**УДК 338.242.2**
**DOI: 10.15587/2313-8416.2015.56347**

# СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РИСКИ ИХ ИСПОЛЬЗОВАНИЯ НА ТУРПРЕДПРИЯТИЯХ

**© А. С. Сидора, С. А. Погасий**

*Исследовано внедрение информационных технологий на предприятиях туристской индустрии, рассмотрены компоненты, которые в настоящее время входят в постоянное использование на туристских предприятиях, для улучшения управления предприятием и скорости обслуживания клиентов. Рассмотрены возможные риски при использовании и передаче информации о предприятии, клиентах и каким образом их возможно уменьшить*
***Ключевые слова:*** *туризм, информационные технологии, системы автоматизации, виртуальные базы, информационные риски*

*An introduction of information technologies in enterprises of the tourism industry is investigated. The components that are currently included in the permanent use in the tourism enterprises to improve enterprise management and speed of customer service are discussed. The possible risks are considered associated with the use and transfer of information about the company, customers, and how they might be reduced*
***Keywords:*** *tourism, information technologies, systems of automation, virtual bases, informative risks*

## 1. Введение

В последнее время информационные технологии оказывают сильное влияние на изменение организационной структуры и производственного процесса на предприятиях. Туризм является информационно насыщенной деятельностью, которая постоянно требует сбора, обработки, применения и передачи информации. Туристская услуга постоянно находится в динамическом изменении и зависит от актуальности информации, средств распространения, передачи и хранения данных.

В туризме используются различные системы информационных технологий, которые работают на базе: компьютерных систем резервирования, автоматизированных систем управления туристскими предприятиями, электронных информационных систем авиалиний, систем электронных расчётов, телефонных сетей и систем передачи данных, систем проведения телеконференций, видеосистем, отдельных компьютеров и т. д. При этом важной особенностью является то, что система технологий разрабатывается не отдельно для турагентов, гостиниц или авиакомпаний, а для всех одновременно. Более того, использование каждым сегментом туризма системы информационных технологий имеет значение для всех остальных частей [1].

## 2. Постановка проблемы

Для того, чтобы в настоящее время быть конкурентоспособным необходимо обязательное использование информационных систем, так как они повышают эффективность и скорость работы. Предприятия туриндустрии постоянно используют личную информацию клиентов (паспортные данные, номера телефонов, номера счетов в банке), и поэтому необходимо принимать меры по предотвращению взлома баз данных клиентов и других информационных баз. Возникает понятие «информационного риска». Целью данной статьи является выяснение информационных рисков в работе туристских предприятий, связанных с применением современных информационных технологий и разработка предложений по их устранению либо минимизации.

Для достижения указанной цели были поставлены такие задачи:

– рассмотрение современного состояния автоматизации работы туристских предприятий;

– выявление новых тенденций в этой сфере и выяснение информационных рисков с ними связанных;

– разработка рекомендаций для устранения или минимизации информационных рисков на туристских предприятиях, обусловленных внедрением современных информационных систем и технологий в работу этих предприятий.

## 3. Литературный обзор

В Украине любая деятельность так или иначе осуществляется согласно законодательству – Законы Украины: «Про информацию», «Про защиту информации в информационно-телекоммуникационных системах», «Про защиту персональных данных», Постановление Кабинета Министров Украины «Об утверждении Правил обеспечения защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах»; нормативные документы системы технической защиты информации: «Типовое положение о службе защиты информации в автоматизированной системе», «Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа», «Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа», «Техническая защита информации. Компьютерные системы. Порядок создания, внедрения, сопровождения и модернизации средств технической защиты информации от несанкционированного доступа», ДСТУ 3396.1-96 «Защита информации. Техническая защита информации. Порядок проведения работ», Отраслевой стандарт

Украины ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 «Информационные технологии, методы защиты, система управления информационной безопасностью». На международном уровне приняты стандарты об информационном риске – ISO/IEC 17799 (англ. Information technology – Security techniques – Code of practice for information security management, рус. – Информационные технологии – Технологии-безопасности – Практические правила менеджмента информационной безопасности), BS7799-3:2006 (англ. – Information security management systems – Guidelines for information security risk management, рус. – Системы менеджмента информационной безопасности – Руководство по управлению рисками информационной безопасности) , ISO/IEC TR 13335-3:1998 (англ. – Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security, рус. – Информационные технологии – Руководящие принципы для управления ИТ-безопасностью – Часть 3: Методы для управления ИТ-безопасностью), NIST SP 800-30 (англ. – Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology, рус. – Руководство по управлению рисками для информационных систем. Рекомендации Национального института стандартов и технологий) [2, 3].

Комплексным изучением информационных рисков посвящены работы таких отечественных учёных как Варфоломеев А. А., Астахов А. М., Петренко С. А., Вишняков Я. Д. Большая часть исследователей посвящают свои работы методам оценки информационных рисков, которые позволят максимально уменьшить риск проникновения посторонних лиц к информации организации [4–6]. В работах этих и других авторов рассматриваются общие вопросы обеспечения информационной безопасности без учёта специфики работы конкретных предприятий. Поэтому в данной статье раскрыты вопросы связанные с информационными рисками на туристских предприятиях.

**4. Использование автоматизированных систем на турпредприятиях и образования понятия «информационного риска»**

Автоматизация позволила упростить и удешевить связи между различными объектами, одновременно повысив качество циркулирующей информации. Интернет-системы создают доступ к своим информационным базам в любое время, что повышает оперативность работы, скорость и эффективность обработки информации.

На рынке программных продуктов представлено несколько компьютерных систем и технологий, позволяющих автоматизировать внутреннюю деятельность туристской фирмы. В основном эти системы обеспечивают ведение справочных баз данных по клиентам, партнерам, гостиниц, транспорта, посольств, а также разработку и ведение туров, учет платежей, прием заказов и работу с клиентами, формирование выходных документов, учет работы персонала туристского предприятия и тому подобное. Практически все программные комплексы обеспечивают формирование бухгалтерской отчетности и часто экспорт-импорт данных в специализированные бухгалтерские программы.

Среди информационных систем, используемых в сфере туризма во всем мире широкое распространение получили глобальные компьютерные системы бронирования, такие как Amadeus, Galileo, Sabre i Worldspan и другие. Кроме того крупные туристские предприятия широко используют инструментарий построения сайтов и локальных систем бронирования туров и различных услуг в сфере туризма.

Одновременно с автоматизацией работы туристских фирм ведутся аналогичные работы по автоматизации деятельности гостиниц, ресторанов и других предприятий туристского бизнеса. Применение информационных систем в этой сфере приводит к существенным изменениям в менеджменте, а также повышает качество обслуживания.

В данной статье более подробно рассмотрим новые тенденции, появившиеся в использовании информационных технологий в деятельности туристских предприятий, появившиеся в последнее время.

В настоящее время в туризме широко стали использоваться банковские карты для оплаты по безналичному перечислению, как между клиентом и турагентом, так и между турагентом и туроператором.

В современном мире клиентам для оплаты отдыха необязательно идти в банк и снимать необходимую сумму и потом возвращаться в турагенство. Можно, с помощью, так называемых, «личных кабинетов» или приложений на мобильных устройствах, сразу расплатиться за услугу, что значительно экономит время, ускоряет процесс оформления услуги и делает более комфортной услугу приобретения тура [7].

Одной из новых тенденций в работе туристских предприятий становится использование виртуальных технологий. Организации, которые находятся в виртуальном пространстве, имеют небольшие основные средства и зачастую рассредоточены. Это даёт возможность сотрудникам работать в отдалённом доступе, не находясь постоянно в офисе и возможность доступа к информационной базе в любое время [1].

Однако, несмотря на явные преимущества работы с автоматизированными информационными системами, существует риск взлома информационной базы турагентов и использование частных данных клиентов в мошеннических целях. Возникает, таким образом, риск повреждения и утери информации.

Существует общее понятие информационного риска – это риск возникновения убытков или ущерба в результате применения информационных технологий [2].

Риски информационной безопасности, которые связаны с современной «интернетизацией» и интеграцией информационных систем большая часть предприятий не считает важным, так как есть заблуждение о том, что ущерб от киберугроз не может быть масштабным. В результате может произойти сбой системы или приостановление её на некоторое время, что приведёт к невозможности осуществления предоставления услуг, создаст предпосылки к вы-

полнению мошеннических операций в системах электронных счетов и будет способствовать угрозе утечки конфиденциальной информации [3].

Элементами информационных рисков являются информационные активы, к которым относятся: информация, напечатанная или записанная на бумаге, пересылаемая по почте или демонстрируемая в видеозаписях, передаваемая устно, информация хранимая на серверах, веб-сайтах, мобильных устройствах, магнитных и оптических носителях, информация обработанная в корпоративных информационных системах и передаваемая по каналам связи, а также программное обеспечение: операционные системы, приложения, утилиты, программная документация [3].

Для турпредприятий важно постоянно следить за своей документацией и записями. На таких предприятиях следует обращать внимание на следующие виды работ с документами: контроль и защита документов и записей; утверждение, анализ и корректировка документов; идентификация изменений статуса текущих версий; обеспечение доступности, передачи, хранения и уничтожения документов; контроль над распространением документов [3].

В соответствии с международными стандартами разработано программное обеспечение по выявлению информационных рисков. Существует программное обеспечение базового и полного анализа рисков. К инструментарию базового уровня относятся:

– COBRA **(**производитель – C&A Systems Security Ltd., позволяет формализовать и ускорить процесс проверки на соответствие режима информационной безопасности требованиям Британского стандарта BS 7799 (ISO 17799) и провести простейший анализ рисков);

– RA Software Tool (базируется на британском стандарте BS 7799, части 1 и 2; на методических материалах Британского института стандартов: (BSI) PD 3002, PD 3003, PD 3005, а также на стандарте ISO 13335,части 3 и 4) [2].

К инструментарию базового уровни относят метод CRAMM (самый распространенный метод анализа рисков и управления ими. CRAMM соответствует стандарту BS 7799 (ISO 17799) [2] и OCTAVE (Operationally Critical Thereat, Asset and Vulnerability Evaluation – оценка критичных угроз, активов и уязвимостей — имеет ряд модификаций, рассчитанных на организации различных размеров и областей деятельности, разработан по международным стандартам) [3].

Большая часть туристских предприятий не считает нужным предпринимать конкретные меры безопасности и используют лишь базовую защиту, что не позволяет защитить от взлома информационных баз. Не каждое предприятие может позволить выделить отдел или сотрудника, который будет постоянно отвечать за безопасность, потому что для малых предприятий это коммерчески не выгодно, но 1–2 раза в год необходимо пользоваться услугами аутсорсинговых компаний, занимающихся контролем информационной безопасности. Так как, пренебрежение защитой информации может привести к потере клиентской базы, материальных средств и к закрытию компании.

**5. Апробация результатов исследования**

Основой методологии анализа рисков на сегодняшний день является американский стандарт NIST (англ. – The National Institute of Standards and Technology, рус. – Национальный институт стандартов и технологий), где приводится общая методология анализа рисков для организаций. В настоящее время в работе туристских предприятий целесообразно использовать коммерческие программные продукты, которые оценивают риски для организаций и выдают некоторые рекомендации по усовершенствованию существующих систем.

Анализ возникновения информационных рисков на туристских предприятиях и управление ими может быть реализован следующими методами:

– качественные, количественные, смешанные;

– статистические (мониторинговые) и экспертные;

– экономико-математическое и ситуационное (имитационное) моделирование;

– индикаторные, методы интервального анализа, диверсификация, хеджирование;

– бифуркационные (критические, катастрофические), когнитивные карты, профили рисков;

– нейросистемные [5];

– модель обобщенного стоимостного результата Миоры (англ. Miora Generalized Cost Consequence Model) [4];

– методология оценки рисков MEHARI (Méthode Harmonisée d'Analyse de Risques – Harmonised Risk Analysis Method), разработанная французской организацией CLUSIF (CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS) [6].

Главная цель использования перечисленных методов оценки и управления рисками заключается в устранении или минимизации информационных рисков в работе туристских предприятий и повышении результативности и эффективности их работы.

**6. Выводы**

Для того чтобы защитить турпредприятие от информационных рисков необходимо создать систему управления информационной базой (СУИБ). Чтобы внедрить СУИБ, необходимо сформировать постоянную экспертную группу, в которой будут входить: специалисты по информационной безопасности, представители ИТ- и бизнес-подразделений. Группа может состоять от 3 до 7 человек. Данную группу необходимо создавать для туроператоров и сетей турагенств, так как в их базах данных большое количество конфиденциальной информации о клиентах, которая должна быть доступной сотрудникам только данных предприятий. Малые предприятия могут обращаться 1 раз в год в аутсорсинговую компанию, так как не имеют возможности и постоянной потребности в данной экспертной группе.

Для оптимального управления рисками руководителям туристских предприятий необходимо постоянно заниматься вопросами планирования, реализации, проверки и регулирования действий, связанных с минимизацией информационных рисков и повышением информационной безопасности работы предприя-

тия, что приведёт к постоянному мониторингу состояния предприятия на предмет посторонних угроз.

**Литература**

1. Сельскова, О. А. Автоматизация и виртуализация как характеристики устойчивости туристических корпораций нового поколения [Текст] / О. А. Сельскова // Технико-технологические проблемы сервиса. – 2013. – № 3. – С. 93–95.
2. Варфоломеев, А. А. Управление информационными рисками [Текст]: учеб. пос. / А. А. Варфоломеев. – М.: РУДН, 2008. – 158 с.
3. Астахов, А. М. Искусство управления информационными рисками [Текст] / А. М. Астахов. – М.: ДМК Пресс, 2010. – 312 с.
4. Понамарёв, А. А. Оценка и управление рисками информационных систем [Текст] / А. А. Понамарёв // Вестник Удмуртского университета. – 2007. – № 6. – С. 151–162.
5. Казиева, Б. В. Методология оценки информационных рисков управления организацией [Текст] / Б. В. Казиева, К. В. Казиев // Современные технологии управления. – 2014. – № 12. – Режим доступа: http://sovman.ru/all-numbers/archive-2014/december2014/item/318-the-methodology-of-an-assessment-of-information-risks-in-management-of-the-organization.html
6. Янчин, М. К. Управление информационными рисками на основе методологии MEHARI [Текст] / М. К. Янчин // – 2011. – С. 152–155. – Режим доступа: http://www.pvti.ru/data/file/bit/bit_4_2011_29.pdf
7. Арапова, Л. А. Современные технологии в туризме [Текст] / Л. А. Арапова // Технико-технологические проблемы сервиса. – 2010. – № 2. – С. 94–97.

**References**

1. Sel`skova, O. A. (2013). Avtomatizatsia I virtualizatsia kak kharakteristiki ustoychivosti turisticheskih korporatsiy novogo pokolenia [Automation and virtualization as the characteristics of sustainability of tourism corporations of a new generation]. Technical-technological problems of service, 3, 93–95.
2. Varfolomeev, A. A. (2008). Upravlenie informatsyonnymi riskami [Information Risk Management]. Moscow: RUDN, 158.
3. Astahov, A. M. (2010). Iskusstvo upravlenia informatsyonnymi riskami [Art Information Risk Management]. Moscow: DMK PRESS, 312.
4. Ponamarev, A. A. (2007). Otsenka i upravlenie piskami informatsyonnyh system [Risk assessment and management of information systems]. Bulletin of Udmurt University, 6, 151–162.
5. Kazieva, B. V., Kaziev, K. V. (2014). Metodologia otsenki informatsyonnyh riskov upravlenia organizatsyei [Information Risk Assessment Methodology Management Organization]. Modern management technologies, 12. Available at: http://sovman.ru/all-numbers/archive-2014/december2014/item/318-the-methodology-of-an-assessment-of-information-risks-in-management-of-the-organization.html
6. Ianchin, M. K. (2011). Upravlenie informatsyonnymi riskami na osnove metodologii MEHARI [Information Risk Management, based on the methodology MEHARI]. 152–155. Available at: http://www.pvti.ru/data/file/bit/bit_4_2011_29.pdf
7. Arapova, L. A. (2010). Sovremennye tehnologii v turizme [Modern technologies in tourism]. Technical-technological problems of service, 2, 94–97.

*Рекомендовано до публікації д-р екон. наук Писаревським І. М.*
*Дата надходження рукопису 23.11.2015*

**Сидора Алина Сергеевна**, кафедра туризма и гостиничного хозяйства, Харьковский национальный университет городского хозяйства им. А. Н. Бекетова, ул. Революции, 12, г. Харьков, Украина, 61002
E-mail: alina.sidora@gmail.com

**Погасий Сергей Александрович,** кандидат технических наук, доцент, кафедра туризма и гостиничного хозяйства, Харьковский национальный университет городского хозяйства им. А. Н. Бекетова, ул. Революции, 12, г. Харьков, Украина, 61002
E-mail: POGASIY07@mail.ru