Published in the Russian Federation
Sochi Journal of Economy
Has been issued since 2007.
ISSN: 1996-9005
Vol. 39, Is. 1, pp. 42-50, 2016

www.vestnik.sutr.ru

UDC 33 + 004.56

The Risk Assessment of the Implementation of Network Attacks on Information Infrastructure on the Example of Tourism Enterprises

[1] Sophia Yu. Mikova
[2] Vladlen S. Oladko

[1] Volgograd state university, Russian Federation
400062 Volgograd region, Volgograd, University Avenue, 100
Laboratory researcher
E-mail: sofya_mikova@mail.ru
[2] Volgograd State University, Russian Federation
400062 Volgograd region, Volgograd, University Avenue, 100
PhD (Engineering), Assistant Professor
E-mail: oladko.vs@yandex.ru

Abstract

The article is devoted the problem of the risk assessment of the implementation of network attacks on information infrastructure of tourism enterprises. Problems of information infrastructure security companies analyzed. Typical business processes that reflect the main activities of tourism organizations in the market studied. The objects and subjects of tourist organizations and their interaction analyzed. The purpose of protecting the tourist organizations of the system identified. Information security risk assessment tasks considered. The model of risk management from the implementation of network attacks on information infrastructure of tourism enterprises compiled by the authors.

Keywords: information security, risk assessment, network attack, network anomaly, tourism, risk management, information infrastructure.

Введение

Глобальная информатизация и автоматизация на сегодняшний день охватила все важнейшие виды экономической деятельности. Практически каждая организация в рамках своей деятельности использует электронную информацию, средства обработки хранения и передачи данных, ресурсы локальных и глобальных сетей, которые образуют ее информационную инфраструктуру. В свою очередь эта информационная инфраструктура – не только инструмент для обмена информацией, но хранилище конфиденциальной информации, персональных, корпоративных и платежных данных, которые в результате воздействия различных событий и инцидентов могут быть подвержены риску. Поэтому для предприятия, вне зависимости от сферы его деятельности важно обеспечивать периодический контроль и мониторинг различных типов рисков, которые могут выражаться через материальный и не материальный ущерб, нарушение экономической безопасности, потерю эффективности деятельности, а самом худшем случае полному прекращению деятельности. А поскольку при реализации бизнес-процессов практически каждое предприятие использует электронные данные и информационную инфраструктуру, то помимо экономических рисков необходимо учитывать риски связанные с нарушением

информационной безопасности. Это связано с несколькими факторами:

1) безопасность, в соответствии с [1], является неотъемлемой составляющей успешного функционирования предприятия и его конкурентоспособности на рынке:

Конкурентоспособность = эффективность + безопасность.

2) в зависимости от категории доступа и класса обрабатываемой на предприятии информации, в соответствии законом РФ №149 ФЗ «Об информации, информационных технологиях и о защите информации» [2], к ней предъявляются различные требования по защите, которые могут носить как рекомендательный характер, так и быть обязательными к исполнению.

Таким образом, адекватная и своевременная оценка рисков, позволит не только спрогнозировать и выявить наиболее опасные для предприятия угрозы и инциденты информационной безопасности (ИБ), но и подобрать комплекс наиболее эффективных средств и механизмов защиты. Состав и требования к которым определяются требованиями законодательства, нормативно-методической документацией регулирующих органов, таких как ФСТЭК России, ФСБ России, Роскомнадзора и др., а также внутренними документами соглашениями и регламентами самого предприятия. Принятие и внедрение в информационную инфраструктуру предприятия подобных защитных контрмер будет способствовать исключению или минимизации рисков от различных источников. Как правило, источниками риска ИБ являются угрозы случайного характера и целенаправленные атаки злоумышленника на информацию и объекты информационной инфраструктуры (ИИ) предприятия. Из-за неправильной оценки рисков, связанных с атаками на информационную инфраструктуру, существует возможность понести значительный ущерб в виде потери персональных данных, порчи программного обеспечения, разрушения конкуренции атакованной компании. Наиболее известным примером подобного случая является самая протяженная DDoS-атака, зафиксированная службой компании «Лаборатория Касперского» в России, которая продолжалась 80 дней 19 часов 13 минут 05 секунд и была нацелена на туристический сайт. Таким образом, решение задач, связанных с оценкой и управлением рисками ИБ является актуальным. В данной работе предлагается рассмотреть проблему управления рисками от реализации сетевых атак на примере ИИ туристического предприятия. Выбор обусловлен тем, что туристические предприятия являются одним из быстро развивающихся направлений экономики (по данным официальной статистики [3] за последние 4 года рост составил 27 %), которые, в своей деятельности, активно применяют информационные технологии, средства электронной коммерции и ресурсы глобальной сети интернет.

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 методология функционального моделирования IDEF0.

Проблемы безопасности ИИ туристической организации

Анализ источника [4] показывает, что типовыми бизнес-процессами, осуществляющими основные направления деятельности туристической организации на рынке услуг являются (см. рисунок 1): принятие заказа на выдачу путёвки и осуществление заказа клиента.

Рис. 1. Бизнес-процессы туристической организации

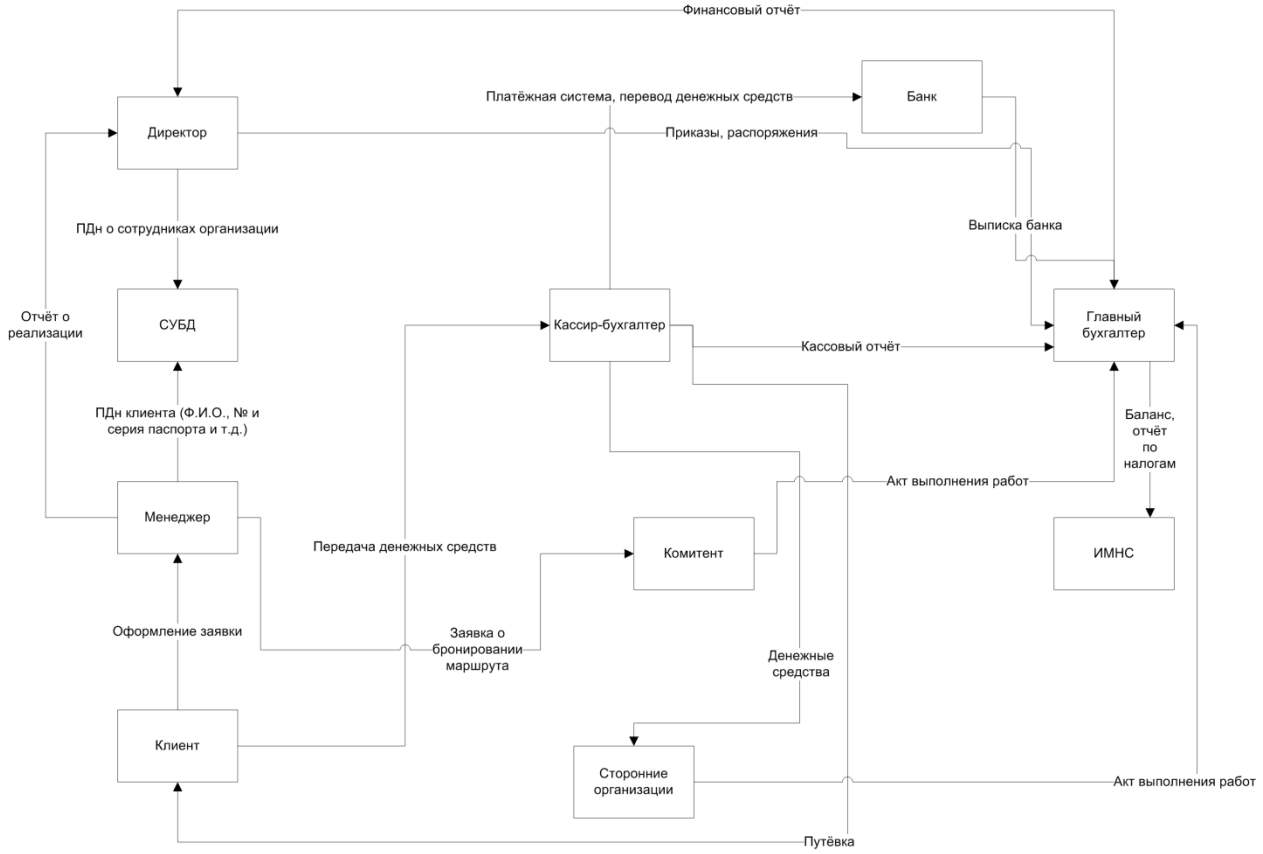

Рис. 2. Объекты информационной инфраструктуры и субъекты взаимодействия

Для реализации данных бизнес-процессов, в том числе и их автоматизации, осуществляется тесное взаимодействие субъектов и объектов экономической деятельности, элементов информационной инфраструктуры, различных ресурсов и типов данных. На рисунке 2 представлена схема, описывающая объекты и субъекты туристической организации, и их взаимодействие. С точки зрения информационной безопасности особое внимание следует уделить таким субъектам, как системы управления базами данных (СУБД), сеть передачи данных и банк, поскольку именно на них в первую очередь

направлены атаки злоумышленника и риск от их успешной реализации будет наиболее существенен.

Сценарий реализации подобной сетевой атаки злоумышленника и ее последствий можно описать следующим образом:

1) клиент, оформляя заявку на путёвку, указывает свои персональные данные (Ф.И.О., дата и место рождения, серия и номер паспорта, семейное положение, место работы, номер банковской карты и т.д.), которые далее передаются на хранение менеджером в СУБД организации, для этого, как правило, используются средства ввода информации и осуществляется передача данных по корпоративной сети.

2) злоумышленник проводит сканирование сетевого трафика, на предмет выявления уязвимостей приложений, используемых организацией, например СУБД;

3) злоумышленник используя, выявленную в СУБД, уязвимость проводит целенаправленную атаку с использованием вредоносного кода или специализированных команд и в случае успеха осуществляет вторжение в систему;

4) злоумышленник получает несанкционированный доступ к данным в СУБД

В результате реализации подобного сценария атаки осуществляется утечка конфиденциальной информации, нарушение целостности и доступности данных и сервисов СУБД. По версии Аналитического центра InfoWatch в I полугодии 2015 года в мире зарегистрировано 723 случая утечки конфиденциальной информации, что на 10 % превышает количество утечек, зарегистрированных за аналогичный период 2014 года. 90 % утечек связаны с компрометацией персональных данных. За исследуемый период скомпрометированы более 262 млн записей, в том числе платежная информация. При этом наиболее распространенными являются именно сетевые атаки, на долю которых приходится около 44 % всех атак на корпоративные системы [5].

Также клиент, оплачивая путёвку, может воспользоваться электронной платёжной системой. Уязвимыми местами при этом являются: пересылка платежных и других сообщений между банками, между банком и банкоматом, между банком и клиентом. В данном случае злоумышленником может быть совершена атака IP-spoofing, состоящая в изменении поля «адрес отправителя» IP-пакета. Целью IP-spoofing обычно является вызов DoS (отказа в обслуживании) или провокация DDoS (распределённой атаки с целью вызова DoS). Таким образом, злоумышленник может находиться за пределами сети и при этом иметь доступ к внутреннему трафику, перехватывая всю необходимую ему информацию.

Приведенная аналитика позволяет сделать вывод, что туристические предприятия чувствительны к угрозам ИБ, поскольку данные предприятия используют для автоматизации бизнес-процессов информационную инфраструктуру, обрабатывают конфиденциальную информацию о клиентах и сотрудниках, тесно взаимодействуют с электронными платежными системами, передают по глобальным сетям данные ограниченного доступа. Таким образом, информационная безопасность туристической фирмы может быть обеспечена только при условии строгого соблюдения норм в области защиты персональных данных и конфиденциальной информации. Кроме того, туризм – одна из отраслей, наиболее часто использующих платежи через интернет. Поэтому одной из самых важных задач туристических компаний является безопасная обработка банковских транзакций реализация всех требований стандарта защиты данных в индустрии платежных систем и карт, а также интернет банкинга.

Задачи оценки рисков информационной безопасности

Как показывает анализ [6-8] целями любой системы защиты туристического предприятия является обеспечение стабильного функционирования объекта, предотвращение угроз его безопасности, защита законных интересов организации от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения персональных данных клиентов и сотрудников, служебной информации, обеспечение нормальной производственной деятельности всех подразделений. Оценка рисков информационной безопасности туристического предприятия позволяет определить, какие мероприятия эффективны для минимизации и предотвращения рисков, а какие нет. Оценка рисков информационной безопасности состоит из трех основных этапов: идентификация угроз, идентификация уязвимостей, идентификация активов (см. рисунок 3).

Рис. 3. Оценка рисков информационной безопасности

Каждая идентифицированная угроза безопасности информации, может быть охарактеризована через такие показатели как вероятность реализации и потенциальный ущерб. Размер ущерба от реализации угрозы в отношении информации или актива предприятия зависит от [9]:

— от стоимости и категории доступа информации;

— стоимости актива, который подвергается риску;

— от степени разрушительности воздействия на информацию или выражаемой, выражаемой в виде коэффициента разрушительности.

Соотношение между ущербом, степенью разрушительности и вероятностью возникновения позволяет оценить уровень риска от реализации угрозы и степень допустимости каждой угрозы. Определение значения риска ИБ связано с результатами оценки риска и выработкой мер по контролю риска, поэтому это является важным и сложным этапом в процессе оценки риска. В целях предотвращения атак или минимизации рисков от них, туристические организации используют различные контрмеры для защиты своих активов, примером которых являются программные средства, обеспечивающие защиту от утечки и искажения конфиденциальной информации. Большинство атак успешно реализуется из-за неправильной конфигурации устройств сети, низкого уровня защищённости, своевременно не устраненных известных или неизвестных уязвимостей, с помощью социальной инженерии. Дальнейшее развитие атаки обычно происходит через компьютерную сеть предприятия, так как внутренний сетевой трафик имеет большую степень доверия. Одним из подходов к контролю над состоянием сети является регулярный мониторинг сетевых аномалий, возникающих в сетевом трафике. Своевременное выявление и подробный анализ сетевой аномалии позволяет специалистам по информационной безопасности обнаружить атаку злоумышленника на ранней стадии её проведения [10] и выработать меры по блокированию атаки и снижению рисков, связанных с ее последствиями.

Таким образом, оценка рисков является одним из важнейших этапов в управлении рисками информационной безопасности. На практике оценка рисков информационной безопасности является довольно сложным и полным неопределенности процессом. Неопределенность, существующая в процессе оценки, является основным фактором, влияющим на эффективность оценки риска информационной безопасности. Поэтому она должна быть принята во внимание при оценке рисков.

Модель управления рисками от реализации сетевых атак на информационную инфраструктуру туристических предприятий

Итак, оценив риски, необходимо выбрать контрмеры, которые идентифицируют риски и их факторы, а также способствуют исключению или уменьшению рисков, т.е. реализовать

цикл управления риском (см. рисунок 4). Управление рисками предполагает оценку стоимости реализации контрмер, которая должна быть меньше величины возможного ущерба от угроз безопасности информации. Под ущербом, в данном случае, понимаются последствия от утечки, искажения, нарушения доступности информации. Ущерб может определяться экспертным путем, на основе анализа статистики последствий и тяжести инцидентов ИБ за определенный период в исследуемой или подобной организации.

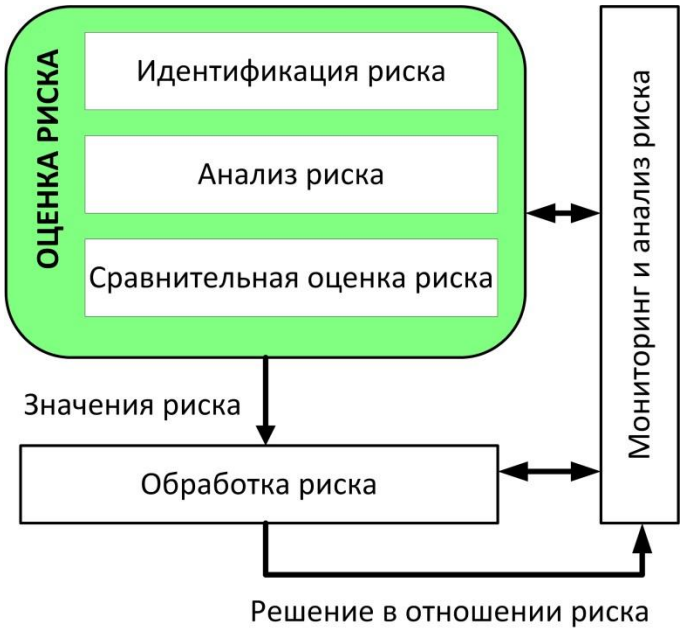

Рис. 4. Обобщенный цикл управления риском

Далее специалист в области ИБ устанавливает уровень приемлемого риска ИБ, оценивает риски ИБ от каждой угрозы из сформированного списка актуальных для организации угроз, определяет ценность ресурсов и выбирает стратегию защиты от угроз в зависимости от значения рассчитанного риска. При разработке стратегии управления рисками возможно несколько подходов:

– уменьшение риска;
– предотвращение риска;
– принятие риска.

Таким образом, управление рисками ИБ туристической организации должно включать следующие этапы, позволяющие:

1. Оценить риск и определить потребности.
2. Установить централизованное управление.
3. Внедрить необходимые политики и соответствующие средства контроля.
4. Содействовать осведомленности сотрудников туристической организации.
5. Осуществлять мониторинг и оценивать эффективность политик и механизмов контроля.

В результате выполнения этих этапов будут получены данные, позволяющие проанализировать уровень обеспечения информационной безопасности организации в текущий момент, определить наиболее уязвимые места в обеспечении защиты информации организации, определить стоимостное обоснование затрат на обеспечение ИБ и минимизировать издержки на обеспечение ИБ.

Авторами была разработана концептуальная модель управления рисками от реализации сетевых атак на информационную инфраструктуру туристических предприятий, представленная в виде схемы на рисунке 5.

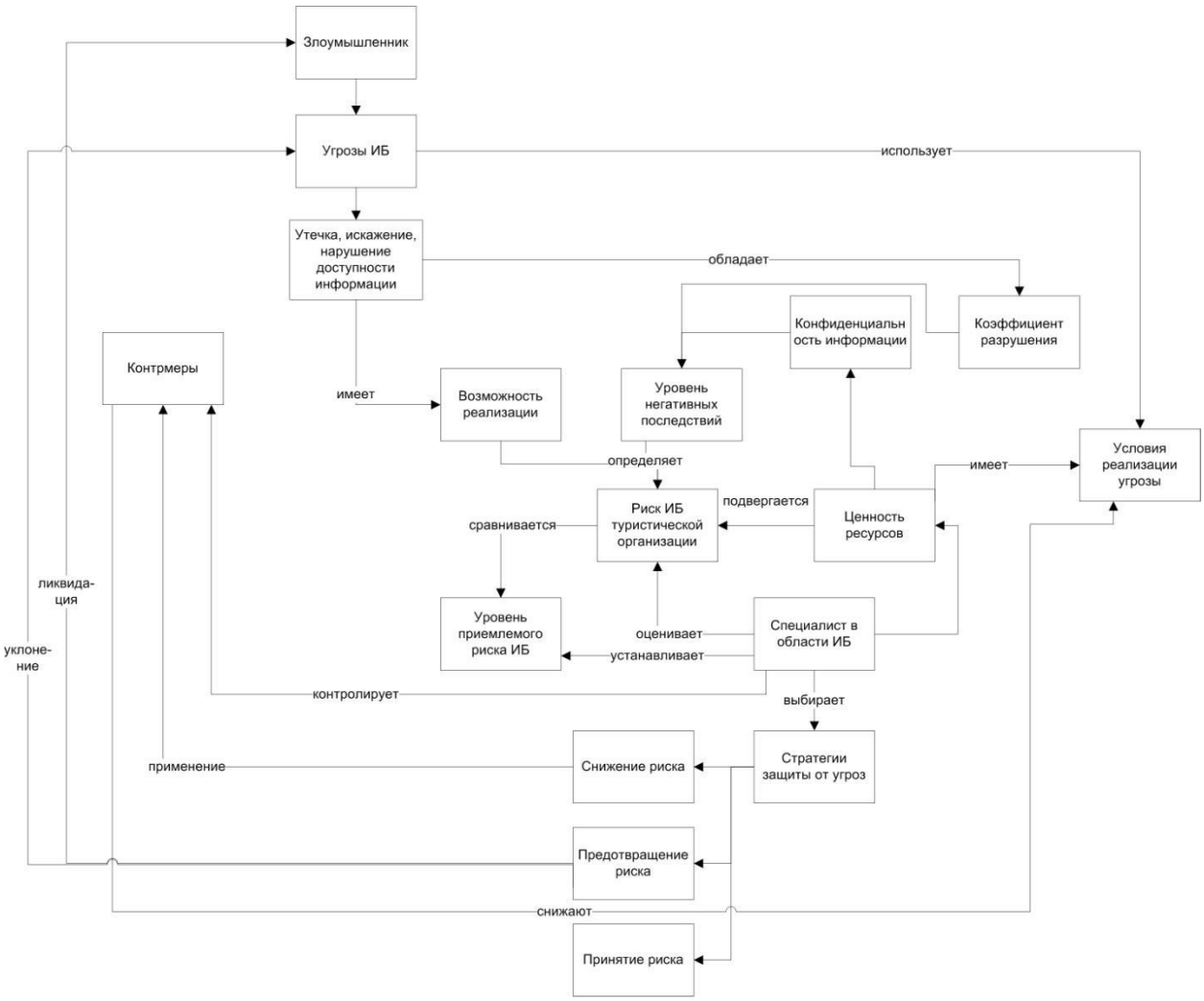

Рис. 5. Модель управления рисками от реализации сетевых атак на информационную инфраструктуру туристических предприятий

Данная модель была автоматизирована и представлена в виде программного прототипа, который может быть использован в качестве средства поддержки принятия решений при разработке и реализации политики ИБ на туристическом предприятии, в процессе проектирования системы защиты и управления информационной безопасностью.

Заключение

В настоящее время сетевые атаки чаще всего нацелены на компрометацию персональных данных пользователей сервиса, в том числе и платежной информации. Поэтому сетевая инфраструктура туристической организации должна обладать различными, в том числе и проактивными механизмами защиты информации, например, системой обнаружения аномалий и вторжений. А для выбора наиболее эффективного и рационального состава средств защиты, позволяющего повысить общий уровень защищенности информационной инфраструктуры туристического предприятия и противостоять наиболее опасным угрозам, необходимо регулярно применять механизмы управления рисками. Предложенная модель управления рисками может применяться на разных стадиях жизненного цикла ИИ туристического предприятия и в качестве средства поддержки принятия решений при разработке и реализации политики ИБ на туристическом предприятии, в процессах проектирования и сопровождения системы защиты и управления информационной безопасностью.

Примечания:

1. Сенчагов В.К. Экономическая безопасность России: Общий курс: Учебник под ред. В.К. Сенчагова. 2-е изд. М.: Дело, 2005. 896 с.

2. 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 23.03.2016).

3. Платное обслуживание населения в России – 2015: Статистический сборник / Росстат. М., 2015. 111 с.

4. Моисеева Н.К. Стратегическое управление туристической фирмой. М.: Финансы и статистика, 2009. 200 с.

5. Микова С.Ю., Оладько В.С. Сетевые аномалии и причины их возникновения в экономических информационных системах//Экономика и социум. 2015. №3 (16). URL: http://www.iupr.ru/domains_data/files/zurnal_16/Mikova%20Informacionnye%20i%20kommu nikativnye%20sistemy.pdf (дата обращения 23.03.2016).

6. Симаворян С.Ж., Симонян А.Р., Ивановна У.Е., Симонян Р.А. Системный подход к проектированию интеллектуальных систем защиты информации // Sochi journal of economy. 2013. №4-2 (28). С. 128-132.

7. Оладько В.С. Модель выбора рационального состава средств защиты в системе электронной коммерции//Вопросы кибербезопасности. 2016. № 1(14). С. 17-23.

8. Трофимова Н.В., Антамошкин О.А., Антомошкина О.А., Ничерпорчук В.В. Информационно-управленческие методы обеспечение безопасности туристической деятельности // Технологии гражданской безопасности. 2013. Т10. № 2(36). С. 62-66.

9. Нестеров С. Управление рисками. Модель безопасности с полным перекрытием. URL: http://www.intuit.ru/studies/courses/531/387/lecture/8990 (дата обращения 22.03.2016)

10. Оладько В.С., Микова С.Ю., Нестеренко М.А., Садовник Е.А. Причины и источники сетевых аномалий//Молодой ученый. 2015. № 22 (102). С. 158-161.

References:

1. V.K. Senchagov. Ekonomicheskaya bezopasnost' Rossii: Obshchii kurs: Uchebnik pod red. V.K. Senchagova . 2-e izd. M.: Delo, 2005. 896 s., 2005.

2. 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 23.03.2016).

3. Platnoe obsluzhivanie naseleniya v Rossii 2015: Statisticheskii sbornik/Rosstat. M.,2015. 111 s.

4. Moiseeva, N.K. Strategicheskoe upravlenie turisticheskoi firmoi. M.: Finansy i statistika, 2009. 200 s.

5. Mikova S.Yu., Olad'ko V.S. Setevye anomalii i prichiny ikh vozniknoveniya v konomicheskikh informatsionnykh sistemakh//Ekonomika i sotsium. 2015. №3 (16). URL: http://www.iupr.ru/domains_data/files/zurnal_16/Mikova%20Informacionnye%20i%20kommu nikativnye%20sistemy.pdf (data obrashcheniya 23.03.2016).

6. Simavoryan S.Zh., Simonyan A.R., Ivanovna U.E., Simonyan R.A. Sistemnyi podkhod k proektirovaniyu intellektual'nykh sistem zashchity informatsii // Sochi journal of economy. 2013. №4-2 (28). S. 128-132.

7. Olad'ko V.S. Model' vybora ratsional'nogo sostava sredstv zashchity v sisteme elektronnoi kommertsii //Voprosy kiberbezopasnosti. 2016. № 1(14). S. 17-23.

8. Trofimova N.V., Antamoshkin O.A., Antomoshkina O.A., Nicherporchuk V.V. Informatsionno-upravlencheskie metody obespechenie bezopasnosti turisticheskoi deyatel'nosti // Tekhnologii grazhdanskoi bezopasnosti. 2013. T10. № 2(36). S. 62-66.

9. Nesterov S. Upravlenie riskami. Model' bezopasnosti s polnym perekrytiem. URL: http://www.intuit.ru/studies/courses/531/387/lecture/8990 (data obrashcheniya 22.03.2016)

10. Olad'ko V.S., Mikova S.Yu., Nesterenko M.A., Sadovnik E.A. Prichiny i istochniki setevykh anomalii//Molodoi uchenyi. 2015. № 22 (102). S. 158-161.

УДК 33 + 004.56

Оценка рисков от реализации сетевых атак на информационную инфраструктуру на примере туристических предприятий

[1] Софья Юрьевна Микова
[2] Владлена Сергеевна Оладько

[1] Волгоградский государственный университет, Российская Федерация
400062 Волгоградская область, г. Волгоград, проспект Университетский, 100
Лаборант-исследователь
E-mail: sofya_mikova@mail.ru
[2] Волгоградский государственный университет, Российская Федерация
400062 Волгоградская область, г. Волгоград, проспект Университетский, 100
Кандидат технических наук, доцент
E-mail: oladko.vs@yandex.ru

Аннотация. В статье рассмотрена актуальная проблема оценки рисков от реализации сетевых атак на информационную инфраструктуру туристических предприятий. Выделены проблемы безопасности информационной инфраструктуры туристической организации. Рассмотрены типовые бизнес-процессы, которые отражают основные направления деятельности туристической организации на рынке услуг. Также проанализированы объекты и субъекты туристической организации, их взаимодействие. В работе выделены цели системы защиты туристической организации и рассмотрены задачи оценки рисков информационной безопасности. В результате составлена модель управления рисками от реализации сетевых атак на информационную инфраструктуру туристических предприятий.

Ключевые слова: информационная безопасность, оценка рисков, сетевая атака, сетевая аномалия, туризм, управление рисками, информационная инфраструктура.