ТЕХНИКАЛЫҚ ҒЫЛЫМДАР
ТЕХНИЧЕСКИЕ НАУКИ
TECHNICAL SCIENCE

CENTRAL ASIAN SCIENTIFIC JOURNAL
ISSN 3135-3061
2026. №4 (32), Том 2. С. 402–405
DOI: https://doi.org/10.5281/zenodo.24299017
Сайт журнала: https://cajournal.kz

УДК 004.056:352

МОДЕЛЬ УГРОЗ И МЕРЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЗАЯВКАМИ ЖИТЕЛЕЙ НА УСТРАНЕНИЕ ГОРОДСКИХ ПРОБЛЕМ

Д.К. Жунусов
Казахский национальный исследовательский технический университет имени К.И. Сатпаева (КазНИТУ), Алматы, Казахстан

Жунусов Даниял Куатович — студент 4 курса образовательной программы «Информационная безопасность», Казахский национальный исследовательский технический университет имени К.И. Сатпаева (КазНИТУ), Алматы, Казахстан.

Научный руководитель: Юбузова Халича Ибрагимовна — PhD, ассоциированный профессор кафедры кибербезопасности, Институт автоматики и информационных технологий, Казахский национальный исследовательский технический университет имени К.И. Сатпаева (КазНИТУ), Алматы, Казахстан.

© Д.К. Жунусов, 2026

Аннотация: В статье рассматривается информационная безопасность системы управления заявками жителей на устранение городских проблем, обрабатывающей персональные данные заявителей. Цель работы — построить модель угроз системы и обосновать минимальный набор мер защиты. Методы: декомпозиция системы на компоненты и потоки данных, классификация угроз по модели STRIDE, качественная оценка рисков по подходу ISO/IEC 27005. Выявлено шесть значимых угроз, три из которых относятся к высокому уровню риска; показано, что комплекс из шести организационно-технических мер снижает суммарный риск с 76 до 27 баллов и устраняет угрозы высокого уровня.

Ключевые слова: информационная безопасность, персональные данные, модель угроз, STRIDE, оценка рисков, контроль доступа, городские заявки

Введение

Обращения жителей о неисправностях городской инфраструктуры — разбитых дорогах, неработающем освещении, переполненных контейнерах, открытых люках — традиционно принимаются по телефону, через социальные сети и в приёмных. Разрозненный приём приводит к потере заявок, дублированию работы и невозможности проследить, на каком этапе находится устранение проблемы. Информационная система управления заявками (далее — ИС) решает эту задачу: она объединяет приём, маршрутизацию, контроль сроков и информирование заявителя в едином контуре.

Вместе с тем такая система неизбежно становится оператором персональных данных. Заявка содержит имя заявителя, номер телефона и адрес, а приложенная фотография может нести сведения о месте и времени съёмки. Закон Республики Казахстан «О персональных данных и их защите» обязывает собственников и операторов принимать меры по защите подобных сведений [1], а объекты информатизации, используемые в публичном управлении, подпадают под требования законодательства об информатизации [2]. На практике же

учебные и пилотные разработки проектируются с упором на функциональность, а вопросы безопасности откладываются на этап эксплуатации, когда исправлять архитектурные ошибки значительно дороже.

Цель работы — построить модель угроз ИС управления заявками жителей и обосновать минимально необходимый набор мер защиты. Для её достижения требуется описать архитектуру и роли пользователей, выявить угрозы, оценить риски до и после применения мер и сформулировать требования к защите, пригодные для включения в техническое задание.

Материалы и методы

Объектом исследования выступает ИС, проектируемая в рамках учебного курса. Она состоит из веб-клиента жителя, кабинетов оператора и исполнителя, серверной части с программным интерфейсом, реляционной базы данных, хранилища фотографий и модуля уведомлений. Заявка проходит этапы: создание жителем, проверка оператором, назначение исполнителю, выполнение работ и закрытие после подтверждения. Система различает четыре роли: житель, оператор, исполнитель и администратор.

Для выявления угроз каждый компонент и поток данных рассматривался по модели STRIDE, которая выделяет шесть категорий угроз: подмену личности, изменение данных, отказ от авторства, раскрытие информации, отказ в обслуживании и повышение привилегий [4]. Типовые веб-уязвимости сверялись с перечнем OWASP Top 10 [3]. Оценка риска выполнялась качественным методом в духе стандарта ISO/IEC 27005 [5] по формуле:

$$R = P \times I \quad (1)$$

где R — уровень риска, баллы; P — вероятность реализации угрозы по шкале от 1 до 5; I — тяжесть последствий по шкале от 1 до 5.

Риск считался низким при $R \le 6$, средним при $8 \le R \le 12$ и высоким при $R \ge 15$. Оценки P и I выставлены автором экспертно по результатам анализа архитектуры и не опираются на статистику реальных инцидентов, поэтому результаты носят предварительный характер. После выбора мер защиты вероятность пересчитывалась, а тяжесть последствий оставалась прежней, так как ущерб от уже случившегося события мерами предотвращения не меняется.

Результаты и обсуждение

Анализ потоков данных показал шесть значимых угроз; их описание и оценки приведены в таблице 1.

Таблица 1 – Угрозы ИС и оценка рисков до внедрения мер защиты

№	Угроза (категория STRIDE)	P	I	R	Уровень
У1	Подбор или кража учётных данных жителя (подмена личности)	4	4	16	Высокий
У2	Доступ к чужим заявкам через подмену идентификатора в запросе (повышение привилегий)	4	4	16	Высокий
У3	SQL-инъекция через поля формы заявки (изменение данных)	3	5	15	Высокий
У4	Раскрытие места съёмки и контактов через метаданные фотографий (раскрытие информации)	4	3	12	Средний
У5	Изменение статуса заявки без следа (отказ от авторства)	3	3	9	Средний
У6	Массовая подача фиктивных заявок (отказ в обслуживании)	4	2	8	Средний

Наибольший риск (16 баллов) у подмены личности и нарушения контроля доступа. Вторая угроза типична для систем, где сервер проверяет, что пользователь вошёл в систему, но не проверяет, что запрашиваемая заявка принадлежит именно ему: подстановка чужого номера заявки в адрес запроса открывает чужие персональные данные. Нарушение контроля доступа возглавляет перечень OWASP Top 10 [3], а значит, это не экзотический, а наиболее

вероятный сценарий. Угроза У3 имеет наименьшую вероятность, но максимальную тяжесть, поскольку успешная инъекция затрагивает всю базу данных.

Для снижения рисков предложен комплекс из шести мер. Первая — защита аутентификации: пароли хранятся только в виде солёных хэшей (bcrypt или Argon2), требования к паролю строятся на рекомендациях NIST, которые делают упор на достаточную длину и проверку по спискам скомпрометированных паролей, а не на периодическую смену [6]; для операторов и администраторов вводится второй фактор. Вторая — ролевая модель с проверкой владельца объекта на стороне сервера при каждом запросе; исполнитель видит контакты заявителя только по назначенной ему заявке, а публичная карта показывает обезличенные данные. Третья — параметризованные запросы, проверка входных данных и учётная запись базы данных с минимальными правами. Четвёртая — удаление метаданных из загружаемых фотографий, проверка типа и размера файла. Пятая — журнал аудита, фиксирующий каждую смену статуса с указанием пользователя и времени. Шестая — ограничение частоты запросов и подтверждение номера телефона при подаче заявки. Канал связи защищается протоколом TLS, а контактные данные шифруются при хранении.

Результат применения мер показан на рисунке 1.

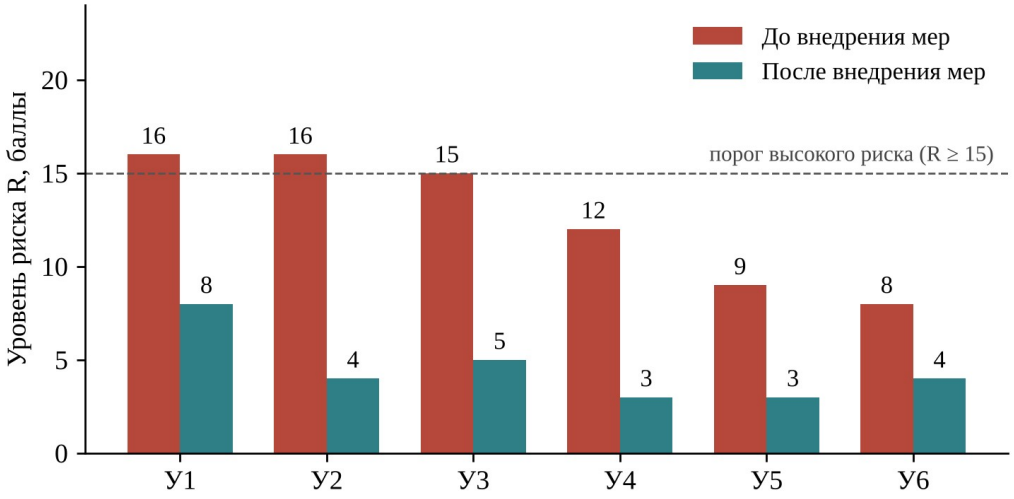


Рисунок 1 - Уровень риска по угрозам до и после внедрения мер защиты, баллы

Суммарный риск снижается с 76 до 27 баллов, то есть примерно на 64 %, а средний уровень риска на одну угрозу — с 12,7 до 4,5 балла. Угроз высокого уровня после внедрения мер не остаётся. Средний уровень сохраняет только У1 (8 баллов): здесь значительную долю вероятности составляет человеческий фактор — фишинг и передача пароля третьим лицам, который техническими средствами устраняется лишь частично и требует просветительской работы с жителями.

Предложенный подход имеет ограничения. Во-первых, оценки экспертные и должны быть уточнены по результатам тестирования прототипа, например сканированием уязвимостей и проверкой сценариев У2 и У3 вручную. Во-вторых, меры не должны создавать лишних барьеров: если потребовать от жителя второй фактор при каждой подаче заявки, часть обращений просто не будет подана, поэтому для жителей он остаётся необязательным, а основной упор делается на проверку телефона и ограничение частоты запросов. Практическая ценность результатов в том, что перечень угроз и мер можно сразу использовать как чек-лист требований безопасности в техническом задании на ИС.

Заключение

В работе построена модель угроз ИС управления заявками жителей на устранение городских проблем: выявлено шесть значимых угроз, из которых три относятся к высокому уровню риска. Предложенный комплекс мер — защита аутентификации, серверный контроль доступа, защита от инъекций, очистка метаданных файлов, журнал аудита и ограничение

частоты запросов — снижает суммарный риск с 76 до 27 баллов. Дальнейшая работа предполагает реализацию мер в прототипе системы и экспериментальную проверку их эффективности, что станет основой для практической части выпускной работы.

Список литературы:

1. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» [Электронный ресурс]. – URL: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 17.11.2026).

2. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» [Электронный ресурс]. – URL: https://adilet.zan.kz/rus/docs/Z1500000418 (дата обращения: 17.11.2026).

3. OWASP Top 10:2021 [Электронный ресурс]. – OWASP Foundation, 2021. – URL: https://owasp.org/Top10/ (дата обращения: 17.11.2026).

4. Shostack A. Threat Modeling: Designing for Security. – Indianapolis: John Wiley & Sons, 2014. – 624 p.

5. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. – Geneva: ISO, 2022.

6. NIST SP 800-63B-4. Digital Identity Guidelines: Authentication and Authenticator Management [Электронный ресурс]. – Gaithersburg: NIST, 2025. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf (дата обращения: 17.11.2026).

© Central Asian Scientific Journal, 2026