Д. О. Чепак, В. А. Ракитин
Тюменский государственный университет, г. Тюмень
УДК 004.94

РАЗРАБОТКА КОМПЛЕКСА МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ ОРГАНИЗАЦИИ РЕСТОРАННОГО БИЗНЕСА

Аннотация. В работе была изучена нормативно-правовая база по защите информации, а также определены особенности обработки и передачи информации ресторанного бизнеса. Далее проведен анализ структуры корпоративной сети для определения рисков информационной безопасности. Результатом данной работы стали выводы по проделанным задачам, которые будут использованы для построения модели нарушителя/угроз и проектирования системы защиты информации.

Ключевые слова: информационная безопасность, ресторанный бизнес, лицензирование, уязвимости it-инфрастуктуры, оценка рисков, pos–системы.

Введение. В современном мире ресторанный бизнес, как и любой другой вид деятельности, подвержен киберугрозам. Согласно данным только за последний год количество кибератак на ресторанный бизнес возросло на 17% [1]. В данной отрасли наиболее часто происходят утечки персональные данных (далее — ПДн) гостей с их дальнейшей компрометацией.

В ресторанном бизнесе все чаще используются цифровые технологии, что несет за собой помимо улучшений бизнес-инфраструктуры, также множество новых уязвимостей [2].

Очевидна необходимость принятия мер для повышения защищенности корпоративной сети ресторанного бизнеса. Для этого подойдет специализированный комплекс мер. В ходе исследований был выбран объект исследования — сеть ресторанов г. Тюмени. Компания обеспокоена недостаточным уровнем информационной безопасности (далее — ИБ) в корпоративной сети организации.

В этой организации были инциденты, связанные с потерей важной информации. Например, был инцидент, когда был получен товар и никто не убедился в том, что при нем присутствует накладная. Когда в дальнейшем понадобилось ее наличие для подтверждения получения товара, ее не оказалось под рукой, соответственно, пришлось потратить дополнительное время и финансы, чтобы урегулировать этот вопрос. Из–за неучтенных аспектов ИБ, компания понесла финансовые убытки. Для минимизации убытков в будущем компании необходим комплекс мер по обеспечению ИБ.

Для разработки комплекса мер по улучшению ИБ корпоративной сети организации изучается нормативно-правовая база по защите информации и анализируются существующие риски ИБ в организации. Далее будет проведена оценка текущего состояния ИБ в корпоративной сети заказчика. С учетом этого спроектирован комплекс мер, включающий в себя систему защиты информации и ряд рекомендаций. Далее пойдет этап внедрения этого комплекса в корпоративную сеть, и его апробация апробирую его.

Проблема исследования. Объектом исследования является система и специфика ИБ в рамках ресторанного бизнеса.

В ходе исследования проводился анализ выявленных рисков с учетом особенностей обработки и передачи информации в этой корпоративной сети.

Особенностью такой системы является то, что компания управляет нескольким филиалами, которые соединены общей сетью и между ними происходит обмен важной информацией.

В рамках работы были поставлены следующие задачи:

- изучить нормативную базу по защите информации;
- определить особенности обработки и передачи информации ресторанного бизнеса;
- провести анализ рисков ИБ корпоративной сети организации.

Выполнение поставленных задач позволит в дальнейшем построить модель угроз/нарушителей, спроектировать систему защиту информации и разработать план внедрения спроектированной системы защиты информации в организацию ресторанного бизнеса. После разработки плана внедрения необходима апробация системы защиты информации внутри корпоративной сети организации.

Материалы и методы. Методами исследования являются анализ, изучение, экспериментирование. Анализ возможностей и функционала сетевого оборудования корпоративной сети организации проводится при непосредственном физическом присутствии. Параллельно, проводились изучение и анализ нормативно-правовой базы для определения порядка регулирования информации.

Результаты. Соблюдение федеральных законов по защите информации является неотъемлемой частью обеспечения ИБ. Поэтому первой задачей является изучение нормативно-правовой базы по защите информации для ресторанного бизнеса. Были выделены основные федеральные законы, которые регламентируют сферу ИБ [3, 4] и информацию, обрабатываемую в ресторанном бизнесе [5-8].

Далее на примере объекта исследования были определены какие типы информации обрабатываются в ресторанном бизнесе:

1) ПДн гостей (ФИО, данные платежных карт, данные бонусной карты, контактная информация: номер телефона, адрес электронной почты);
2) записи камер видеонаблюдения;
3) продуктовый учет;
4) меню ресторана;
5) технологические карты блюд;
6) веб–сайт ресторана;
7) номера телефонов ресторана;
8) договора о закупке продуктов для кухни;
9) договора о закупке оборудования для ресторана;
10) договора о закупке расходных материалов;
11) ПДн персонала (ФИО, сведения об образовании и квалификации, информация о трудовой деятельности, медицинская книжка, контактная информация: номер телефона, адрес проживания, адрес электронной почты).

Федеральные законы, регулирующие обработку приведенных выше типов информации: ФЗ-149, ФЗ-152, ФЗ-63, ФЗ-98, ФЗ-99, ФЗ-197 [3-8].

Далее были определены особенности обработки и передачи информации ресторанного бизнеса. Для этого была построена типовая топология корпоративной сети для двух филиалов

организации, где представлены сетевые устройства, их способ подключения и сторонние информационные сервисы, которые используются организацией.

Как видно, у данной топологии (рис. 1) есть свои минусы. В числе которых недостатки топологии «звезда». В случае, если главный коммутатор выйдет из строя, то и вся сеть перестанет функционировать. Также эта топология требует больших затрат на соединительные кабели, так как коммутатор соединяется с каждым устройством в сети. При большом количестве подключенных устройств нагрузка на центральный коммутатор возрастает, что может привести к снижению производительности сети. Стоит сказать, что из всех возможных типов топологий, она считается одной из самых простых в управлении [9]. При возникновении проблем с одним устройством его легко отключить от коммутатора, не влияя на работу остальной сети. Для увеличения отказоустойчивости сети, важно использовать правильную настройку центрального устройства.

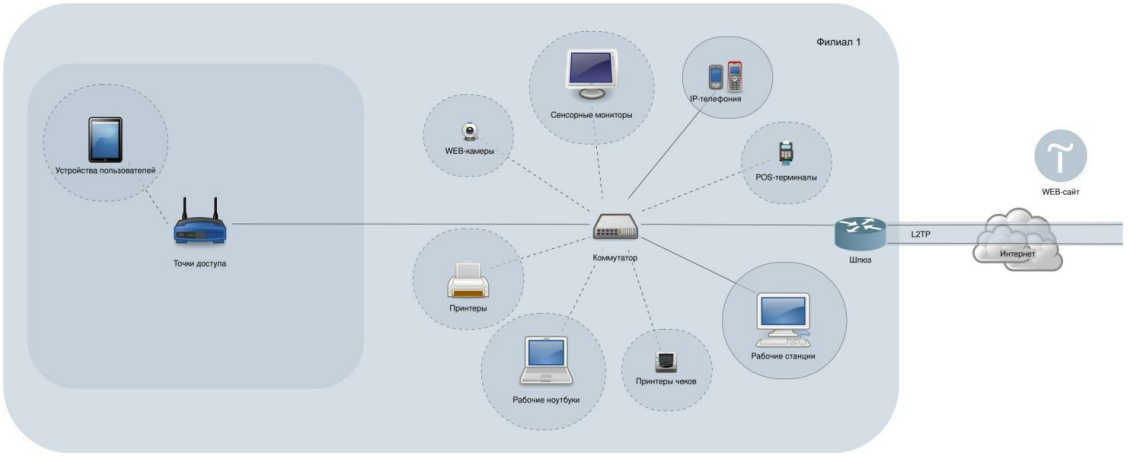

Рис. 1. Типовая топология корпоративной сети — Филиал № 1

Второй филиал организации базируется на смешанной топологии «шина» и «звезда» (см. рис. 2). Для главных серверов выделена отдельная подсеть, связанная шиной с топологией «звезда», объединяющей остальные устройства. Одним из существенных недостатков топологии «шина» является то, что при ее неполадке в любом месте (выход из строя сетевого коннектора, обрыв кабеля) сеть становится неработоспособной. Поэтому важно обеспечить надежность используемого оборудования и связующего кабеля. Коммутаторы, которые используются в организации — Cisco 2960. Как известно, компания Cisco ушла с российского рынка, и их поддержка полностью прекращена. Использование их сетевых устройств несет за собой риски для информационной безопасности, поскольку без обновлений безопасности сетевые устройства могут стать уязвимыми для различных киберугроз, таких как вирусы, атаки на систему и несанкционированный доступ. В качестве альтернативы были рассмотрены коммутаторы от компании Eltex — MES2324/MES2348 (коммутаторы с 24/48 гигабитными портами, в зависимости от потребностей сети). Для связи между филиалами используется L2TP туннель. Сам по себе он не обеспечивает конфиденциальность и шифрование трафика. Для повышения уровня ИБ необходимо использовать дополнительное шифрование трафика между филиалами, к примеру протокол IPsec, который прекрасно работает в связке с L2TP [10]. Web-сайт организации расположен на платформе Tilda. Она обеспечивает его отказоустойчивость.

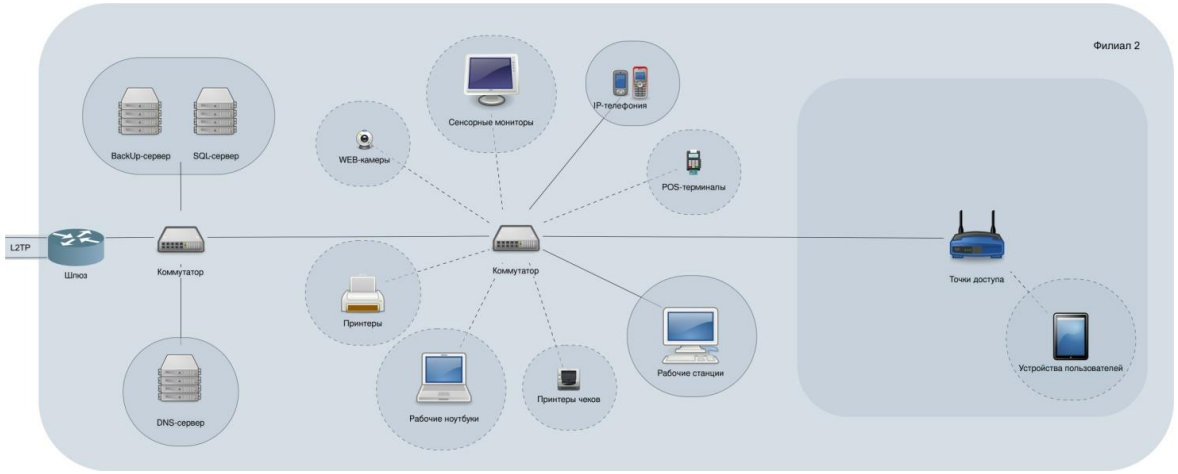

Рис. 2. Типовая топология корпоративной сети — Филиал № 2

Следующий этап — анализ рисков ИБ. Были выделены следующие риски:

1) утеря документов по закупке/получению товаров (например, при сбое сервера, где они хранятся);
2) кража ПДн клиентов/персонала ресторана;
3) взлом камер видеонаблюдения (с возможностью дальнейшей слежки для совершения неправомерных действий);
4) несанкционированный доступ к сетевому оборудованию;
5) сбой сетевого оборудования;
6) перехват и вскрытие трафика, ходящего между филиалами;
7) взлом терминалов;
8) взлом IP-телефонии (дальнейшее прослушивание с целью заполучить секретную информацию);
9) эксплуатация уязвимостей iiko-системы, ПО, установленного на корпоративных компьютерах;
10) ошибки персонала, неосведомленного в области защиты информации ресторана;
11) репутационные риски (кража рецептуры, подрыв доверия клиентов и персонала);
12) выход из строя главных серверов (SQL-сервер, DNS-сервер);
13) сбой инженерных систем (электросистема, водоснабжение и т.д.).

Заключение. В результате работы была изучена нормативно-правовая база по защите информации, определены особенности обработки и передачи информации в ресторанном бизнесе, проведен анализ рисков ИБ корпоративной сети организации. В дальнейшем планируется построение модели угроз и нарушителей на основе полученных данных, а также проектирование системы защиты информации с последующим планированием ее внедрения и апробацией в исследуемой организации.

СПИСОК ЛИТЕРАТУРЫ

1. Positive Technologies // Актуальные киберугрозы: II квартал 2023 года. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/ (дата обращения: 14.02.2024).

2. Козлов Д.А. Цифровые технологии в ресторанном бизнесе / Д.А. Козлов, О.И. Иринина // Научные достижения и открытия современной молодежи: сборник статей IV Международной научно-практической конференции, Пенза, 17 апреля 2018 года. — Пенза: «Наука и Просвещение» (ИП Гуляев Г.Ю.), 2018. — С. 66-71. — EDN YWOZYX. URL: https://elibrary.ru/item.asp?id=32830012.
3. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. — URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 17.02.2024).
4. Федеральный закон № 152 «О персональных данных» от 27.07.2006 г. — URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 18.02.2024).
5. Федеральный закон № 63 «Об электронной подписи» от 06.04.2011 г. — URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 18.02.2024).
6. Федеральный закон № 98 «О коммерческой тайне» от 29.07.2004 г. — URL: https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 18.02.2024).
7. Федеральный закон № 99 «О лицензировании отдельных видов деятельности» от 04.05.2011 г. — URL: https://www.consultant.ru/document/cons_doc_LAW_113658/ (дата обращения: 19.02.2024).
8. Федеральный закон № 197 «Трудовой кодекс Российской Федерации» от 30.12.2001 г. — URL: https://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 20.02.2024).
9. Топологии ЛВС: Оценка и Выбор // Статья на тему. — URL: https://www.drdoors-msc.ru/stati/topologia-lvc.html (дата обращения: 21.02.2024).