ОСОБЕННОСТИ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСТИНИЧНЫХ И ТУРИСТИЧЕСКИХ КОМПЛЕКСАХ

Журавлева В.В.[1], Поляков В.В.[1], Фролов А.Е.[1], Родионов И.М.[2]
[1]Алтайский государственный университет, г. Барнаул
[2]Восточно-Казахстанский государственный университет им. С. Аманжолова, г. Усть-Каменогорск, Республика Казахстан
email: torinka8@gmail.com

Аннотация. Рассмотрены особенности информационной безопасности гостиничных комплексах, заключающиеся в большом объеме непрерывно поступающих персональных данных, требующих специального режима хранения и обработки. Сформулированы рекомендации по организации защиты информации в организациях туристической индустрии, включающие в себя комплексные меры технического, методического и организационного характера.

Ключевые слова: защита персональных данных, туристические информационные системы, комплексная защита информации.

В настоящее время в Российской Федерации происходит быстрое развитие индустрии туризма, занимающей все более значительное место в экономике. Эта деятельность регламентируется Федеральным законом от 24 ноября 1996 г. №132-ФЗ «Об основах туристской деятельности в Российской Федерации». Согласно данному закону, в туристическую индустрию входит «совокупность гостиниц и иных средств размещения, средств транспорта, объектов санаторно-курортного лечения и отдыха», а также деятельность «организаций, осуществляющих туроператорскую и турагентскую деятельность, операторов туристских информационных систем». Таким образом, в сферу туристических услуг включены гостиницы, дома отдыха и т.д. Использование этих услуг клиентами неотрывно связано со специализированными туристическими информационными системами, специализирующимися на размещении клиентов и удовлетворении их разнообразных запросов [1, 2]. Это означает, что одной из актуальных задач современного гостиничного бизнеса является обеспечение информационной безопасности туристических комплексов, прежде всего - защита персональных данных клиентов.

Большой объем персональных данных формируется и обрабатывается в виде компьютерной информации в информационных системах гостиничных комплексов. Эти комплексы по роду своей деятельности проводят обработку сведений о клиентах, содержащих их персональные данные, то есть являются операторами обработки персональных данных [3, 4]. Это регламентируется Федеральным законом №152-ФЗ «О персональных данных» от 27 июля 2006 года [3], а также приказами регуляторов (приказ ФСТЭК от 18 февраля 2013 г. №21) [4], отвечающих за обеспечение защиты персональных данных от несанкционированного доступа.

Процедура обработки персональных данных обычно начинается с момента получения информации о клиентах при online-бронировании или, при его отсутствии, при непосредственном заполнении анкеты при заселении в гостиницу. В обоих случаях используются компьютерные системы, подключенные к локальной сети организации и глобальной информационной сети «Интернет». Это означает, что существует реальная угроза неправомерного доступа (прежде всего удаленного по сети «Интернет») к компьютерной информации, содержащей персональные данные клиентов. В связи с большим объемом таких данных и спецификой их поступления и обработки, обусловленной поступлением этих сведений прежде всего по информационно-коммуникационным каналам связи, актуальной задачей является

разработка рекомендаций по обеспечению информационной безопасности в туристических организациях и гостиничных комплексах.

Решение данной задачи требует применения комплексного подхода к защите информации, включающего в себя меры технического, организационного, методического характера [5]. Они заключаются прежде всего в проведении различных мероприятий по технической защите информации.

Для осуществления процесса обслуживания туристов в гостинице должен быть предусмотрен минимальный набор следующих служб, обеспечивающих предоставление основных гостиничных услуг:

- служба управления номерным фондом;
- административная служба;
- служба общественного питания;
- коммерческая служба;
- технические службы;
- вспомогательные и дополнительные службы.

Все эти службы подключены к локальной корпоративной сети гостиницы и тем самым составляют риски для несанкционированного доступа к конфиденциальной информации.

Гостиничный комплекс является «оператором обработки персональных данных» в соответствии с п. 2, 3 ст. 3 152-ФЗ. В дополнение к этому Федеральному закону должны учитываться нормативные документы приведенные в таблице 1.

Все процедуры проверок определяет Административный регламент проведения проверок Роскомнадзором (утверждённый приказом № 630 от 01.12.2009 г.). Любой гостиничный комплекс до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) о своем намерении осуществлять обработку персональных данных. Порядок направления уведомления определен приказом Россвязьохранкультуры № 3 от 11.01.08 г. «Об утверждении формы уведомления об обработке (о намерении осуществлять обработку) персональных данных». Любой гостиничный комплекс до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) о своем намерении осуществлять обработку персональных данных. Порядок направления уведомления определен приказом Россвязьохранкультуры № 3 от 11.01.08 г. «Об утверждении формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».

Наибольшую опасность несанкционированного доступа представляет заполнение данных при online-бронировании на сайте гостиницы. В связи с этим необходимо учитывать, что доступ к информационным сетям общего пользования, в том числе к сети Интернет, допускается только с использованием специально предназначенных для этого средств защиты информации.

Каждой гостиничной организации присваивается определенный класс информационной системы персональных данных (ИСПДн) в зависимости от числа субъектов, например, 1 класс, если обрабатываются персональные данные 1 категории и количество субъектов более определенного числа. Основная масса хранимых персональных данных представлена в виде собой электронных документов, хранимых и обрабатываемых в компьютерных системах.

Таблица 1. Список документов, дополняющих и разъясняющих требования основного закона о персональных данных.

№ п/п	Наименования документа № и дата выхода
1.	Постановление Правительства № 1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (Определяет типы актуальных угроз и необходимые уровни защищенности ПДн, которые должен обеспечить оператор при обработке)
2.	Постановление Правительства № 687 от 15.09.2008 г. «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (Определяет требования к обработке ПДн в «бумажном» виде)
3.	Постановление Правительства № 211 от 21 марта 2012 г. «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятых, в соответствии с ним, нормативными актами, операторами, являющимися государственными органами» (в ред. Постановлений Правительства РФ № 607 от 20.07.2013, № 911 от 06.09.2014)
4.	Приказ ФСТЭК России № 17 от 11.02.2013 г. (ред. от 15.02.2017 г.) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 за № 28608)
5.	Приказ ФСТЭК России № 21 от 18.02.2013 г. (ред. от 23.03.2017 г.) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 г. за № 28375). Приказ определяет методы и средства обеспечения соответствующего уровня защищенности.

В большинстве случаев для обработки персональных данных о клиентах используются офисные программы и специальные программы типа «1С». Система «1С» предназначена для поддержки бизнес-процессов организации и позволяет вести учет всей хозяйственной деятельности, формировать различные отчеты и т.д. Режим обработки персональных данных предусматривает следующие действия: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных. Обработка персональных данных в системе «1С» обычно ведется в многопользовательском режиме, что требует разграничений прав доступа и парольной защиты на корпоративных компьютерах.

Актуальными угрозами для электронной информации, содержащей персональные данные клиентов и сотрудников гостиничных комплексов, являются несанкционированные уничтожение, копирование, модификация и блокирование информации за счет несанкционированного доступа. Такой доступ может быть совершен как удаленным образом по информационной сети с применением вредоносного программного обеспечения, так и за счет ошибочных или злонамеренных действий сотрудников организации, имеющих допуск к корпоративной сети. Для минимизации рисков рекомендуется составление матрица доступа групп пользователей, которые имеют доступ к компьютерным системам в

гостинице, содержащей разрешенные действия. Пример такой матрицы доступа для различных групп пользователей приведен в таблице 2.

Таблица 2. Матрица доступа групп пользователей.

Типовая роль	Уровень доступа к персональным данным	Разрешенные действия с персональными данными
Управляющий персонал	Обладает полной информацией о персональных данных работников и клиентов. Имеет доступ к личным делам работников и клиентов	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование - уничтожение - распространение - блокирование - обезличивание
Ресепшн	Имеет доступ к личным данным клиентов и информации, содержащей персональные данные клиентов	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование - уничтожение - распространение - блокирование - обезличивание
ИТ - персонал	Имеет доступ к информации, содержащей персональные данные клиентов.	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование - уничтожение - распространение - блокирование - обезличивание
Ответственный за обеспечение информационной безопасности	Обладает правами Администратора ИСПДн. Обладает полной информацией об ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Оператор ИСПДн	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем персональным данным	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование - уничтожение - распространение - блокирование - обезличивание

Очевидно, что наибольшим уровнем доступа обладают следующие группы: управляющий персонал, ответственный за обеспечение информационной безопасности, и оператор ИСПДн.

Рекомендуется проводить оценку рисков несанкционированного доступа к персональным данным. Это может быть проведено, например, с помощью специализированного программного обеспечения MSAT v 4.0 по двум основным факторам: профилю риска для бизнеса (BRP) и индекса эшелонированной защиты (DiDI). Критерии анализа при этом идут по двум основным направлениям:

- - бизнес-модель организации;
- - применение мер защиты информации.

Итоговая оценка рисков распределяется по следующим направлениям: инфраструктура; приложения; операции; персонал.

Для уменьшения рисков возникновения угроз каждой гостиничной организации необходимо разработать и принять комплекс технических и организационных мер защиты, то есть обеспечить комплексную защиту информации. К техническим мерам защиты могут быть отнесены следующие:

- установка охранной сигнализации;
- использование сейфов;
- установка решеток на окнах, кодовых замков и т.п.;
- установка средств видеонаблюдения;
- обеспечение бесперебойного электропитания;
- установка межсетевых экранов;
- постоянное обновление программно-аппаратных средств антивирусной защиты;
- резервное хранение информации.

К организационным мерам защиты относятся, в частности:

- разработка и внедрение инструкций пользователей и администраторов безопасности;
- учет всех носителей электронной и иной информации;
- подписание договоров о неразглашении;
- составление инструкций по технологическому порядку обработки данных;
- составление регламента информационной безопасности;
- составление актов об установке средств защиты информации;
- установление пропускного режима и охраны

и другие меры.

Особое значение в связи с актуальностью реализации угроз по удаленному доступу к компьютерной имеют меры по антивирусной защите, прежде всего обеспечение защиты на уровне фильтрации входящего трафика. Для этого рекомендуется использование специализированного сервера, выступающего в роли почтового сервера и сервера фильтрации трафика (например, использовать SMTP сервер, использующий основной пакет программ платформы Windows Server 2008 R2). Одновременно необходимо запретить передачу входящего трафика по максимально возможному количеству портов. Антивирусная защита проводится с помощью установки специализированного программного обеспечения, например, «Kaspersky remove tool» или «Dr.Web Curent».

Для организации хранения и обмена информацией используется рекомендуется использовать файловый сервер, например, ftp-сервер, также входящий в основной пакет программ платформы Windows Server 2008 R2. При этом все пользователи разбиваются на категории с различными правами доступа к этому серверу в соответствии с регламентом информационной безопасности. Такие меры позволят снизить возможность несанкционированного доступа сотрудников и утечку

инсайдерской информации. Кроме того, чтобы предотвратить заражение корпоративной сети вредоносными программами со съемных носителей информации рекомендуется запретить сотрудникам их использование.

Для обеспечения криптографических мер защиты информации гостиницам рекомендуется использовать средства типа ViPNet CSP 4.2. Так, средство защиты ViPNet CSP 4.2 обеспечивает класс защищенности КС1, что обычно удовлетворяет требованиям защиты информационной системы организации, и позволяет осуществлять следующие функции:

- создание ключей электронной подписи, формирование и проверка электронной подписи согласно ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012;
- хэширование данных по ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012;
- шифрование и имитозащита данных по ГОСТ 28147-89;
- поддержание работы с внешними устройствами (токенами) для создания и хранения ключей и сертификатов, возможность интеграции новых устройств;
- возможность экспорта и импорта ключей в формате #PKCS12;
- поддержание вызова криптографических функций CSP сторонними приложениями через API PKCS#11, Microsoft CryptoAPI и Microsoft CNG.

Для защиты информационных ресурсов организации также имеет смысл применять программно-аппаратные средства типа Secret Net 7 на базе ОС Windows или Secret Net LSP на базе ОС Linux. Для обеспечения защиты наиболее важной информации от несанкционированного доступа рекомендуется установить в организации средство защиты информации от несанкционированного доступа типа Dallas Lock. Это средство позволит дополнительно решать следующие задачи:

- разграничение прав пользователей при работе на компьютерах и запрет лицам, не имеющим учетной записи на данном компьютере, доступа к его информационным ресурсам; такое разграничение касается прав доступа к сети, к объектам файловой системы, к беспроводным устройствам и накопителям информации;
- управление средствами аутентификации, в том числе хранение, выдачу, инициализацию, блокирование этих средств в случае утраты и (или) компрометации;
- разделение полномочий пользователей, администраторов и иных лиц, обеспечивающих функционирование информационной сети организации.

После завершения установки и настройки антивирусного программного обеспечения администрации гостиничного комплекса необходимо разработать внутренние организационные документы для персонала. Список этих документов включает в себя:

- инструкции по информационной безопасности, включающие себя правила по использованию АРМ пользователя (в том числе запрет использования рабочего места посторонними лицами и другими сотрудниками организации, кроме ответственного персонала);
- правила по контролю персонала на рабочем месте;
- политику безопасности;
- правила по обслуживанию, модернизации, конфигурации и отключению установленных средств защит информации.

Для минимизации рисков нарушения информационной безопасности организации рекомендуется разрабатывается политика информационной безопасности, которая представляет собой перечень правил для различных областей деятельности организации. Политика безопасности предполагает, в частности, четкое распределение функциональных обязанностей между администраторами сети, специалистами по информационной безопасности, руководителем информационного отдела и т.д., она должна предусматривать непрерывность

контроля за системами защиты информации, персональную ответственность специалистов, оперативность в принятии управленческих решений в зависимости от конкретной складывающейся ситуации, нацеленность руководства и персонала гостиничного комплекса на обеспечение информационной безопасности.

Применение предложенных комплексных мер позволит обеспечить более надежную защиту компьютерной информации в туристических и гостиничных комплексах.

Библиографический список

1. Кобяк М.В. Стандартизация и контроль качества гостиничных услуг: практическое пособие. - СПб.: «Интермедия», 2014. – 284 с.
2. ГОСТ Р 51185-98 «Туристские услуги. Средства размещения. Общие требования».
3. О персональных данных : Федеральный закон от 27 июля 2006 г. № 152 // Российская газета. – 2006. – 29 июля.
4. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК от 18 февраля 2013 года № 21 - ФЗ // Российская газета. - 2013. -22 мая.
5. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости // М.: Стандартинформ, 2009. – 226 с.
6. Журавлева В.В., Поляков В.В. Обеспечение защиты персональных данных в гостиничных комплексах // Сб. тезисов VII Всероссийской междисциплинарной молодежной научной конференции «Проблемы правовой и технической защиты информации». 14 июня 2020 г., Барнаул. Изд-во Алтайского ун-та, 2020. - С. 20-21.
7. Минакова Н.Н., Поляков В.В., Плетнев П.В. Методы и средства защиты информации в коммерческой организации: монография. Барнаул: Изд-во «Новый формат», 2016. – 158 с.
8. Поляков В.В., Трушин В.А., Рева И.А. и др. Региональные аспекты технической и правовой защиты информации // Монография. - Барнаул: Изд-во Алт. ун-та, 2013. – 194 с.

FEATURES ENSURING INFORMATION SECURITY IN HOTEL AND TOURIST COMPLEXES

Zhuravleva V.V.[1], Polyakov V.V.[1], Frolov A.E.[1], I.M. Rodionov[2]
[1]Altai State University, Barnaul
[2]East Kazakhstan State University named after S. Amanzholova, Ust-Kamenogorsk, Republic of Kazakhstan
email: torinka8@gmail.com

Abstract. The features of information security of hotel complexes, which consist in a large volume of continuously incoming personal data, requiring a special mode of storage and processing, are considered. Recommendations are formulated for organizing information security in organizations of the tourism industry, including complex measures of a technical, methodological and organizational nature.

Keywords: personal data protection, tourist information systems, comprehensive information protection.