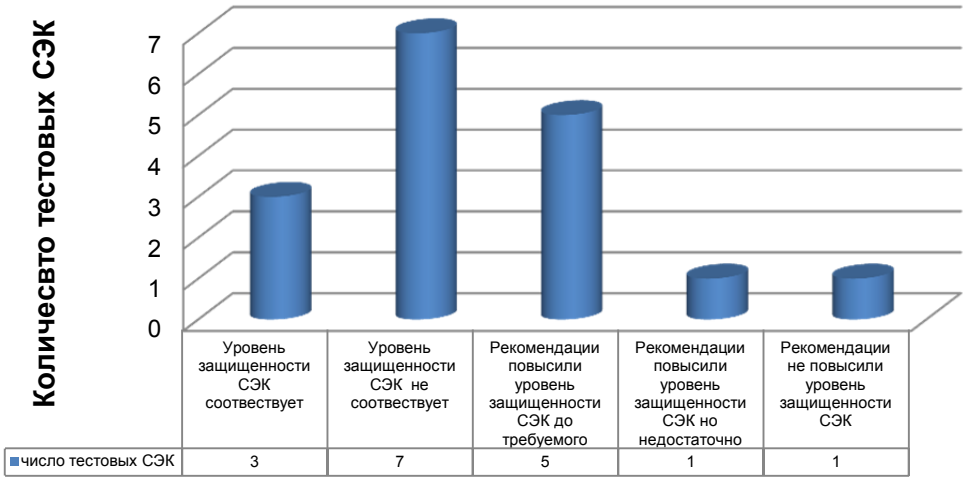

Рис. 6. Распределение результатов оценки защищенности для 10 тестовых СЭК различного вида.

Анализ полученных результатов позволяет сделать вывод, что в 86% случаях рекомендации, предложенные программным комплексом в ходе оценки, позволяют повысить уровень защищенности СЭК, при этом в 71% этого повышения достаточно для достижения требуемой защищенности. Таким образом, можно сделать вывод о возможности применения рекомендаций модели для повышения общей защищенности СЭК различного вида.

Заключение

Была разработана процедура оценки защищенности СЭК. В нотации IDEF0 описаны функции и этапы процедуры оценки защищенности СЭК, выделены входные и выходные данные. Описаны архитектура и пользовательский интерфейс программного комплекса, автоматизирующего предложенную процедуру. Разработанный программный комплекс может применяться в учебном процессе на лабораторном практикуме для обучения студентов направления «информационная безопасность» и на практике при проектировании систем электронной коммерции и в процессе функционирования для контроля над состоянием их безопасности.

ЛИТЕРАТУРА

1. *Абдеева З.Р.* Проблемы безопасности электронной коммерции в сети Интернет // Проблемы современной экономики. 2012. № 1. С. 172–175.
2. *Агафонова А.Н.* Информационный сервис в Интернет-экономике. М. : БИБЛИО-ГЛОБУС, 2014. 152 с.
3. *Ефимкин Н.В.* Электронная коммерция как современная форма торговли // Экономика и социум. 2015. № 2. URL: http://www.iupr.ru/domains_data/files/zurnal_15/Efimkin%20N.V.%20%28Informacionnye%20i%20kommunikativnye%20tehnologii%29.doc%20%281%29.pdf (дата обращения: 24.08.2015).
4. *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: 01.04.2015).
5. *Яндыбаева Э.Э. Машкина И.В.* Оценка актуальности угроз информационной безопасности в информационной системе электронной торговой площадки // Безопасность информационных технологий. 2014. № 1. С. 41–44.
6. *Оладько В.С.* Модель действия злоумышленника в системах электронной коммерции // Международный научно-исследовательский журнал. 2015. № 7 (38). С. 83–85.
7. *Федеральный закон* от 27.06.2011 № 161-ФЗ (ред. от 29.12.2014) «О национальной платежной системе» (с изм. и доп., вступ. в силу с 01.03.2015) (27 июня 2011 г.) // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_173643 (дата обращения: 15.03.2015).
8. *Максимов В.* № 161-ФЗ «О национальной платежной системе»: роли, правила, требования Банка России к защите информации, сроки исполнения, последствия // Андек. URL: http://www.andek.ru/ehkspertiza/banki/nacionalnaya-platezhnaya-sistema/ (дата обращения: 15.03.2015).
9. *Положение* Банка России от 09.06.2012 г. № 382-П: «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_131473/ (дата обращения: 24.08.2015).
10. *Указание* Банка России от 09.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств» // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_131471/ (дата обращения: 23.08.2015).
11. *Положение* Банка России от 31.05.2012 г. № 379-П: «Положение о бесперебойности функционирования платежных систем и анализе рисков в платежных системах» // Консультант Плюс. URL: http://base.consultant.ru/cons/CGI/online.cgi?req=doc;base=LAW;n=167370 (дата обращения: 23.08.2015).
12. *Ерохин С.* Методика оценки рисков нарушения информационной безопасности // Информационная безопасность. URL: http://esstm.blogspot.com/2011/09/microsoft.html (дата обращения: 16.04.13).
13. *Банокин П.И., Вичугов В.Н.* Реализация программной системы для предотвращения внутренних утечек корпоративных данных // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2014. № 1 (26). С. 84–88.
14. *Аткина В.С., Оладько А.Ю.* Модель оценки безопасности систем электронной коммерции // Вестник компьютерных и информационных технологий. 2015. № 3. С. 33–37.

Оладько Владлена Сергеевна, канд. техн. наук, доцент. E-mail: oladko.vs@yandex.ru
Волгоградский государственный университет

Поступила в редакцию 7 сентября 2015 г.

Oladko Vladlena S. (Volgograd State University, Russian Federation).

The program is assessing the level of security of e-commerce.

Keywords: electronic substituent; risk; payment system; threat.

DOI: 10.17223/19988605/33/6

This article deals with the problem of information security in data processing system of e-commerce. The author highlights the scope and the main models of e-commerce. Models type B2E and B2B are selected for the study of security. The main objects that are processed in the system of e-commerce are the payment information, finance, electronic substituents, transaction data, personal data, user's identification and authentication data.

The main causes of violations of data security and business continuity in the systems of electronic commerce are analyzed. These are the threat of unintentional and intentional. Unintentional threats include natural disasters and man-made disasters, user errors and software failures. Intentional threats relate to the actions of an insider or an external attacker or group of attackers. The main objects of the impact of the attacker's e-commerce systems are electronic substituents financial resources and personal data. Regulatory requirements to protect payment data and e-commerce systems from the threats of a different nature are allocated. It is concluded that in addition to the use of information security tools necessary to carry out regular monitoring of the security of e-commerce and data processed by it.

It is proposed to consider security as a measure of the quality associated with the value of the residual risk by using means of information protection. Security of e-commerce is divided into three levels and describes the scale of L = {low, medium, high}. It is designed and described how the qualitative assessment of the level of security of e-commerce. Its main steps are:

– drafting a model of e-commerce with an indication of the objects of protection, protection systems and users;

– drafting threat models and risk assessment;

– assessment of the security of e-commerce on the basis of data on the means used to protect and risks of the actual threats;

– forming a report on the evaluation of security and making recommendations on the reconfiguration of the system of protection in case of need.

Functional assessment model of security is composed. The modular architecture of software for the evaluation of the level of protection has been developed and described. The main function modules include:

– performance data collection of e-commerce and the input requirements of security and the level of acceptable risk;

– selection module remedies designed to select from a list of possible means and mechanisms of protection that are used in the system to ensure safety;

– selection module threat and risk assessment system for e-commerce for drawing up the threat model, the settings for each threat and probability of potential damage and the calculation of risk for each threat, and the overall risk;

– module security assessment is designed to evaluate the quality level of system security;

– generation unit and the recommendations of the report.

The graphical user interface is presented. The experimental results of test models of e-commerce systems are described. The author concluded that performance of software and applications as a tool for the assessment of the current security systems, e-commerce and make recommendations for its increase.

REFERENCES

1. Abdeeva, Z.R. (2012) Electronic commerce in the Internet: problems of security. *Problemy sovremennoy ekonomiki – Problems of modern economics*. 1(41). pp. 172-175. (In Russian).
2. Agafonova, A.N. (2014) *Informatsionnyy servis v Internet-ekonomike* [Information service in the Internet economy]. Moscow: BIBLIO-GLOBUS.
3. Efimkin, N.V. (2015) Elektronnaya kommertsiya kak sovremennaya forma torgovli [E-commerce as a modern form of trading]. *Ekonomika i sotsium*. 2. [Online] Available from: http://www.iupr.ru/domains_data/files/zurnal_15/Efimkin%20N.V.%20%28Informacionnye%20i%20kommunikativnye%20tehnologii%29.doc%20%281%29.pdf. (Accessed: 24th August 2015).
4. Wolfson, M. (2015) *Za proshlyy god global'nyy e-commerce vyros na 20%* [Over the past year the global e-commerce has grown by 20%]. [Online] Available from: http://el-business.ucoz.ru/news/za_proshlyj_god_globalnyj_e_commerce_vyros_na_20/2015-03-14-167. (Accessed: 1st April 2015).
5. Yandybaeva, E.E. & Mashkina, I.V. (2014) The Relevance Assessment of Information Security Threats in the Information System of Electronic Trading Platform. *Bezopasnost' informatsionnykh tekhnologiy*. 1. pp. 41-44. (In Russian).
6. Olad'ko, V.S. (2015) Model' deystviya zloumyshlennika v sistemakh elektronnoy kommertsii [Model action attacker in electronic commerce systems]. *Mezhdunarodnyy nauchno-issledovatel'skiy zhurnal – International Research Journal*. 7(38). pp. 83-85.
7. Russian Federation. (2011) *Federal'nyy zakon ot 27.06.2011 № 161-FZ (red. ot 29.12.2014) "O natsional'noy platezhnoy sisteme" (s izm. i dop., vstup. v silu s 01.03.2015) (27 iyunya 2011 g.)* [Federal Law N 161-FZ of June 27, 2011 (ed. by December 29, 2014) "On the national payment system" (rev. and ext., joined. in force from March 1, 2015) (27 June 2011)]. [Online] Available from: http://www.consultant.ru/document/cons_doc_LAW_173643. (Accessed: 15th March 2015).
8. Maksimov, V. (n.d.) *№ 161-FZ "O natsional'noy platezhnoy sisteme": roli, pravila, trebovaniya Banka Rossii k zashchite informatsii, sroki ispolneniya, posledstviya* [N161-FZ "On the national payment system": roles, rules, requirements of the Bank of Russia to the protection of information, deadlines, and consequences]. [Online] Available from: http://www.andek.ru/ehkspertiza/banki/nacionalnaya-platezhnaya-sistema/. (Accessed: 15th March 2015).
9. The Bank of Russia. (2012) *Polozhenie Banka Rossii ot 09.06.2012 g. № 382-P: "Polozhenie o trebovaniyakh k obespecheniyu zashchity informatsii pri osushchestvlenii perevodov denezhnykh sredstv i o poryadke osushchestvleniya Bankom Rossii kontrolya za soblyudeniem trebovaniy k obespecheniyu zashchity informatsii pri osushchestvlenii perevodov denezhnykh sredstv"* [The Bank of Russia on June 9, 2012, the N382-P: "Regulations on requirements to ensure the protection of information in the implementation of remittances and the exercise by the Bank of Russia control over compliance with the requirements for the protection of inforation in the implementation of remittances"]. [Online] Available from: http://www.consultant.ru/document/cons_doc_LAW_131473/. (Accessed: 24th August 2015).
10. The Bank of Russia. (2012) *Ukazanie Banka Rossii ot 09.06.2012 № 2831-U "Ob otchetnosti po obespecheniyu zashchity informatsii pri osushchestvlenii perevodov denezhnykh sredstv operatorov platezhnykh sistem, operatorov uslug platezhnoy infrastruktury, operatorov po perevodu denezhnykh sredstv"* [The Bank of Russia Resolution N2831-U of June 9, 2012, "O accountability to ensure the protection of information in the implementation of remittance payment system operators, service operators of the payment infrastructure operators for the transfer of funds"]. [Online] Available from: http://www.consultant.ru/document/cons_doc_LAW_131471/ (Accessed: 23rd August 2015).
11. The Bank of Russia. (2012) *Polozhenie Banka Rossii ot 31.05.2012 g. № 379-P: "Polozhenie o bespereboynosti funktsionirovaniya platezhnykh sistem i analize riskov v platezhnykh sistemakh"* [The Bank of Russia Resolution N379-P of May 31, 2012: "Regulaions on the smooth functioning of payment systems and risk analysis in payment systems"]. [Online] Available from: http://base.consultant.ru/cons/CGI/ online.cgi?req=doc;base=LAW;n=167370. (Accessed: 23rd August 2015).
12. Erokhin, S. (2011) *Metodika otsenki riskov narusheniya informatsionnoy bezopasnosti* [Methods of assessing the risks of violation of information security]. [Online] Available from: http://esstm.blogspot.com/2011/09/microsoft.html. (Accessed: 16th April 2013).
13. Banokin, P.I. & Vichugov, V.N. (2014) Implementation of Software system for prevention of internal data leaks. *Vestnik Tomskogo gosudarstvennogo universiteta. Upravlenie, vychislitel'naya tekhnika i informatika – Tomsk State University Journal of Control and Computer Science*. 1(26). pp. 84-88.
14. Atkina, V.S. & Olad'ko, A.Yu. (2015) Model of e-commerce security assessment. *Vestnik komp'yuternykh i in-formatsionnykh tekhnologiy – Herald of Computer and Information Technologies*. 3. pp. 33-37. (In Russian).