Игнатенко Дарья Павловна
Студентка Института инженерных и цифровых технологий НИУ «БелГУ»
г. Белгород
Ignatenko Darya Pavlovna
Student, Institute of Engineering and Digital Technologies, Belgorod State University
Belgorod

ВОПРОСЫ ВЕДЕНИЯ ГОСТИНИЧНОГО БИЗНЕСА С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ISSUES OF CONDUCTING HOTEL BUSINESS FROM THE POINT OF VIEW OF INFORMATION SECURITY

Аннотация: Статья посвящена актуальным проблемам обеспечения информационной безопасности в индустрии гостеприимства. В условиях цифровизации гостиничного бизнеса и повсеместного внедрения систем бронирования, бесконтактных технологий и интернета вещей (IoT) защита персональных данных гостей и непрерывность оказания услуг становятся критическими факторами конкурентоспособности.

Ключевые слова: безопасность, сеть, гостиничный бизнес.

Abstract: This article examines current issues related to information security in the hospitality industry. With the digitalization of the hotel industry and the widespread adoption of reservation systems, contactless technologies, and the Internet of Things (IoT), protecting guest personal data and ensuring service continuity are becoming critical factors for competitiveness.

Keywords: security, network, hotel industry.

Внедрение телекоммуникационной сети планируется в гостиничном комплексе. Главным принципом ее построения является обеспечение стабильности, отказоустойчивости и сохранности информации, поскольку от ее бесперебойной работы зависят критически важные бизнес-процессы: бронирование и размещение гостей, функционирование системы питания, безопасность, развлекательные услуги и финансовые операции. Проектирование телекоммуникационной сети гостиничного комплекса должно

исходить из триединого требования: обеспечения высокой доступности сервисов для гостей, интеграции со всеми внутренними бизнес-системами и реализации встроенных механизмов информационной безопасности.

Современные постояльцы рассчитывают на качественную связь, быстрый интернет и бесперебойную работу сервисов, телевидения и других цифровых услуг. Администрация должна интегрировать сетевые инфраструктуры с системами бухгалтерского учета, контроля доступа, видеонаблюдения и системами управления недвижимостью.

Информационная инфраструктура гостиничного комплекса – это сложная распределённая система, которая подвержена самым разным угрозам. Из-за этих угроз могут случаться сбои в важных бизнес-процессах, а также нарушаться конфиденциальность, целостность и доступность данных. Чтобы выстроить эффективную защиту, нужно сначала проанализировать и классифицировать эти угрозы.

Внешние угрозы, такие как DDoS-атаки, эксплуатация уязвимостей и целевое вредоносное ПО, представляют собой постоянный вызов для безопасности сетевой инфраструктуры, требуя непрерывного мониторинга и обновления средств защиты периметра. Внешние угрозы исходят из интернета и направлены на преодоление периметральной защиты. К ним относятся: сканирование портов и поиск уязвимостей в настройках сетевого оборудования, веб-серверов и систем управления; попытки взлома через известные «дыры» в операционных системах и прикладном ПО; DoS и DDoS-атаки на интернет-каналы и публичные сервисы отеля (сайт бронирования, гостевой портал). Такие атаки способны привести к финансовым потерям и репутационному ущербу. Отдельную категорию составляют фишинг и целевое вредоносное ПО, рассылаемые сотрудникам по электронной почте для кражи учётных данных или получения контроля над внутренними системами.

Учитывая тип хранимой информации, угрозы нарушения конфиденциальности и утечки данных являются чрезвычайно важными. Они могут быть реализованы как через сетевые каналы, так и физически, путем

кражи или несанкционированного копирования данных с серверов, рабочих станций или резервных носителей.

Обеспечение высокой доступности критичных сетевых компонентов, таких как маршрутизаторы, коммутаторы ядра и системы хранения, является необходимым условием для непрерывности бизнес-процессов и предотвращения финансовых потерь, связанных с простоями. Информационная безопасность в широком смысле как обеспечение доступности тоже страдает от сбоев в работе оборудования и программ. Сбои в системах бронирования, расчёта и управления, например выход из строя маршрутизатора, центрального коммутатора, системы хранения данных, отключение электричества или ошибки в программах, могут привести к прямым финансовым убыткам и потере доверия со стороны клиентов.

Выбор средств защиты информации для телекоммуникационной сети гостиничного комплекса осуществляется на основе комплексного анализа ранее определённых требований и идентифицированных угроз информационной безопасности. Обоснование выбора строится на принципах адекватности, экономической целесообразности, совместимости с существующей инфраструктурой и соответствия требованиям регуляторов.

Для защиты сети используется управляемый коммутатор с поддержкой списков доступа (ACL) и сегментации трафика. Он позволяет логически разделить трафик гостей, сотрудников и служебных систем на изолированные VLAN, а также фильтровать потоки данных между ними, предотвращая несанкционированный доступ.

Беспроводная сеть защищается контроллером, который обеспечивает строгую аутентификацию для персонала и отдельный гостевой доступ через портал (Captive Portal) — например, по номеру комнаты или одноразовому коду. Благодаря этому гость не может проникнуть во внутренние системы отеля.

При передаче данных во внешние сети обязательно используется шифрование с сертификатом ФСБ России — например, VPN-шлюзы и защищённый протокол TLS.

На всех серверах и компьютерах функционирует централизованная антивирусная защита. Доступом сотрудников управляет российская служба каталогов (ALD Pro), интегрированная с доменной инфраструктурой организации. Аутентификация выполняется по протоколам Kerberos и LDAP, что позволяет строго проверять личность при входе и автоматически назначать права доступа на основе ролевой модели.

Для выполнения требований регуляторов внедряется система сбора событий безопасности (SIEM), которая аккумулирует журналы со всего сетевого оборудования и средств защиты. Такой комплекс мер формирует сбалансированную систему защиты, соответствующую законодательству РФ.

При выборе конкретных моделей и производителей для каждого компонента следует учитывать не только их функциональность, но и надёжность, наличие сертификатов ФСТЭК России и ФСБ России, а также возможность технической поддержки на территории РФ.

Конечным этапом процесса выбора и внедрения средств защиты является разработка регламентов их эксплуатации и интеграция в общую систему управления информационной безопасностью гостиничного комплекса. Для каждого внедряемого решения должны быть созданы инструкции по настройке, ежедневному администрированию, обновлению правил, а также процедуры аварийного восстановления.

При выборе средств защиты нужно считать не только то, сколько стоит оборудование и лицензии сразу, но и все расходы. Сюда входят подписка на обновления, обучение сотрудников. Предпочтение следует отдавать решениям, имеющим лицензии и включённым в реестр сертифицированного программного обеспечения ФСТЭК России и ФСБ России, с закрытыми лицензируемыми программными интерфейсами. Это обеспечит возможность

дальнейшего расширения функционала, подключения систем аналитики и автоматизации реагирования на инциденты информационной безопасности.

В итоге выбор средств защиты для сети гостиницы – это непростая инженерная задача. Нужно найти баланс между требованиями регуляторов, реальными угрозами, выделенным бюджетом и тем, чтобы внутренние сервисы работали без сбоев. Предложенный здесь многоуровневый подход с защитой периметра, разделением сети на части, шифрованием, контролем доступа, системой обнаружения атак и централизованным сбором логов даёт гибкую и надёжную архитектуру безопасности. Эта архитектура послужит основой для детального проектирования и практической реализации защищённой сетевой инфраструктуры.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. **Баланов А. Н.** Комплексная информационная безопасность : учебное пособие для СПО / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург : Лань, 2025. – 284 с. – ISBN 978-5-507-52953-7. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/463001.

2. **Внуков, А. А.** Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 161 с. – (Профессиональное образование). – ISBN 978-5-534-13948-8. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/542340.

3. Гостиничный комплекс «Белгород»: сайт / https://hotelbelgorod.ru/.– Белгород, 2019 – 2026. – URL: https://hotelbelgorod.ru/ (дата обращения: 01.12.2025). – Режим доступа: для авториз. пользователей. – Текст: электронный