УДК 379.85

ОБЕСПЕЧЕНИЕ ЦИФРОВОЙ БЕЗОПАСНОСТИ В ТУРИЗМЕ

Еремин Н.В.

Студент 1 курса направления подготовки 43.03.02 туризм (туристический бизнес), ЧОУ ВО ЮУ (ИУБиП)

Научный руководитель: Григорьева Н.С., доцент, к.э.н.

Аннотация: В статье проанализирована деятельность туристского предприятия в области информационной безопасности и представлены методы ее повышения.
Ключевые слова: туризм, цифровизация, безопасность, программные продукты, антивирус.

ENSURING DIGITAL SECURITY IN TOURISM

Eremin N.V.

Abstract: The article analyzes the activities of a tourist enterprise in the field of information security and presents methods for its improvement.
Keywords: tourism, digitalization, security, software, antivirus.

Современное развитие мировой экономики характеризуется всё большей зависимостью рынка от значительного объёма информационных потоков. Несмотря на всевозрастающие усилия по созданию технологии защиты данных, их уязвимость не только не уменьшается, но и постоянно возрастает [1]. Поэтому актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи, всё более усиливается. Проблема обеспечения внутренней информационной безопасности становится все более актуальной для российских компаний [2]. Это связано и с обострением конкурентной борьбы на внутренних рынках, и с выходом компаний на международный уровень. Многие из них уже не могут обеспечить защиту коммерческой информации собственными силами и вынуждены пользоваться услугами профессионалов.

Данная работа направлена на улучшение структуры информационной безопасности туристской организации. На сегодняшний день информационная безопасность требует более пристального внимания со

стороны руководства и грамотной программы по обеспечению информационной безопасности фирмы, потому что появилось достаточно много конкурентов, которые вряд ли упустят возможность воспользоваться, например, клиентской базой.

Для того, чтобы оградить себя от утечки конфиденциальной информации, турфирма осуществляет следующую политику информационной безопасности:

1) установка на всех компьютерах антивирусного программного обеспечения и регулярное его обновление;

2) использование межсетевого экрана - программного или аппаратного маршрутизатора, совмещённого с firewall (особой системой, осуществляющей фильтрацию пакетов данных), он не пропускает наружу внутренние пакеты локальной сети предприятия и блокирует доступ к ней чужих компьютеров;

3) защита электронной почты (поставлен антивирус на корпоративный сервер электронной почты) [3];

4) использование Proxy-сервера. Во-первых, это позволит незначительно сократить интернет-трафик. Во-вторых, это позволит скрыть от посторонних глаз внутренние имена и адреса компьютеров. И, в-третьих, это позволит выявлять нарушителей, подключившихся к сети предприятия с целью получения доступа в Интернет [4].

5) постоянный мониторинг состояния компьютеров пользователей и локальной сети;

6) документооборот предприятия в большей степени ведётся в электронном виде [5].

К сожалению, предоставленные средства не могут обеспечить информационную безопасность в полной мере, межсетевой экран не в состоянии решить все проблемы безопасности корпоративной сети, а также существуют угрозы безопасности, от которых межсетевые экраны не могут защитить. Прокси-сервер уменьшает скорость передачи данных [6].

На сегодняшний день существует большой арсенал методов обеспечения информационной безопасности, предлагается осуществить следующие действия:

1) создать приложение к программе Консультант Плюс, которое будет автоматически высылать на электронную почту введённые изменения в законодательстве РФ в отношении оформления и формы предоставления услуг туристской организации, что значительно сократит время, проведённое в глобальной сети [7].

2) установить средства идентификации и аутентификации пользователей (так называемый комплекс 3А) [8];

3) установить средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;

4) установить средства восстановления системы защиты информации;

5) обеспечить физическую охрану средств вычислительной техники и магнитных носителей;

6) установить аппарат для уничтожения ненужных документов [9].

«Комплекс 3А» включает аутентификацию (или идентификацию), авторизацию и администрирование. Идентификация и авторизация - это ключевые элементы информационной безопасности. При попытке доступа к информационным активам функция идентификации дает ответ на вопрос: «Кто вы?» и «Где вы?», а также являетесь ли вы авторизованным пользователем сети. Функция авторизации отвечает за возможность доступа конкретного пользователя к различным ресурсам. Функция администрирования заключается в наделении пользователя определенными идентификационными особенностями в рамках данной сети и определении объема допустимых для него действий.

Системы шифрования позволяют минимизировать потери в случае несанкционированного доступа к данным, хранящимся на жестком диске или ином носителе, а также перехвата информации при ее пересылке по электронной почте или передаче по сетевым протоколам. Задача данного

средства защиты – обеспечение конфиденциальности. Основные требования, предъявляемые к системам шифрования – высокий уровень криптостойкости и легальность использования.

Описанные способы обеспечения информации предприятия являются мало затратными и достаточно эффективными, в целях обеспечения безопасности предприятия от множества угроз информационной безопасности как извне, так и изнутри. Хотя существуют и другие способы, вроде тотальной слежки за сотрудниками, их эффективность значительно ниже и не попадает под категорию простых средств. Кроме того, не стоит забывать, что обеспечение информационной безопасности не должно наносить вред деятельности предприятия или создавать помехи для работы сотрудников, ведь, в конечном счёте, любые бизнес-процессы предприятия должны быть направлены на обеспечение основной деятельности, а не вспомогательных служб.

Библиографический список

1. Григорьева Н.С., Александрова К.В. Цифровые технологии как средство восстановления предприятий туриндустрии после кризиса 2020 года // Интеллектуальные ресурсы – региональному развитию. – 2020. – № 2. – С. 326-331.
2. Григорьева Н.С. Проблемы и перспективы развития сферы туризма в условиях цифровой экономики // Интеллектуальные ресурсы – региональному развитию. – 2019. Т.5, №2. – С. 47-52.
3. Григорьева Н.С. Проблемы и перспективы развития туризма в Ростовской области // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2019. – №3 (106). – С. 31-35.
4. Григорьева Н.С. Возможности и перспективы развития сельского туризма в Ростовской области // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2020. – № 1 (116). – С. 24-28.
5. Григорьева Н.С. Повышение информационной доступности к туристской информации региона // Правовестник. – 2019. – № 1 (12). – С. 8-10.
6. Григорьева Н.С. Образовательные технологии в подготовке кадров для сферы туризма // Правовестник. – 2019. – № 3 (14). – С. 75-78.
7. Григорьева Н.С., Шевердина И.В. Ключевые параметры поддержки развития делового туризма в Ростовской области // Интеллектуальные ресурсы – региональному развитию. – 2018. – Т.4, №1. – С. 22-26.
8. Григорьева Н.С. Развитие регионального туризма в современных условиях // Ученые записки Института управления, бизнеса и права. Серия: Экономика. – 2017. – № 5. – С. 373-378.
9. Григорьева Н.С. Повышение конкурентоспособности предприятий гостиничного бизнеса Ростовской области // Государственное и муниципальное управление. Ученые

записки. – 2020. – № 1. – С. 115-120.