МОДЕЛЬ ВЫБОРА РАЦИОНАЛЬНОГО СОСТАВА СРЕДСТВ ЗАЩИТЫ В СИСТЕМЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Оладько В.С.[1]

В статье рассмотрена проблема обеспечения безопасности информации в области электронной коммерции. Определена область применения и назначение электронной коммерции. Выделены основные виды систем электронной коммерции и типы данных, хранящихся и обрабатываемых в подобных системах. Представлена типовая структура системы электронной коммерции, разделенная на четыре сегмента: бизнес–инфраструктура и центр обработки данных, web–сайт, сетевая инфраструктура и автоматизированные системы пользователей. Рассмотрен технологический процесс функционирования системы электронной коммерции. Выделены наиболее уязвимые с точки зрения информационной безопасности процессы: передача идентификационных и аутентификационных данных пользователя, авторизация пользователя, перевод денежных средств или электронных заместителей, хранение данных ограниченного доступа в центрах обработки данных. В соответствии с выделенными сегментами определены основные направления организации защиты. Представлены требования регуляторов к составу системы защиты информации в системе электронной коммерции. Проанализированы и описаны этапы процесса планирования и выбора состава средств защиты информации: определение перечня требований к защищенности системы, определение состава и подсистем защиты, выбор средств защиты для внедрения. Предложены частные показатели оценки эффективности средств защиты: стоимость средства защиты; величина предотвращенного ущерба; наличие сертификата ФСТЭК/ФСБ; количество перекрываемых угроз; совместимость с другими средствами защиты. Разработана и описана в нотации IDEFO функциональная модель выбора рационального состава средств защиты информации в системе электронной коммерции. Представлено формализованное описание многокритериального выбора рационального состава средств защиты информации в соответствии с разработанной функциональной моделью.

***Ключевые слова**: информационная безопасность, многокритериальная оценка, защищенность, система защиты, электронная торговая площадка, электронная платежная система, интернет–магазин, инцидент, риск, угроза, ущерб, эффективность.*

Введение

В настоящее время активное развитие и распространение получила электронная коммерция темпы роста которой, по данным исследований [1], составляют от 15 до 20% в год. Используя различные информационно-коммуникационные технологии, распределенные приложения и сервисы в виде единой системы, электронная коммерция активно применяется в таких отраслях как высокотехнологичное производство; интернет-банкинг, платежные системы и финансовый сервис; розничная и оптовая торговля; телекоммуникации; государственные услуги и закупки; транспорт. Как показывают данные аналитики, в системах электронной коммерции (СЭК) с каждым годом увеличивается число инцидентов, связанных с утечкой персональных и платежных данных пользователей, хищением денежных средств и нарушением информационной безопасности, по данным [2] ущерб от подобных инцидентов колеблется в диапазоне от 250 тысяч до 60 млн. рублей. Поэтому для предотвращения или снижения рисков от подобных инцидентов, востребованным является решение задач, связанных с обеспечением безопасности данных и сервисов в СЭК. А для обеспечения требуемого уровня безопасности необходимо использовать различные средства и механизмы защиты. Таким образом, одной из важнейших задач рационального построения комплексной системы защиты СЭК является выбор из множества существующих средств защиты такого их набора, который позволит обеспечить нейтрализацию большинства актуальных угроз безопасности с наилучшим качеством и минимально возможными затраченными на это ресурсам.

Система электронной коммерции как объект защиты

Существует множество моделей и способов реализации систем электронной коммерции, наиболее известными из которых являются:

– электронные торговые площадки, биржи и аукционы;

1 Оладько Владлена Сергеевна, доцент, кандидат технических наук, ФГАОУ ВПО «Волгоградский государственный университет», г. Волгоград, oladko.vs@yandex.ru

– электронные платежные системы и сервисы;
– интернет магазины, каталоги и витрины;
– системы услуг, в том числе и государственных;
– корпоративная электронная коммерция.

В рамках данных систем производиться выполнение транзакций и бизнес-процессов, предоставление товаров и услуг, а также обработка и сбор сведений, представляющих собой персональные данные пользователей, налоговую отчетность, состояние ресурсных фондов, платежные данные, финансовые средства и их электронные заместители.

Анализ [3 - 5] показывает, что условно типовую структуру СЭК можно разделить на следующие принципиально разные сегменты:

– общая бизнес-инфраструктура и центр обработки данных (ЦОД) СЭК;
– web-сайт (информация, сервисы и инфраструктура публичной сети);
– сетевая инфраструктура;
– автоматизированная система (АС) пользователей СЭК.

Тогда типовой технологический процесс обработки информации в СЭК допустимо представить следующим образом:

1. Подключение пользователя СЭК к web-сайту СЭК;
2. Авторизация пользователя на сервере и системе управления базами данных ЦОД СЭК;
3. Запрос в ЦОД на предоставление услуги или покупку;
4. Ввод, модификация или вывод информации открытого и/или ограниченного доступа;
5. Получение пользователем запрошенного продукта или услуги;
6. Отключение пользователя от ресурсов СЭК.

При этом наиболее уязвимыми с точки зрения информационной безопасности являются процессы:

– передачи идентификационных и аутентификационных данных пользователя СЭК;
– авторизации пользователя в СЭК;
– перевод денежных средств для получения запрошенной услуги или продукта;
– хранение данных ограниченного доступа в ЦОД СЭК.

Таким образом, можно выделить три возможных направления защиты СЭК: бизнес-инфраструктура и ЦОД СЭК, каждое АС пользователя в СЭК, межсегментное взаимодействие АС пользователей СЭК, web-сайта и ЦОД СЭК посредством сетевой инфраструктуры. Однако, как доказано в [4], ни один удаленный пользователь не является полноценной частью СЭК и не должен иметь прав доступа к полному массиву информации, обрабатываемой в ЦОД. Следовательно, при планировании и организации системы защиты СЭК допустимо снизить приоритет защиты удаленной АС пользователя СЭК по отношению к двум другим направлениям защиты, поскольку обеспечение безопасности внутри АС пользователя СЭК в полной мере лежит на самом пользователе.

Требования к защите информации в системах электронной коммерции

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 описывается в стандартах и рекомендациях регулирующих органов. За рубежом решением проблемы обеспечения безопасности СЭК занимается независимый консорциум – Internet Security Task Force (ISTF) – организация, состоящая из представителей и экспертов компаний-поставщиков средств информационной безопасности, электронного бизнеса и провайдеров Интернет - услуг. В Российской Федерации основными регулирующими органами в области электронной коммерции и ее безопасности являются ЦБ России, ФСТЭК России и ФСБ России. В соответствии с их нормативно-методическими и законодательными документами система защиты информации в СЭК должна включать следующие компоненты:

– средства защиты от несанкционированного доступа;
– криптографические средства защиты информации (электронная подпись, криптографические протоколы передачи данных, VPN и т.п.);
– средства распределенной фильтрации трафика;
– средства антивирусной защиты;
– средства предотвращения вторжений;
– средства регистрации событий и выявления инцидентов, связанных с нарушением информационной безопасности;
– средства обеспечения непрерывности и восстановления деятельности;
– регулярный контроль выполнения требований к защите информации на собственных объектах инфраструктуры СЭК.

Поэтому при планировании и выборе состава средств защиты информации в СЭК, особенно государственных, необходимо учитывать наличие представленных выше средств и подсистем.

Планирование состава средств защиты информации в системе электронной коммерции

Наиболее эффективно задачи защиты информации решаются в рамках упреждающей стратегии защиты, когда на этапе проектирования оцениваются потенциально возможные угрозы, планируются и реализуются механизмы защиты от них. С учетом [6], планирование и итоговый выбор состава средств защиты информации в СЭК осуществляется в три этапа, описание которых представлено в таблице 1.

На третьем этапе планирования системы защиты информации в СЭК осуществляется непосредственный выбор возможных вариантов средств защиты. Для перекрытия одних и тех же уязвимостей и угроз, могут быть использованы различные наборы средств и методов защиты, которые отличаются друг от друга показателями качества защиты, наличием сертификата или отсутствием ФСТЭК и ФСБ и стоимостью внедрения, т.е. некоторыми критериями эффективности. Следовательно, решив задачу подбора наиболее рационального сочетания средств защиты информации, можно значительным образом повысить общую защищенность СЭК.

Функциональная модель выбора рационального состава средств защиты информации

Анализ подходов к решению задачи оценки эффективности и выбора альтернатив среди средств защиты информации [6 - 8] показывает, что система защиты, является сложной человеко-машинной системой, разнородной по составляющим компонентам. Поэтому выбор наиболее рационального состава такой системы можно осуществить в основном различными методами попарного сравнения альтернатив, многокритериальной оценки и эвристическими методами, связанными с экспертной оценкой и с последующей интерпретацией результатов.

В соответствии с моделью безопасности с полным перекрытием одним из основных критериев выбора средств защиты является количество угроз, которые способно перекрыть при использовании данное средство. При этом стоимость внедряемых средств защиты, соотношения затрат на защиту не должно превышать стоимость информации и величины максимального риска.

В данной работе при выборе рационального состава средств защиты СЭК предлагается использовать критерии:

- стоимость средства защиты;
- величина предотвращенного ущерба;
- наличие сертификата ФСТЭК/ФСБ;
- количество перекрываемых угроз;
- совместимость с другими средствами защиты.

Данные критерии могут иметь как количественную, так и качественную оценку и иметь в зависимости от ситуации разную значимость. Совокупность оценок по данным критериям и будет указывать на общую эффективность средства защиты. Чем лучше показатель эффективности оцениваемого средства, тем больший приоритет оно будет иметь перед другими альтернативами. Чем более полный, эффективный и рационально подо-

***Таблица 1**. Описание этапов планирования состава средств защиты информации в СЭК*

№1	Название этапа	Описание
1	Определение перечня требований к защищенности СЭК	Определение требований регуляторов и владельца к уровню защищенности СЭК. Составление перечня критичных ресурсов и оценка их стоимости. Определение допустимого уровня риска и ограничений на стоимость системы защиты. Составление модели актуальных для СЭК угроз и оценка рисков. Сравнение риска и принятие решений о стратегии защиты.
2	Определение состава и подсистем защиты СЭК	Определение перечня недопустимых по уровню риска угроз Определение перечня функциональных подсистем защиты информации, которые позволят снизить риски и повысить общий уровень защищенности СЭК за счет нейтрализации выделенных актуальных угроз
3	Выбор средств защиты для внедрения в СЭК	Составление списка возможных альтернатив для каждой из выбранных функциональных подсистем защиты Выбор метода оценки альтернатив Оценка альтернатив для каждой функциональной подсистемы защиты Составление списка необходимых средств защиты для последующего внедрения в СЭК

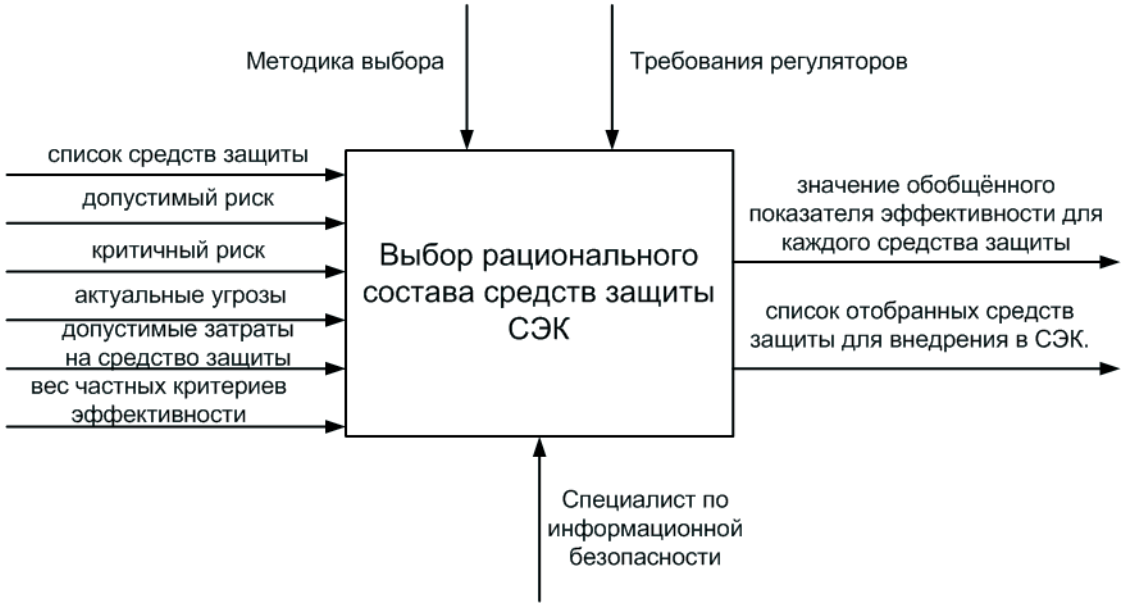

***Рис. 1**. Функциональная модель выбора рационального состава средств защиты информации в нотации IDEF0.*

бранный набор средств защиты используется, тем более высокой будет общая защищённость СЭК.

Модель выбора рационального состава средств защиты информации в СЭК можно представить в виде функциональной диаграммы в нотации IDEF0 (см. рис. 1).

Входными данными модели являются:

- список потенциальных средств защиты;
- приемлемый уровень риска;
- критический уровень риска;
- максимально допустимые затраты на средство защиты;
- список актуальных для СЭК угроз;
- веса частных критериев эффективности средства защиты;

Выходными данными модели являются:

- значение обобщённого показателя эффективности для каждого средства защиты;
- список отобранных средств защиты для внедрения в СЭК.

На рис. 2 представлена декомпозиция рационального состава средств защиты информации.

1. В общем виде выбор рационального состава средств защиты состоит из пяти основных шагов:
2. Формирование модели угроз и оценка рисков, направлен на получение информации об ак-

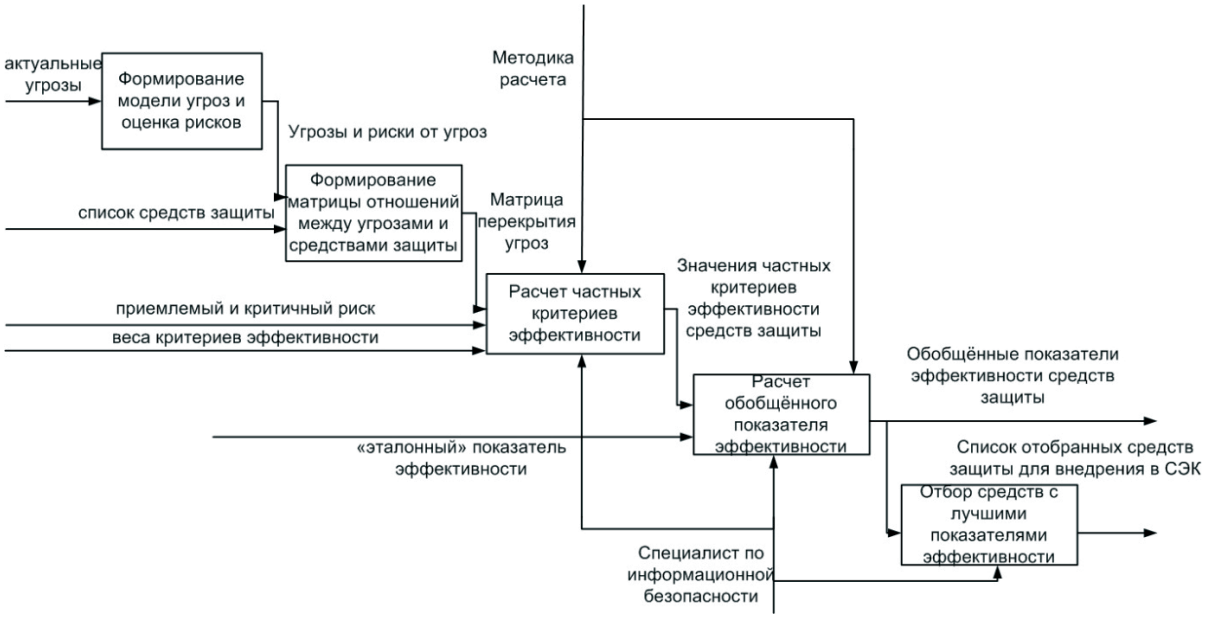

***Рис. 2.** Декомпозиция функциональной модели выбора рационального состава средств защиты информации в СЭК.*

туальных для данной СЭК угрозах, вероятности их возникновения и возможного ущерба от них.

3. Формирование матрицы отношений между выделенными угрозами и средствами защиты, указывает на то, какие угрозы могут быть перекрыты конкретными средствами защиты.

3. Расчет частных показателей эффективности средств защиты. Для выделенных выше пяти критериев эффективности, устанавливаются веса и производится оценка, с учетом информации о рисках, стоимости средств защиты, наличие у средств защиты сертификата ФСБ России или ФСТЭК России и количестве перекрытых средством защиты угроз.

4. На основании рассчитанных значений пяти частных критериев эффективности, приводиться расчет обобщённого показателя эффективности каждого средства защиты.

5. Средства защиты ранжируются по приоритету в зависимости от значения обобщенного показателя эффективности, чем лучше значение показателя эффективности, тем больший приоритет имеет средство защиты. Затем из списка отбираются такие комбинации средств, которые имеют наибольший приоритет и удовлетворяют ограничению по стоимости.

Формализованная процедура выбора рационального состава средств защиты информации

Формализовано процедуру оценки эффективности средств защиты можно представить следующим образом.

$$E = \{TR, SP, KE, RE\}, \quad (1)$$

где TR – множество угроз безопасности СЭК, где $\forall TR_i \in TR, i = 1..n$, n– количеством актуальных угроз, описывается следующим вектором значений $TR_i = \{P, U, R\}$, $P \in [0,1]$ - вероятность реализации угрозы, U - ущерб от реализации угрозы, риск от каждой угрозы $R_i = U_i P_i$. Общий ущерб от реализации все угроз будет определяться как $U_{TR} = \sum_{i=1}^{n} U_i$, а суммарный риск $R_{TR} = \sum_{i=1}^{n} R_i$.

SP – множество средств защиты, $\forall SP_k \in SP$ описывается вектором значений $SP_k = \{C_{SP}\}$, где C_{SP}–стоимость средства защиты.

$KE = \{KE_j\}$, j=1..5 – множество критериев оценки эффективности средств защиты.

RE – множество требований к средствам защиты, определяют критический уровень риска - $R_{крит}$, максимально допустимые затраты на средства защиты C_{max} и приемлемый уровень риска $R_{доп}$.

Отношение между средствами защиты SP и множеством актуальных угроз TR описывается матрицей бинарных отношений $M_{TR}^{SP} = \left\| m_{TRi}^{SPk} \right\|$, где m_{TR}^{SP} отображает наличие и тип связи между TR_i угрозой и SP_k средством защиты. По сути является матрицей перекрытия угроз безопасности ПК средствами защиты ПК.

$$m_{TRi}^{SPk} = \begin{cases} 1, \text{если } TR_i \text{ закрывается } SP_k \text{ средством защиты} \\ 0, \text{если } TR_i \text{ не закрывается } SP_k \text{ средством защиты} \end{cases} \quad (2)$$

Каждому частному критерию оценки эффективности средств защиты экспертным путем выставляется значение в соответствии со следующими правилами.

KE_1- стоимость средства защиты.

$$KE_1 = \begin{cases} 1, \text{если } C_{SP} < 0.5C_{max} \\ 0.5, \text{если } 0.5C_{max} \le C_{SP} < C_{max} \\ 0, \text{если } C_{SP} \ge C_{max} \end{cases} \quad (3)$$

KE_2 - количество перекрываемых угроз, каждым SP_k средством защиты с учетом формулы 2, определяется по формуле 4.

$$KE_2 = \begin{cases} 1, \text{если } \sum_{TRi=1}^{n} m_{TRi}^{SPk} = |TR| \\ 0.5, \text{если } 0.5|TR| \le \sum_{TRi=1}^{n} m_{TRi}^{SPk} < |TR| \\ 0.3, \text{если } 0 < \sum_{TRi=1}^{n} m_{TRi}^{SPk} < 0.5|TR| \\ 0, \text{если } \sum_{TRi=1}^{n} m_{TRi}^{SPk} = 0 \end{cases} \quad (4)$$

KE_3 - величина предотвращенного средством защиты риска от реализации угрозы. Риск от угрозы считается предотвращенным, если она закрывается средством защиты, тогда с учетом формулы 2, оценка показателя KE_3 будет осуществляться по формуле 5.

$$KE_3 = \begin{cases} 1, \text{если } \sum_{TRi=1}^{n} R_{TRi} \overline{m_{TRi}^{SPk}} < R_{доп} \\ 0.5, \text{если } R_{доп} \le \sum_{TRi=1}^{n} R_{TRi} \overline{m_{TRi}^{SPk}} < 0.5R_{крит} \\ 0.3, \text{если } 0.5R_{крит} \le \sum_{TRi=1}^{n} R_{TRi} \overline{m_{TRi}^{SPk}} < R_{крит} \\ 0, \text{если } \sum_{TRi=1}^{n} R_{TRi} \overline{m_{TRi}^{SPk}} \ge R_{крит} \end{cases} \quad (5)$$

KE_4 - наличие сертификата ФСТЭК/ФСБ.

$$KE_4 = \begin{cases} 1, \text{если средство имеет сертификат} \\ 0, \text{если средство не имеет сертификат} \end{cases} \quad (6)$$

KE_5 - совместимость с другими средствами защиты.

$$KE_5 = \begin{cases} 1, \text{если средство совместимо с другими средствами} \\ 0, \text{если средство не совместимо с другими средствами} \end{cases} \quad (7)$$

Эффективность через частные критерии каждого средства защиты $\forall SP_k \in SP$ в идеальном случае будет описываться вектором $EF = \{1,1,1,1,1\}$, который и будет считаться эталоном. Для сравнения вектора эффективности каждого из исследуемых средств защиты EF_{SPK} с эталоном будет ис-

пользоваться метрика, на основе Евклидова расстояния – E, соответственно, чем меньше расстояние между векторами, и чем ближе оно к нулю, тем большую эффективность имеет средство защиты.

$$E(EF, EF_{SPK}) \to min$$

А поскольку каждый частный критерий эффективности в зависимости от особенностей СЭК может иметь разную значимость, то для каждого частного критерия используется весовой коэффициент важности W_j, нормированный в единицу, при этом $\sum_{j=1}^{5} W_j = 1$.

Таким образом, обобщенный показатель эффективности средства защиты определяется по формуле:

$$E(EF, EF_{SPK}) = \sqrt[2]{\sum_{j=1}^{5} W_j (EF_j - EF_{SPKj})^2} \quad (8)$$

Далее средства защиты ранжируются по обобщённому показателю эффективности $E(EF, EF_{SPK}): SP_i < SP_j \Rightarrow E(EF, EF_{SPi}) > > E(EF, EF_{SPj})$ и при формировании рационального состава отбираются из списка те средства защиты, которые имеют минимальное значение $E(EF, EF_{SPK})$ и попадают под заданные ограничения на стоимость.

Заключение

Разработанная модель была автоматизирована и представлена в виде программы. На практике может применяться при планировании состава средств защиты СЭК или при сопровождении существующей системы защиты для ее модификации в процессе управления инцидентами информационной безопасности.

Литература:

1. Холодкова К.С. Анализ рынка электронной коммерции в России // Современные научные исследования и инновации. 2013. № 10 (30). С. 17. [Электронный ресурс]. URL: http://web.snauka.ru/issues/2013/10/26760 (дата обращения: 19.10.2015).
2. Абдеева З.Р. Проблемы безопасности электронной коммерции в сети интернет // Проблемы современной экономики. 2012. № 1. С. 172-175.
3. Каменщиков А. А., Олейников А. Я., Разинкин Е. И., Чусов И. И., Широбокова Т. Д. Обеспечение интероперабельности в области элек тронной коммерции // Журнал радиоэлектроники. 2015. № 6. С. 14. [Электронный ресурс]. URL: http://jre.cplire.ru/iso/jun15/17/text.html (дата обращения 19.10.2015).
4. Тищенко Е.Н., Буцик К.А., Деревяшко В.В. Концепция защиты web-сайтов государственных информационных систем // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: материалы IV Всероссийской научно-практической конференции, г. Волгоград, 23-24 апр. 2015. С. 70-73.
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. Яндыбаева Э.Э., Машкина И.В. Разработка модели планирования используемых средств защиты информации для информационных систем электронных торговых площадок // Вестник Уфимского государственного авиационного технического университета. 2015. Т. 19. № 1. С. 264-269.
7. Оладько В.С. Оценка эффективности средств защиты персонального компьютера // Евразийский союз ученых (ЕСУ). 2015. № 3 (12). С. 130-132.
8. Чабонян В.А., Шалахов Ю.И. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2013. № 1 (1). С. 17-27.

Рецензент: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им.Н.Э.Баумана, v.tsirlov@bmstu.ru

THE MODEL FOR THE CHOICE OF A RATIONAL COMPOSITION OF THE PROTECTION SYSTEM IN E-COMMERCE

***Oladko V.S.*[2]**

The article deals with the problem of information security in e–commerce. Assignment of e–commerce and its area of application defined. The main types of e–commerce systems and types of data stored and processed in such systems are allocated. Standard structure of e–commerce system is represented. It is divided into four segments. There are business infrastructure, data center, web–sites, network infrastructure,

2 Vladlena Oladko, Associate Professor of Information Security, Ph.D., Volgograd State University, Volgograd, oladko.vs@yandex.ru

and custom automated systems. The technological process of the system in the e–commerce described. The most vulnerable are the processes: the transfer of user identity, user authorization, funds transfer or electronic assistants, confidential data storage in the data center. On the basis of the allocated segments of the main directions of organization of protection defined. Regulatory requirements for the composition of the protection of information in the e–commerce represented. Analyzed and described the stages of planning of the information security: the definition of the list of requirements for the security of the system, the composition and security subsystems, and the choice of remedies for implementation. Private indicators to assess the effectiveness of the protection described. There are the cost of protection; the value of avoided damage; a certificate FSTEC / FSB; the number of overlapping threats; compatibility with other means of protection. Functional model of rational choice of the composition of the protection system in the e–commerce system is developed and is described in the IDEFO notation. The formal description of the multi–criteria choice of rational composition of protection system developed.

***Keywords**: information security, multi–criteria evaluation, security, security system, electronic trading platform, e–payment system, incident, risk, threat, harm, efficiency*

References:

1. Kholodkova K.S. Analiz rynka elektronnoy kommertsii v Rossii, Sovremennye nauchnye issledovaniya i innovatsii. 2013. No 10 (30). P. 17. [Elektronnyy resurs]. URL: http://web.snauka.ru/issues/2013/10/26760 (data obrashcheniya: 19.10.2015).
2. Abdeeva Z.R. Problemy bezopasnosti elektronnoy kommertsii v seti internet, Problemy sovremennoy ekonomiki. 2012. No 1, pp. 172-175.
3. Kamenshchikov A. A., Oleynikov A. Ya., Razinkin E. I., Chusov I. I., Shirobokova T. D. Obespechenie interoperabel'nosti v oblasti elektronnoy kommertsii, Zhurnal radioelektroniki. 2015. No 6. P. 14. [Elektronnyy resurs]. URL: http://jre.cplire.ru/iso/jun15/17/text.html (data obrashcheniya 19.10.2015).
4. Tishchenko E.N., Butsik K.A., Derevyashko V.V. Kontseptsiya zashchity web-saytov gosudarstvennykh informatsionnykh system, Aktual'nye voprosy informatsionnoy bezopasnosti regionov v usloviyakh globalizatsii informatsionnogo prostranstva: materialy IV Vserossiyskoy nauchno-prakticheskoy konferentsii, g. Volgograd, 23-24 apr. 2015. P. 70-73.
5. Yandybaeva E.E., Mashkina I.V. Otsenka aktual'nosti ugroz informatsionnoy bezopasnosti v informatsionnoy sisteme elektronnoy torgovoy ploshchadki, Bezopasnost' informatsionnykh tekhnologiy. 2014. No 1, pp. 41-44.
6. Yandybaeva E.E., Mashkina I.V. Razrabotka modeli planirovaniya ispol'zuemykh sredstv zashchity informatsii dlya informatsionnykh sistem elektronnykh torgovykh ploshchadok, Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta. 2015. T. 19. No 1, pp. 264-269.
7. Olad'ko V.S. Otsenka effektivnosti sredstv zashchity personal'nogo komp'yutera, Evraziyskiy soyuz uchenykh (ESU). 2015. No 3 (12), pp. 130-132.
8. Chabonyan V.A., Shalakhov Yu.I. Analiz i sintez trebovaniy k sistemam bezopasnosti ob"ektov kriticheskoy informatsionnoy infrastruktury, Voprosy kiberbezopasnosti. 2013. No 1 (1), pp. 17-27.