УДК 004.056.5; 004.738.5

**Оладько В. С.**

# ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОЙ КОММЕРЦИИ

*Статья нацелена на рассмотрение основных подходов к защите информации в системах электронной коммерции. Представлена архитектура системы электронной коммерции, выделены основные причины и последствия нарушения безопасности. Проанализированы требования регуляторов к обеспечению информационной безопасности в электронной коммерции. Представлен жизненный цикл синтеза системы защиты информации в электронной коммерции.*

***Ключевые слова:*** *система электронной коммерции, система защиты, криптографическая защита, межсетевое экранирование, угроза, риск.*

**Oladko V. S.**

# THE INFORMATION SECURITY IN E-COMMERCE SYSTEM

*This article focuses on a review of key approaches to data protection in e-commerce systems. The architecture of e-commerce system is represented, identified the main causes and consequences of a security breach. The requirements of regulators to ensure information security in e-commerce are analyzed. The life cycle of the synthesis of information security in e-commerce represented.*

***Keywords:*** *internet, security system, cryptographic protection, firewall, threat, risk.*

**Введение.** Электронная коммерция (ЭК) с каждым годом играет все большее значение в экономической сфере и интернет среде, в настоящий момент, по данным Synovate Comcon, 58% пользователей рунета прибегают к услугам ЭК. Результаты исследований компаний eMarketer и J'son & Partners Consulting показывают, что рост мирового рынка ЭК в 2014 году составил 20%, а доля интернет-продаж составила 5,9% от мирового товарооборота, что составляет $1,316 трлн. Активно применяясь в финансовом и банковском секторе, области оптовых и розничных продаж через интернет, электронных аукционах, предоставлении государственных услуг и управление корпоративными сетями, системы ЭК подвергаются атакам злоумышленников и дестабилизирующим воздействиям случайного характера. Ущерб от подобных нарушений составляет от 250 тысяч до 60 млн. рублей [1], при этом наиболее подвержены воздействиям персональные и платежные данные [2]. Поэтому актуальным является решение задач, связанных с синтезом систем защиты информации в ЭК, применение которых позволит предотвратить ряд нару-

шений и существенно снизить риски от их последствий.

**Проблемы безопасности в системах электронной коммерции.** Электронная коммерция – это форма коммерческой деятельности, осуществляемая полностью или частично в виртуальной среде, при которой информационные или транзакционные взаимодействия осуществляются на основе применения информационно-коммуникационных технологий [3]. Как и в любых других видах деятельности для ЭК выделяют несколько форм, наиболее распространенными из которых являются: модель Бизнес-Бизнес (B2B); модель Бизнес-Потребитель (B2C); модель Бизнес-Правительство (B2G); модель Правительство-Граждане (G2C) и модель Бизнес-Сотрудники (B2E). Выделенные модели затрагивают такие области экономики как ритейл (B2C), электронные торговые площадки и аукционы (B2B, B2E) и государственный сектор (B2G, G2C). В соответствии с каждой моделью строится своя система ЭК, включающая в себя информационную и обеспечивающую инфраструктуру (сервера, базы данных, веб-приложения, сервисы), корпоративные, межкорпоративные и глобальные сети, субъекты (финансовые организации, правительство, поставщики, продавцы, производители и потребители) и объекты взаимодействия (информационные продукты, персональные и платежные данные пользователей, денежные средства и электронные заместители, логины и пароли, техническая и служебная информация, реквизиты). Все выделенные элементы, входящие в состав системы ЭК участвуют в реализации ключевых бизнес-процессов системы и должны учитываться при обеспечении безопасности функционирования системы.

На рис. 1 представлена типовая схема системы ЭК.

В ней основными функциональными сегментами являются:

- прикладная сеть электронной коммерции, включающая в себя общую бизнес-инфраструктуру, платежный сервер, СУБД;
- веб-сайт;
- сетевая инфраструктура (глобальные, межкорпоративные и корпоративные сети);
- автоматизированная система (АС) пользователей-потребителей системы ЭК;
- финансовые организации (банк – эквайер, банк эмитент).

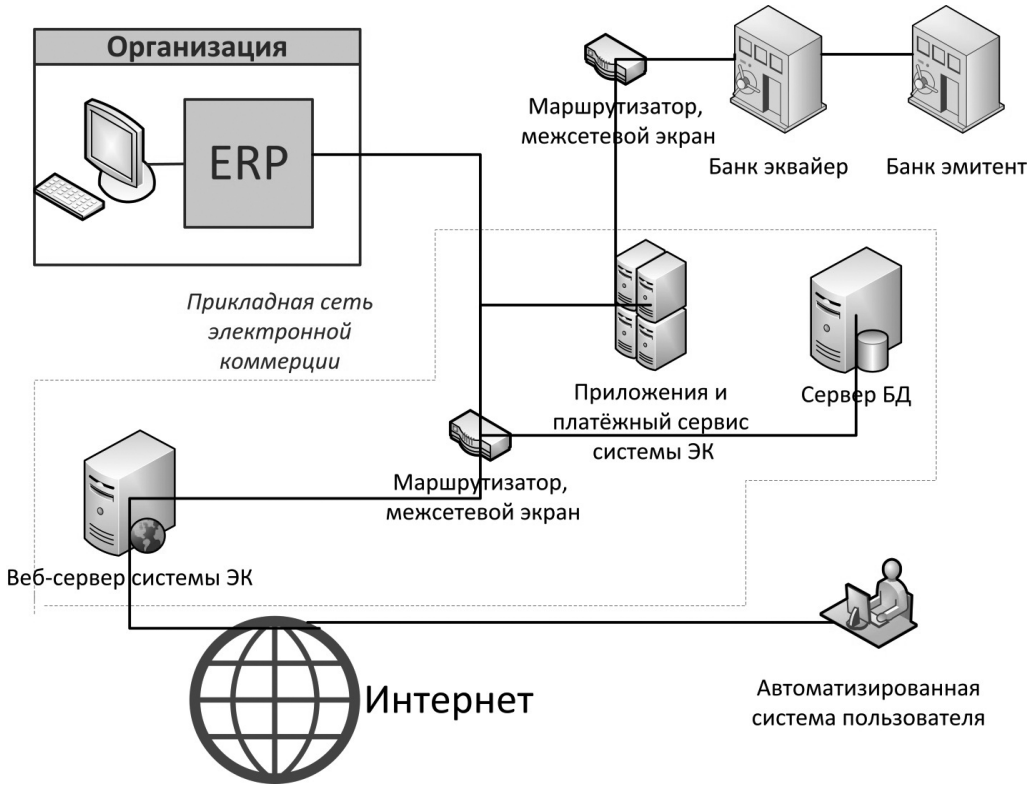


Рис. 1. Структура типовой системы электронной коммерции

Все структурные сегменты системы ЭК, в процессе своего функционирования, могут подвергаться ряду угроз, как случайного, так и умышленного характера. Как показано в работах [4,5], наиболее распространёнными причинами нарушения безопасности в электронной коммерции являются:

- сетевые атаки;
- атаки на пароли и системы аутентификации пользователя;
- ошибки, сбои и отказы программно-аппаратного обеспечения системы ЭК;
- вредоносное программное обеспечение;
- мошенничество;
- ошибки и другие неумышленными действиями обслуживающего персонала системы ЭК;
- разрушение сетевой и обеспечивающей инфраструктуры вследствие катастроф, различной природы.

В результате данных воздействий может произойти:

- кража денежных средств и их электронных заместителей;
- утечка конфиденциальной информации;
- отказ в обслуживание пользователей системы ЭК;
- недоступность сервисов и данных;
- прерывание бизнес-процессов и нарушение непрерывности функционирования ЭК;
- фальсификация данных, отказ от совершенных операций.

Для снижения рисков, связанных с нарушениями ИБ в системе ЭК, необходимо строить защиту по следующим направлениям:

- защита информации на уровне сервера и прикладной сети системы ЭК;
- защита соединений;
- защита информации на уровне АС клиента системы ЭК.

**Требования к обеспечению безопасности информации в ЭК.** Для эффективного противодействия большинству угроз безопасности систем ЭК и обеспечения безопасности информации и всех участников бизнес-процессов ЭК должны применяться различные средства и методы защиты, правила применения и состав которых описывается в стандартах и рекомендациях регулирующих органов.

Анализ [6] показывает, что за рубежом решением проблемы обеспечения безопасности систем ЭК занимается независимый консорциум – Internet Security Task Force (ISTF), представляющий собой организацию, состоящую из представителей и экспертов компаний-поставщиков средств информационной безопасности (ИБ), электронного бизнеса и провайдеров Интернет - услуг. Консорциум ISTF выделяет двенадцать направлений ИБ, которые необходимо учитывать при проектировании и реализации системы защиты ЭК:

- защита персональных данных субъектов ЭК;
- обеспечение объективного подтверждения идентифицирующей информации;
- защита корпоративного периметра объектов системы ЭК;
- обеспечение контроля доступа к объектам, данным и сервисам системы ЭК;
- обеспечение контроля потенциально опасного содержимого запросов и страниц web-сайта системы ЭК;
- администрирование функциональных подсистем системы ЭК;
- обнаружение и идентификация атак;
- регистрация и анализ событий безопасности;
- реакция на события безопасности и управление инцидентами.

Анализ литературных источников [7-10] 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 соответствие с ФЗ№161-ФЗ образуют три уровня регулирования (см. рис. 2).

В частности одними из основных документов в области защиты СЭК и платежных систем являются Банка России:

- Положение Банка России от 09.06.2012 г. N382-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»;
- Указание Банка России от 09.06.2012 N2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств»;

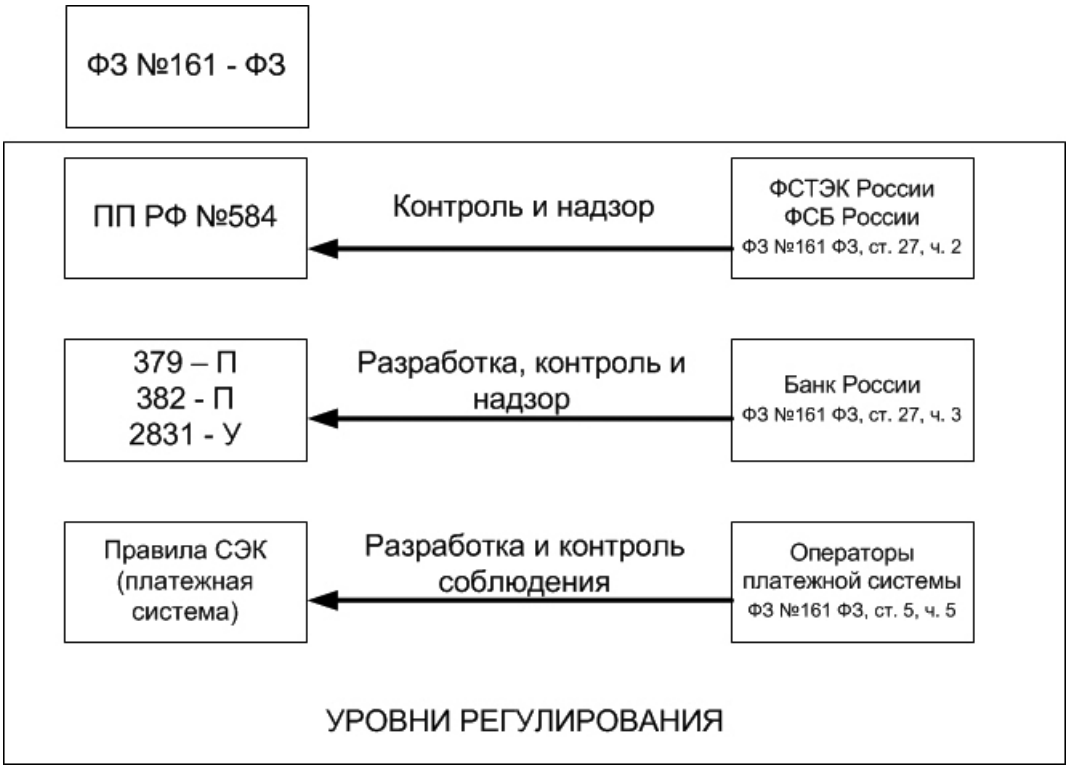


Рис. 2. Уровни регулирования безопасности в СЭК (область платежных систем)

- Положение Банка России от 31.05.2012 г. N379-П: «Положение о бесперебойности функционирования платежных систем и анализе рисков в платежных системах».

Таким образом, для защиты от основных угроз и злоумышленных воздействий при синтезе системы защиты информации в системе ЭК должны учитываться следующие базовые требования:

- система должна обеспечивать защиту данных платежных поручений от несанкционированного изменения и модификации;
- система не должна увеличивать возможности злоумышленника по организации атак на компьютер клиента;
- система должна обеспечивать защиту данных, расположенных на сервере от несанкционированного чтения и модификации;
- система должна обеспечивать или поддерживать систему защиты локальной сети сервера системы ЭК от воздействия из глобальной сети;
- система должна уведомлять о фактах обнаружения и/или воздействия вредоносного программного обеспечения на подсистемы СЭК;
- система должна обеспечивать криптографическую защиту информации;
- система должна регистрировать события и выявлять инциденты, связанные с нарушением информационной безопасности;
- должен проводится периодический контроль выполнения требований к защите информации на собственных объектах инфраструктуры системы ЭК;

Таким образом, на основании проведённого анализа можно сделать вывод, что в системе ЭК должны применяться организационные, программно-аппаратные и технические средства по защите информации. Данные средства при синтезе системы защиты должны учитывать распределённую архитектуру, гетерогенность и использование в системе ЭК сетей общего пользования. Кроме того, система защиты должна проектироваться и реализовываться в соответствии с требованиями к защите информации в платежной системе и предусматривать применение криптографических средств защиты информации, средств межсетевого экранирования, антивирусной защиты, обнаружения вторжений и анализа защищенности. Следовательно, минимальным набором средств защиты в системе ЭК являются: системы шифрования

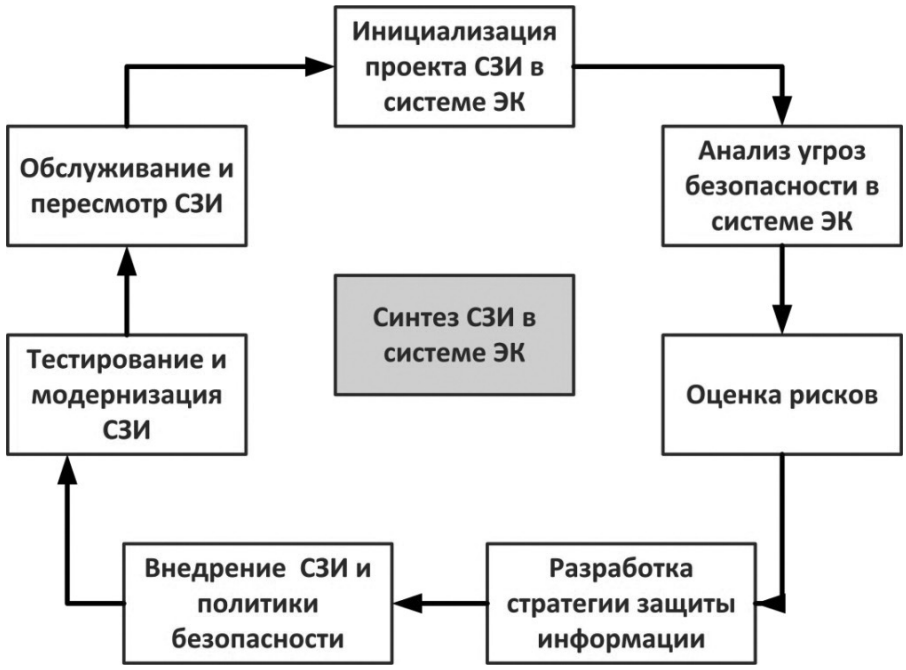


Рис.3. Модель жизненного цикла СЗИ в системе ЭК

данных при передаче и хранении, системы аутентификации пользователей, межсетевые экраны, антивирусы, системы обнаружения атак и средства анализа защищенности.

**Подход к синтезу системы защиты информации в системе ЭК.** Система защиты информации - совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации. Как и любая другая система, система защиты информации имеет свой жизненный цикл, в данной работе для систем ЭК жизненный цикл предлагается рассматривать в виде бесконечного цикла (см. рис. 3), состоящего из 7 этапов.

Подобный подход обусловлен тем, что система защиты информации должна быть адаптивной и учитывать возможные изменения в экономике, сфере информационных технологий, законодательстве и других областях, влияющие на деятельность системы ЭК, а также быть готовой противостоять новым неизвестным типом атакам злоумышленников.

**Примечания**

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

2. Глобальное исследование утечек конфиденциальной информации в I полугодии 2015 года [Электронный ресурс]. //Аналитический центр InfoWatch. URL: http://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2015_half_year.pdf (дата обращения 18.11.2015).

3. Агафонова А.Н. Информационный сервис в Интернет-экономике / А.Н. Агафонова. – М.: БИБЛИО-ГЛОБУС, 2014. – 152 с.

4. Оладько В.С. Модель действий злоумышленника в системах электронной коммерции//Международный научно-исследовательский журнал.2015.№7-1(38).С.83-85.

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. 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 18.14.2015)

7. Федеральный закон от 27.06.2011 N 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 20.11.2015).

8. Максимов В. N161-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 20.11.2015)

9. Положение Банка России от 09.06.2012 г. N382-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»;

10. Указание Банка России от 09.06.2012 N2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств».

---

**Оладько Владлена Сергеевна,** кандидат технических наук, доцент кафедры информационной безопасности, ФГАОУ ВПО «Волгоградский государственный университет», г. Красногорск. E-mail: oladko.vs@yandex.ru

**Oladko Vladlena Sergeevna,** PhD (Engineering), Associate Professor of Information Security of «Information Security» department, Volgograd State University, E-mail: oladko.vs@yandex.ru