КиберЛаб

УТВЕРЖДАЮ
ральный директор
ООО «КиберЛаб»
___ Шайдерова И.Л.
декабря 2025 года

ИНФОРМАЦИЯ ДЛЯ УСТАНОВКИ И ЭКСПЛУАТАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ РУКОВОДСТВО ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ Ai.Industry.Platform

Руководство по безопасной разработке
«Ai.Industry.Platform»

1. Идентификация и аутенфикация

1.1. Реализуйте надежные механизмы идентификации и аутентификации для контроля доступа к системе.

1.2. Поддерживайте использование сильных паролей и многофакторной аутентификации.

2. Управление доступом

2.1. Внедрите систему управления доступом на основе ролей и принципа наименьших привилегий.

2.2. Обеспечьте постоянный мониторинг и аудит доступа для выявления подозрительных активностей.

3. Защита данных

3.1. Шифруйте конфиденциальные данные при передаче и хранении.

3.2. Регулярно создавайте резервные копии данных.

3.3. Выполнять иные поручения Непосредственного руководителя, а в период

4. Мониторинг и обнаружение инцидентов

4.1. Внедрите системы мониторинга для отслеживания активности в сети.

4.2. Создайте процедуры реагирования на инциденты и планы обеспечения непрерывности бизнеса.

4.3. Требования к ИТ-мониторингу АС

• Обеспечьте визуализацию всех межкомпонентных и межсистемных взаимодействий со светофорами работоспособности.

• Реализуйте метрики в разрезе каналов поступления информации.

• Синхронизируйте вывод нового функционала с разработкой соответствующих метрик.

4.4. Требования к бизнес-мониторингу АС

• Реализуйте инструменты для онлайн-мониторинга бизнес-процессов.

• Обеспечьте визуализацию метрик для владельцев продуктов.

5. Обновления и патчи

5.1. Регулярно обновляйте операционные системы, прикладное ПО и другие компоненты системы.

6. Тестирование безопасности

6.1. Проводите регулярные тесты на проникновение.

6.2. Выполняйте аудит систем и процессов безопасности.

7. Соблюдение стандартов безопасности

7.1. Соблюдайте требования стандартов:

- ГОСТ Р ИСО/МЭК 15408;
- ГОСТ Р ИСО/МЭК 27034;
- ГОСТ Р ИСО/МЭК 27035;
- ГОСТ Р ИСО/МЭК 30111;
- ГОСТ Р ИСО/МЭК 15446.

7.2. Проводите регулярный аудит соответствия.

8. Требования к разработке

8.1. Защита от инъекций:

• Реализуйте валидацию входящих данных на frontend (регулярные выражения, правила OWASP);

• Интегрируйте WAF (например, ModSecurity);

• Используйте параметризированные запросы к БД;

• Правильно применяйте ORM-технологии.

8.2. Защита от XSS-атак:

• Преобразуйте специальные символы HTML (<, >, (,), #, &) в соответствующие сущности;

• Используйте innerText вместо innerHTML;

• Применяйте метод ValidateRequest для проверки входных данных;

• Реализуйте проверку данных на стороне сервера;

• Запретите ввод HTML-тегов в пользовательских данных;

• Используйте капчу или ограничение запросов для неавторизованных пользователей.

8.3. Обработка ошибок:

• Не раскрывайте подробную информацию об ошибках пользователям;

• Сохраняйте полные сообщения об ошибках в журнале аудита;

• Используйте стандартные HTTP-статусы ответов;

• Обеспечьте защиту от раскрытия структуры файловой системы и фрагментов кода.

8.4. Работа с данными:

• Используйте только легальные данные с подтвержденным происхождением;

• Обрабатывайте персональные данные только с согласия субъектов;

• Реализуйте функционал проверки согласия и удаления ПДн;

• Исключите использование внешних сущностей в XML.

8.5. Аудит и логирование:

• Фиксируйте события аудита с обязательным набором атрибутов;

• Обеспечьте неизменность и защиту данных аудита;

• Реализуйте локальную буферизацию событий при недоступности централизованного аудита;

• Настройте срок хранения данных аудита.

9. Инфраструктурные требования:

• Выносите административные панели на отдельные URL с ограниченным доступом;

• Настройте TLS с обязательной аутентификацией и шифрованием;

• Реализуйте автоматическую блокировку пользователей при множественных неудачных попытках аутентификации;

• Отключайте автозаполнение для полей ввода секретной информации;

• Контролируйте версии и уязвимости используемых библиотек;

• Проверяйте сторонние JavaScript-ресурсы.

10. Пользовательские взаимодействия:

• Ограничьте прямой доступ к защищенным ресурсам;

• Не сохраняйте чувствительные данные в клиентских хранилищах;

• Реализуйте валидацию номеров телефонов по формату и типам номеров.

11. Одноразовые пароли (ОТП):

• Генерируйте ОТП-коды длиной от 6 символов со сроком жизни до 5 минут;

• Ограничивайте количество попыток ввода (рекомендуется 3 попытки);

• Контролируйте частоту отправки ОТП-кодов на один номер;

• Фиксируйте события проверки ОТП в журнале аудита;

• Используйте SMS для отправки ОТП-кодов при критичных операциях.

12. Приложение представлено в виде набора контейнеров. Список контейнеров образа виртуальной машины приложения:

Имя	порт	Назначение	Версия
frontend	80	Интерфейс приложения	0.1.0
backend	3000	Функциональная часть	0.0.1
minio-server	9000,9001	Файловое хранилище	От 2024-01-29
postgres	5432	База данных	14.8

• Файлы приложения размещены в каталоге /home/ikt/app/

• Каталог содержит файлы базы данных, файлового хранилища, а также образы составляющих частей приложения.

13. Настройка сети:

• Контейнеры доступны на перечисленных портах виртуальной машины по ip адресу заданного при старте ВМ.

• Запуск приложения происходит автоматический при старте ВМ.

14. Файл диска виртуальной машины с установленным экземпляром приложения:

• https://disk.yandex.ru/d/ZiekVDtLyLa0dg