СТАТЬИ

УДК 004.942:004.056.5
DOI 10.17513/snt.39924

ТЕХНОЛОГИЯ КОРПОРАТИВНОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

[1]Башарина О.Ю., [1]Буценко Е.В., [2]Похомчикова Е.О., [3]Шильникова И.С.

ФГБОУ ВО «Уральский государственный экономический университет», Екатеринбург, e-mail: basharinaolga@mail.ru
ФГБОУ ВО «Иркутский национальный исследовательский технический университет», Иркутск, e-mail: elena.isea@mail.ru
ФГБОУ ВО «Иркутский государственный университет», Иркутск, e-mail: 19irina76@mail.ru

В статье рассматриваются актуальные вопросы, связанные с защитой информации от внутренних угроз. Организации сталкиваются с серьезными вызовами информационной безопасности, которые возникают из-за недобросовестных действий или ошибок сотрудников. Статья описывает процессы разработки и внедрения компьютерной программной системы, предназначенной для защиты персональных данных и конфиденциальной корпоративной информации. Представленная система основана на организационных обучающих процедурах, которые реализованы с помощью чат-бота мессенджера Telegram. Telegram-бот – удобный, доступный и эффективный инструмент для автоматизации рутинных задач. Благодаря своей мгновенной и надежной связи бот является отличным средством коммуникации внутри компании. Основными функциями разработанного Telegram-бота являются обучение пользователей принципам работы с конфиденциальной информацией, методам ее защиты, для проверки знаний предлагаются тестовые и кейс-задания. Также реализована возможность обращения к специалистам информационной безопасности при возникновении инцидентов. Умения сотрудников грамотно обращаться с данными, распознавать возможные угрозы их безопасности и правильно на них реагировать позволят создать безопасную информационную среду компании. Дальнейшее развитие проекта позволит совершенствовать процессы защиты данных и адаптировать программу под новые требования информационной безопасности корпоративных процедур.

Ключевые слова: персональные данные, чат-бот, Telegram, защита данных, информационная безопасность, разработка системы

TECHNOLOGY FOR CORPORATE PROTECTION OF PERSONAL DATA AND CONFIDENTIAL INFORMATION

[1]Basharina O.Yu., [1]Butsenko E.V., [2]Pokhomchikova E.O., [3]Shilnikova I.S.

Ural State University of Economics, Ekaterinburg, e-mail: basharinaolga@mail.ru
Irkutsk National Research Technical University, Irkutsk, e-mail: elena.isea@mail.ru
Irkutsk State University, Irkutsk, e-mail: 19irina76@mail.ru

The article reveals the current issues related to the protection of information from internal threats. The companies face the serious information security challenges caused by employees' unfair activities or mistakes. The article describes the processes of development and implementation of a computer software system, designed to protect personal data and confidential corporate information. The represented system is based on organizational educational procedures which are implemented via the Telegram messenger chatbot. The Telegram bot is a convenient, accessible, and effective tool for automating routine tasks. Due to its instant and reliable communication, the bot is an excellent means of communication within the company. The developed Telegram bot is designed to make the process of users training automotive in terms of the principles of working with confidential information and methods of protecting it. The results of education are tested, using tests and case assignments. The ability to contact information security specialists in the case of incidents has also been foreseen. The ability of the staff to handle data competently, to recognize possible threats to their security and respond to these threats correctly will help increase the level of security of the company's information environment. The further development of the project is aimed at improving the data protection processes and adapting the chatbot to new information security requirements of corporate procedures.

Keywords: personal data, chatbot, Telegram, data protection, system development, information security

Бурный рост объемов хранимых и обрабатываемых данных, вызванных, в частности, использованием современных ИТ и расширением клиентской базы хозяйствующих субъектов, требует повышения уровня защищенности этих данных. Особое внимание в деятельности любой компании должно быть уделено защите персональных данных сотрудников и клиентов в соответствии с требованиями законодательства в сфере обеспечения конфиденциальности и безопасности информации [1]. Использование современных методов защиты информации и многоуровневого

подхода, включающего надежные процедуры аутентификации, шифрования данных, резервного копирования и восстановления данных, позволит снизить потери данных и реализовать необходимые бизнес-процессы компании [2; 3].

Важным также является уровень компетентности сотрудников в работе с персональными данными компании, поэтому необходимо проводить регулярное обучение работников, включающее изучение нормативно-правовой информации, методов распознавания и снижения потенциальных угроз и формирование навыков по снижению и/или устранению выявленных угроз [4; 5].

Серьезные внутренние угрозы информационной безопасности возникают из-за недобросовестных действий сотрудников, ошибок и недостатков в системах и процессах. Проведённый компанией Gartner опрос показал, что 69% сотрудников нарушали регламенты своей организации в области кибербезопасности [6]. Такие случайные или преднамеренные действия персонала могут иметь катастрофические последствия для компании: утечка конфиденциальной информации, финансовые потери и повреждение репутации.

Обучение сотрудников работе с конфиденциальной информацией и их информированность в этой сфере являются ключевыми факторами в защите данных [7]. Грамотные пользователи с необходимыми знаниями и навыками, а также регулярное информирование о возможных угрозах и методах защиты помогают создать безопасную среду в организации и предотвратить потенциальные нарушения конфиденциальности и целостности информации.

Материалы и методы исследования

Методы защиты персональных данных принято разделять на правовые, организационные и технические. Правовые методы устанавливаются государственными органами и включают различные нормативно-правовые акты, регулирующие деятельность по работе с персональными данными. Организационные меры устанавливают для сотрудников компании четкие правила и регламенты работы с конфиденциальной информацией. К техническим методам защиты относятся физические, аппаратные и программные средства, позволяющие защитить персональные данные от несанкционированного доступа [8; 9].

Целью данной работы является автоматизация организационных методов защиты, в частности процессов информирования и обучения персонала правилам обращения с персональными данными и предотвращения утечки данных, с помощью программных средств для мессенджера Telegram. На его платформе разработан чат-бот, который служит инструментальной средой для автоматизации процесса обучения в системе защиты персональных данных.

Telegram-боты обладают целым рядом преимуществ, которые делают их популярными и удобными инструментами для различных задач (табл.).

Преимущества инструментального средства Telegram-бот

Преимущество	Характеристика
Удобство использования	Интерфейс мессенджера позволяет легко и быстро настраивать и управлять сценарием, не требуя навыков программирования
Автоматизация задач	Инструментарий бота реализует широкий спектр решаемых задач, связанных с автоматизацией отправки/получения сообщений, рассылки информации, уведомлений, создания опросов и др.
Быстрый доступ к информации	Обработка запросов осуществляется в режиме реального времени, благодаря этому обмен данными происходит достаточно быстро
Низкая стоимость	Создание и поддержка Telegram-ботов не требует привлечения высококвалифицированных программистов, занимает меньшее время на разработку приложения, тем самым значительно снижая затраты на автоматизацию задач
Безопасность данных	Технологии защиты данных мессенджера гарантируют высокий уровень конфиденциальности информации
Интеграция с другими сервисами	Инструментальные возможности Telegram-ботов позволяют использовать их сторонними приложениями и сервисами
Универсальность	Чат-боты широко используются для поддержки пользователей в различных сферах, таких как маркетинг, продажи, образование, медицина, финансы, консалтинг, логистика и др.

Проект разработки Telegram-бота включал нескольких этапов. Вначале были определены цель проекта, требования к функционалу бота, проведен анализ аналогичных продуктов и программных сервисов. В качестве инструментальной программной среды была выбрана платформа Robochat, она имеет удобный и понятный интерфейс, ее базовый функционал предоставляется бесплатно. Далее были разработаны сценарии бота, реализующие поставленные задачи проекта. После успешного прохождения тестирования и отладки Telegram-бот был внедрен в эксплуатацию. Кроме того, необходимо обеспечить поддержку работоспособности бота.

Результаты исследования и их обсуждение

Функционал бота включает следующие сервисы по защите персональных данных: сообщение о проблеме; проверка входящего сообщения; связь с дежурным специалистом; обучение персонала (рис. 1).

Обучение в свою очередь состоит из трёх сценариев: теория, тесты, кейсы. Блок «Теория» разбит на три раздела: общая информация; методы защиты персональных данных; нормативно-правовые акты (НПА).

Система Telegram-бота включает в себя множество взаимосвязанных сценариев, что позволяет упростить процесс разработки и навигации.

На первом этапе разработки бота необходимо указать ключевые слова для перехода к боту, поприветствовать пользователя, реализовать защиту от набора несуществующих команд и разработать главное меню. Сценарий основного меню бота представлен на рисунке 2. Экранная форма начального этапа приветствия и меню представлена на рисунке 3.

Сотрудники компании должны быть осведомлены о возможных угрозах, с которыми они могут столкнуться в Сети. Это включает в себя знания о социальной инженерии, фишинге, вредоносном программном обеспечении и других методах атаки. Пользователи должны быть обучены распознавать подозрительные письма, ссылки или запросы, а также знать, как сообщать о подобных инцидентах.

Команды бота «Сообщить о проблеме», «Проверка почтового сообщения» и «Связь с дежурным специалистом» позволяют направить информацию о предполагаемых угрозах (рис. 4) или оперативно связаться со специалистом информационной безопасности. Информация о входящем сообщении или проблеме будет переслана администратору бота, ответственному лицу или в группу экспертов информационной безопасности в зависимости от настроек бота.

Важным является и реализация проверки почтового обращения, которая актуальна в случае поступления сотруднику на почту письма с подозрительной ссылкой.

Вместе с развитием технологий появляются новые угрозы и методы атаки. Пользователи должны быть осведомлены о последних трендах в области кибербезопасности и обучены новым методам защиты. Это поможет им быть готовыми к новым угрозам и эффективно реагировать на них.

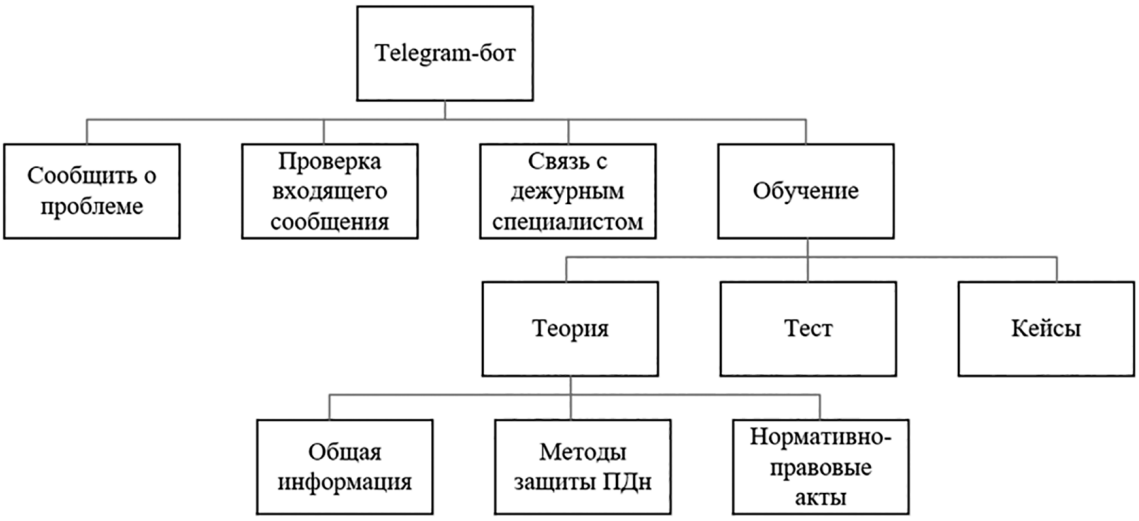

Рис. 1. Схема работы Telegram-бота

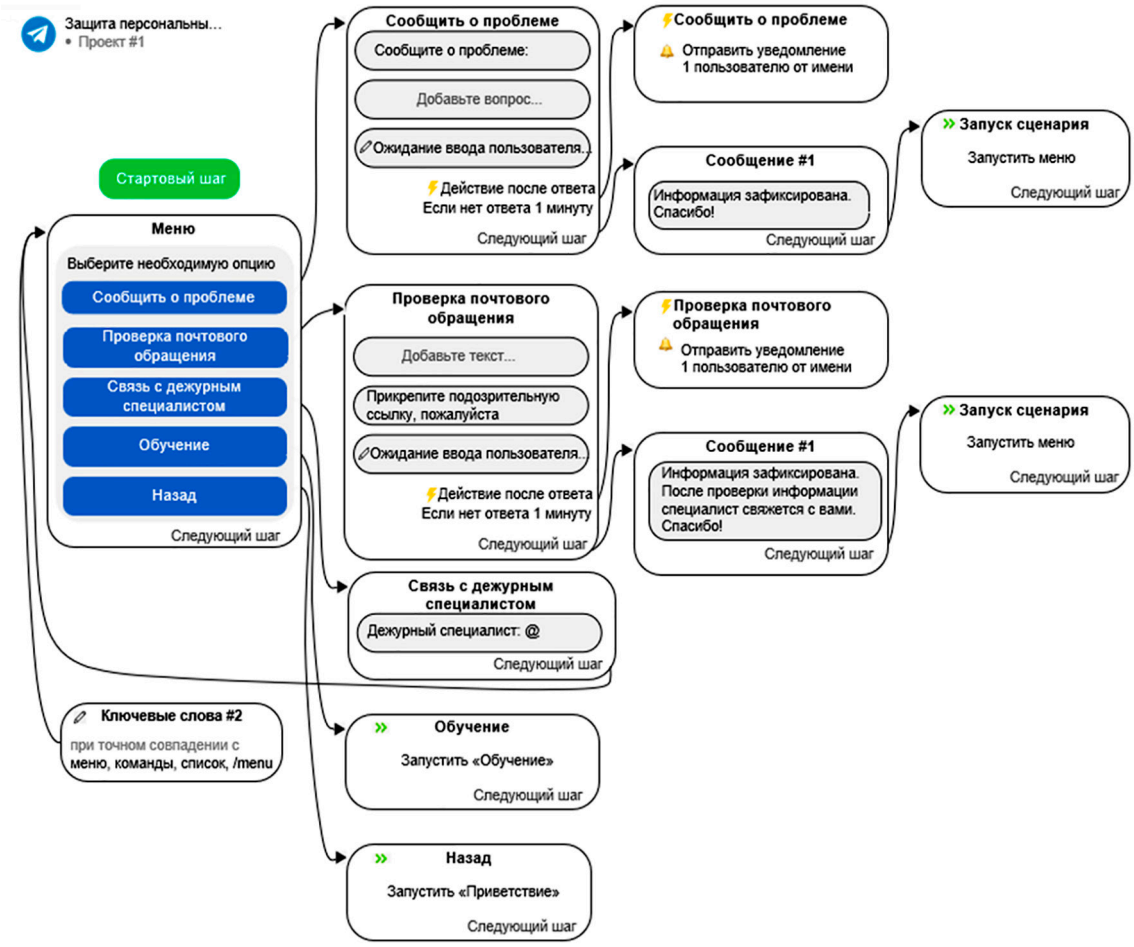

Рис. 2. Сценарий основного меню бота

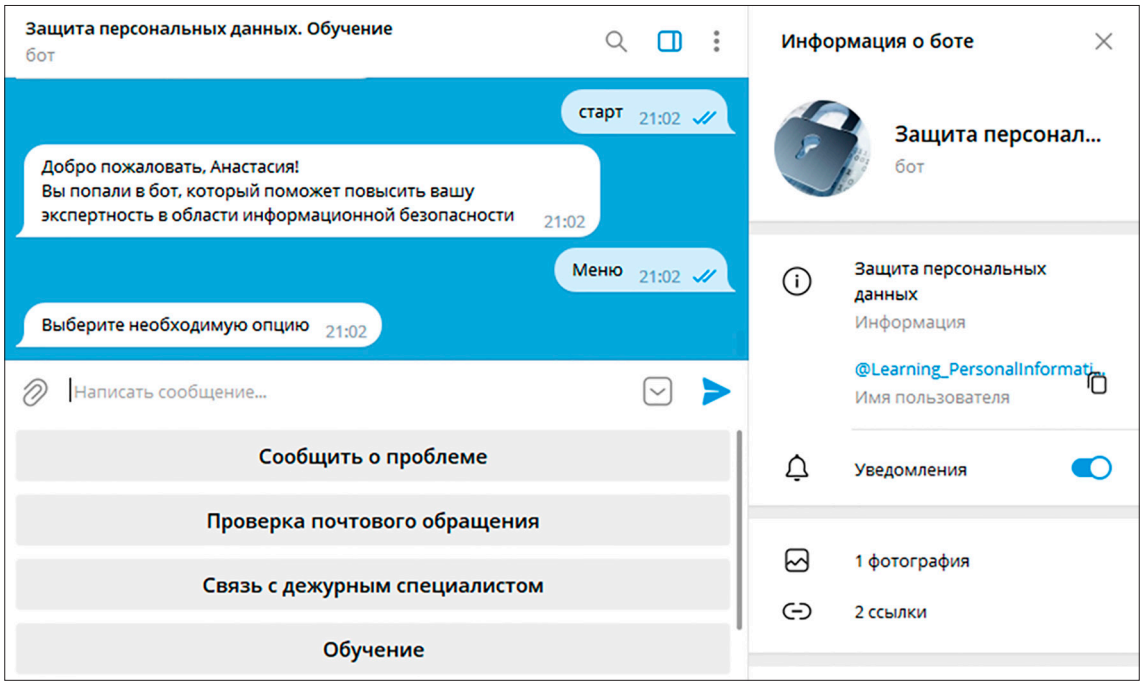

Рис. 3. Экранная форма меню бота

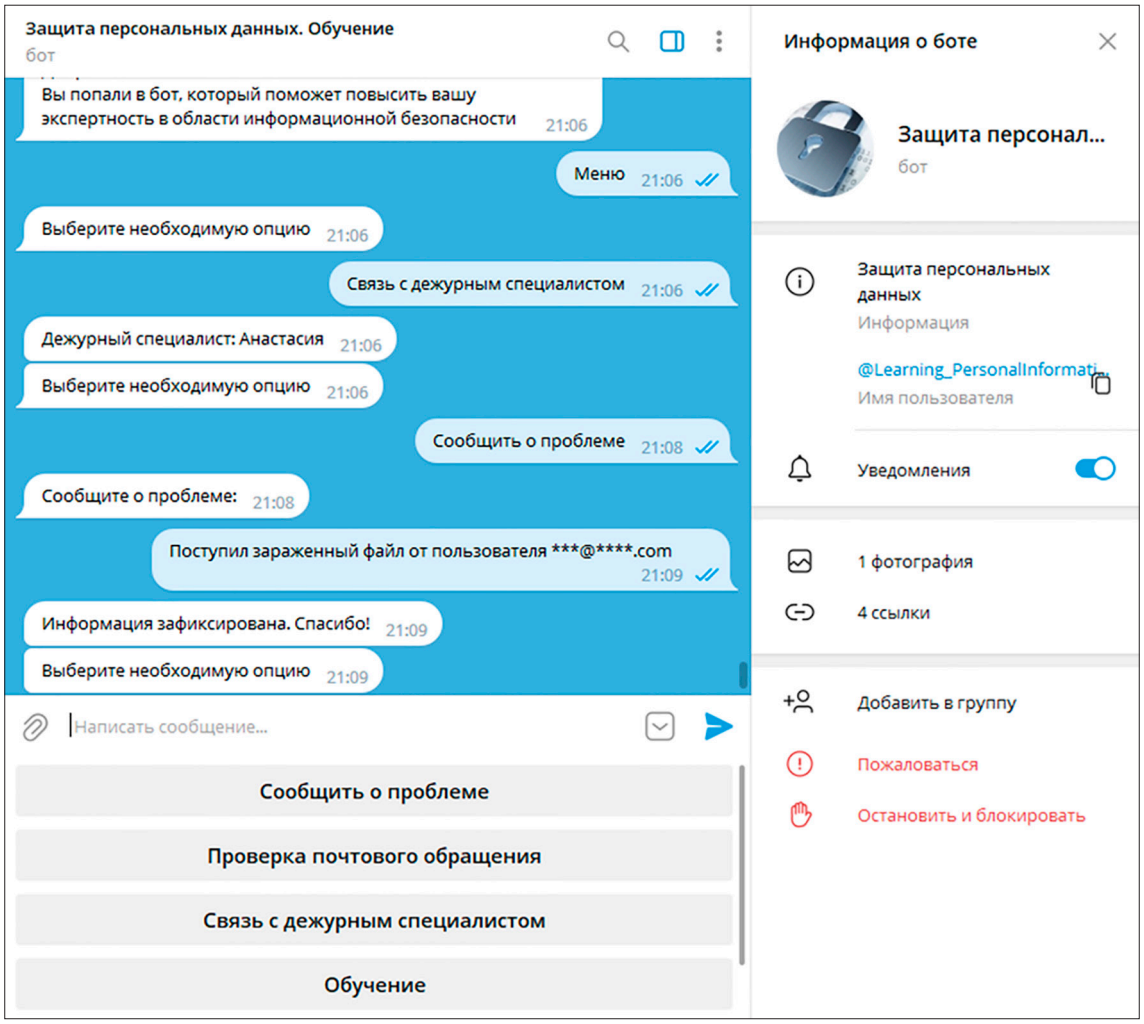

Рис. 4. Информирование пользователем о проблеме

Важно отметить, что обучение и осведомленность должны быть непрерывными процессами. Организация должна предоставлять регулярные обучающие программы и информационные материалы, чтобы поддерживать высокий уровень осведомленности среди пользователей.

Кроме того, необходимо устанавливать политики и процедуры, которые обеспечивают безопасное обращение с конфиденциальной информацией, и регулярно проверять их соблюдение.

На основании вышеизложенного в раздел «Обучение» включены три сценария: теория, тесты, кейсы. Блок «Теория» предлагает пользователю изучить нормативно-правовые акты и методы защиты персональных данных, в дальнейшем оценивает их усвоение с помощью тестовых или кейс-заданий.

В рамках сценария «Тесты» действия пользователя будут играть роль счётчика, который перед первым вопросом обнуляет количество заработанных баллов, а далее при верном ответе добавляет их. Проверка ответа на правильность осуществляется через привязку к кнопке действия на добавление балла. По итогам выбора кнопки с тем или иным вариантом ответа тестируемому будет сообщен результат правильности данного варианта. Реализация перехода к тестовому вопросу и его проверки представлена на рисунке 5.

По итогам тестирования пользователь получает определенное количество баллов. Если результат тестирования неудовлетворительный, пользователю предлагается пройти его повторно. Раздел «Кейсы» предназначен для того, чтобы тестируемый сотрудник на примере различных ситуаций смог проверить свои знания. Процесс реализации данного сценария аналогичен сценарию «Тесты».

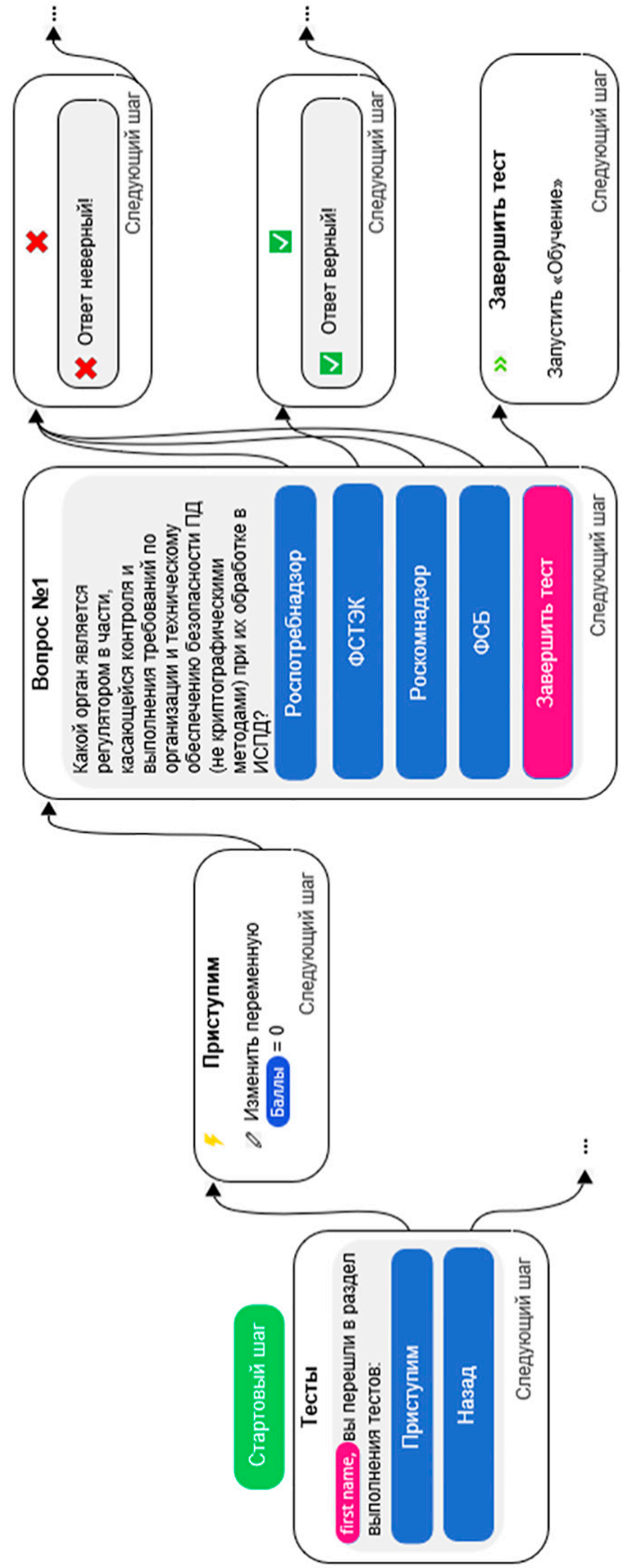

Рис. 5. Фрагмент сценария реализации тестового вопроса пользователю

Заключение

В условиях стремительного роста объема генерируемых данных защита конфиденциальности и безопасности данных приобретает первостепенное значение. Организациям необходимо применять многоуровневый подход к обеспечению безопасности, постоянно обновлять технологии защиты и соблюдать соответствующие нормативные требования по защите данных. Уделяя должное внимание защите конфиденциальности и безопасности данных, организации снижают риски имиджевых и финансовых потерь.

Внутренняя угроза защиты данных является приоритетной, и в большинстве своем она исходит от сотрудников, которые не понимают значимость мероприятий по защите конфиденциальной информации, не знают или пренебрегают регламентами кибербезопасности. Именно поэтому необходимо регулярное информирование сотрудников и их обучение работе с конфиденциальными данными.

В целом можно сказать, что реализация корпоративной системы защиты персональных данных путем создания Telegram-бота является хорошим решением для обучения сотрудников – бот прост для понимания, интерактивен и достаточно надежен. Функциональность бота может быть усовершенствована с помощью добавления новых разделов, дополнения имеющихся тестов, кейсов, справочной и нормативно-правовой информации.

Список литературы

1. Электронный фонд правовых и нормативно-технических документов. ФСТЭК. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. URL: https://docs.cntd.ru/document/902330983 (дата обращения: 15.10.2023).

2. Портал компании SearchInform. Защита информации от несанкционированного доступа [Электронный ресурс]. URL: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/ot-nesanktsionirovannogo-dostupa/ (дата обращения: 10.10.2023).

3. Селюк А.С. Защита персональных данных в цифровом пространстве // Вестник Университета имени О.Е. Кутафина. 2023. № 2 (102). С. 110-119.

4. Портал Центра безопасности данных. Угрозы безопасности персональных данных [Электронный ресурс]. URL: https://data-sec.ru/personal-data/threats/ (дата обращения: 23.11.2023).

5. Соколова А.В., Гришкевич Д.Д., Губенко И.М. Обзор методов и средств защиты персональных данных // Информационное общество. 2022. № 3. С. 90-97.

6. Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025. URL: https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025 (дата обращения: 29.05.2023).

7. Санникова А.С., Фастович Г.Г. К вопросу о защите персональных данных // Вестник науки. 2019. Т. 5, № 3 (12). С. 83-86.

8. Буценко Е.В. Разработка системы информационной безопасности компании на основе методов инженерно-технической защиты информации // Урал – драйвер неоиндустриального и инновационного развития России: Материалы IV Урал. эконом. форума (Екатеринбург, 20-21 октября 2022 г.). Екатеринбург: Изд-во УрГЭУ, 2022. С. 147-153.

9. Евстифеев А.А., Ерошев В.И., Мартынов А.П. Основы защиты информации от утечки по техническим каналам. Саров: РФЯЦ-ВНИИЭФ, 2019. 267 с.