

**ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
АВТОМАТИЗАЦИИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ПОДГОТОВКИ И
ОЦЕНКИ СООТВЕТСТВИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ
«СОКОЛ» (ППО «СОКОЛ») ВЕРСИИ 1.0**

**РАЗРАБОТКА, СОВЕРШЕНСТВОВАНИЕ И
ПОДДЕРЖКА ППО**

Страниц 8

МОСКВА

2026

1. РЕШЕНИЕ ПРОБЛЕМ В ПО

Для решения проблем в работе ППО «СОКОЛ» используется следующий алгоритм:

1. Пользователь системы обратился в отдел технической поддержки компании-разработчика через портал техподдержки (ПТП) либо направил обращение на электронную почту info@techinnovations.ru.
2. Менеджер технической поддержки фиксирует проблему. Созданная задача передается инженеру технической поддержки.
3. Инженер задает уточняющие вопросы и пытается воспроизвести проблему. Если воспроизведение не удалось на стороне Заказчика, проблема воспроизводится в тестовом контуре Разработчика (AuthService + Planning + MinIO + Valkey). Если воспроизвести не удалось вовсе, задача закрывается с уведомлением Заказчика.
4. Подтверждённая ошибка регистрируется в баг-трекере с приоритетом (критичностью) и передается разработчику.
5. Исправление включается в очередной релиз. Вместе с релизом выпускается документ «Что нового».

Алгоритм при использовании неизвестной уязвимости для атаки на информационную систему Заказчика:

1. Обращение фиксируется как инцидент информационной безопасности.
2. При подтверждении на контуре Заказчика принимаются срочные меры: блокировка отдельных компонентов (Admin UI, загрузка файлов в MinIO, внутренний API), пересмотр регламентов доступа, изоляция сегмента, уведомление иных Заказчиков при типовом характере уязвимости.
3. Собираются журналы AuthService и Planning Backend, события смены статусов, аудит контейнерной среды.
4. Выпускается срочное исправление либо временная компенсационная мера (отключение функции без остановки всего комплекса — модульная поставка это допускает).

1.1. Экстренный выпуск обновлений

Перечень ситуаций, при которых возможен экстренный выпуск обновлений в обход стандартной процедуры:

- неработоспособность ключевых серверных компонентов на отдельных версиях системного ПО, оборудования или платформ виртуализации;

- конфликт с прикладным или системным ПО Заказчика, приводящий к остановке бизнеса;
- проблема, признанная критичной по согласованию с Заказчиком;
- регрессия ранее исправной функции после планового обновления;
- уязвимость в контуре аутентификации (JWT, cookie, внутренний ключ) или в разграничении ролей планировщика, допускающая повышение привилегий.

Временные меры, если экстренный выпуск невозможен:

- рассылка уведомления о необходимости применить срочное исправление;
- отключение проблемной функции (например, загрузки файлов, смены статуса, панели администратора) без остановки остальных модулей;
- изоляция комплекса в отдельный сегмент сети, ограничение сетевого обмена;
- пересмотр регламентов доступа к приложению, API и СУБД;
- временная блокировка учетных записей служб и скомпрометированных пользователей;
- отзыв сессий (сброс секретов JWT / ротация ключей JWKS) и принудительный повторный вход.

1.2. Поиск уязвимостей

Анализ и поиск уязвимостей выполняются с каждым выпуском новой версии:

- статический анализ кода (Ruff, BasedPyright, Biome для клиентских приложений);
- экспертиза исходного кода;
- функциональное тестирование (pytest, сценарии ролевой модели планировщика);
- тестирование на проникновение;
- динамический анализ и фаззинг входных данных API.

Отделом аналитики ежемесячно проводится поиск в общедоступных источниках сведений об уязвимостях собственных компонентов и заимствованных библиотек (FastAPI, Joserfc, Valkey, MinIO, React и др.). При выпуске новых версий проводятся те же проверки, что и при разработке безопасного ПО.

Особый контроль уделяется инвариантам ролевой модели: невозможность назначить координатора вне роли *Менеджер проекта*; невозможность назначить ответственного за этап вне роли *Начальник отдела* и вне команды проекта;

невозможность назначить исполнителя задачи вне отдела ответственного и вне команды проекта; неизменность внешней видимости предпроектной задачи; запрет удаления продукта при существующих покупках.

2. СОВЕРШЕНСТВОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Продукт развивается: расширяется набор модулей платформы, уточняется ролевая модель, оптимизируется интерфейс. Доработки выполняются по календарному плану.

Клиенты могут направлять технические предложения на электронную почту info@techinnovations.ru. Предложение рассматривается; при признании эффективности оно включается в план разработки.

3. МЕНЕДЖМЕНТ ДОКУМЕНТАЦИИ И КОНФИГУРАЦИИ ПО

В область действия системы управления конфигурацией включаются:

- исходный код программы (репозитории `auth_service`, `planning_backend`, `planning_frontend`);
- требования и эксплуатационные документы;
- загрузочные модули, в том числе модули сторонних разработчиков;
- инструментальные средства и связанная с ними информация;
- информация об обновлениях и устранении уязвимостей;
- перечень выявленных уязвимостей.

Элементы конфигурации изменяются в процессе разработки. Система конфигурационного управления регистрирует историю изменений и поддерживает целостность версий. Набор элементов конфигурации полностью и однозначно определяет состояние продукта. Ответственность за полноту и актуальность информации лежит на руководителе отдела разработки. В согласованные моменты времени производится сборка готовой версии. После сборки проводится тестирование. Готовой поставке присваивается уникальный номер версии.

4. МЕНЕДЖМЕНТ ИНФРАСТРУКТУРЫ

Защите подлежат: дистрибутивы; исходный код; загрузочные модули; инструментальные средства; сведения об обновлениях и уязвимостях; требования и эксплуатационные документы.

Несанкционированный доступ, управление правами и защита веток обеспечиваются GitLab. Слияние функциональности в ветки master/dev запрещено для большинства разработчиков и выполняется руководителями проектов через Merge Request. При увольнении сотрудника учётная запись блокируется.

Рабочие станции находятся под защитой антивирусного ПО с актуальными базами. Серверные помещения имеют отдельный регламент доступа: вход фиксируется в журнале (время, Ф. И. О., причина, выполненные работы). Доступ в помещение отдела разработки ограничивается СКУД, физический контроль — системой видеонаблюдения.

Резервное копирование: инкрементальная копия репозитория Git — ежедневно; полная копия сервера Git — ежемесячно. Копия сетевого файлового хранилища — каждые 24 часа, ежемесячно — на изолированный внешний носитель. Git фиксирует уникальный идентификатор события, тип операции, комментарий, инициатора, дату и время, контрольную сумму, состав изменённых файлов.

5. МЕНЕДЖМЕНТ ЧЕЛОВЕЧЕСКИХ РЕСУРСОВ

Профессиональное обучение сотрудников и анализ существующей системы обучения проводится для поддержания и улучшения компетентности сотрудников разработчика ПО в области разработки безопасного ПО, формирования необходимой профессионально-квалификационной структуры работников, постоянного расширения и обновления знаний работников, непрерывного роста их профессионального мастерства.

При приеме на работу оценивается квалификация сотрудника. Все вновь принятые работники проходят инструктаж и информируются о правилах и условиях работы, а также об ответственности за действия, влияющие на снижение качества работ.

Все сотрудники проходят необходимое обучение и имеют квалификацию, позволяющую им работать самостоятельно.

Определение необходимости обучения, повышения квалификации и проверки знаний производится руководителями отделов, составляющих годовые планы. Результаты проверок знаний, квалификационных экзаменов и прохождения обучения регистрируются в специальном журнале.

Менеджер по персоналу на основании заявок руководителей отделов, с учетом проектов планов повышения квалификации в учебных центрах, разрабатывает годовые

планы подготовки и повышения квалификации служащих, специалистов и руководителей организации. Планы утверждаются исполнительным директором организации.

План обучения составляется в произвольной форме с обязательным включением следующих сведений: направление обучения; бюджет обучения; сведения об организации, проводящей обучение и стоимость ее услуг; сроки проведения обучения; сведения об обучаемых сотрудниках (Ф.И.О., должности); форма и время обучения с учетом рабочего времени персонала; места для отметок о проведении мероприятий и комментариев.

Профессиональное обучение сотрудников проводится в целях расширения и углубления технических знаний, совершенствования мастерства служащих, специалистов и руководителей.

Каждому сотруднику предоставляется возможность самостоятельно улучшать знания в рабочее время за счет чтения профильной литературы, изучения тематических сайтов Интернет, посещения специализированных интернет-форумов и т.д. Такая активность считается рабочей и подлежит 100% оплате в соответствии с оговоренными условиями работы.

Профессиональное обучение сотрудников компании-разработчика проводится в течение всей трудовой деятельности в связи с постоянной потребностью организации в квалифицированных кадрах.

- Используются следующие виды обучения руководителей, специалистов и служащих: самообразование;
- занятия, посвященные моделированию угроз безопасности информации, экспертизе исходного кода программы, безопасному тестированию ПО;
- курсы в учебных центрах или с привлечением специалистов других организаций (курсы английского языка) – получение знаний для возможности самообразования.

Длительность обучения на обучающих курсах составляет от нескольких дней до нескольких недель без отрыва от производства. Обучение ведется на основании договоров организации с учебными центрами.

Самостоятельное обучение сотрудников (самообразование) осуществляется по индивидуальному плану. Контроль над повышением уровня знаний и квалификации сотрудника осуществляется его непосредственным руководителем. Занятия могут проводиться с частичным отрывом от работы в выделенных для этого помещениях.

Программа обучения сотрудников анализируется каждые 6-12 месяцев руководителями отделов для установления ее пригодности, адекватности и результативности для достижения установленных целей в области разработки безопасного

ПО. Результаты анализа программы обучения и сведения о ее корректировке (при наличии) вносятся руководителями отделов в годовой отчет.

Для разработчиков, сопровождающих ролевую модель планировщика, обязательно изучение настоящего комплекта документов и внутренних регламентов на изменение справочников `organization_roles` и `project_roles` (справочники не редактируются из панели администратора прикладным персоналом Заказчика).

6. СОПРОВОЖДЕНИЕ ПО

Сопровождение ППО «СОКОЛ» осуществляется компанией-разработчиком программного обеспечения – ООО «Инновационные технологии».

Процесс сопровождения включает в себя:

- техническую поддержку пользователей;
- устранение неисправностей;
- помощь в конфигурации всех компонент программного обеспечения;
- консультирование по работе с ПО.

Вопросы и предложения по работе и доработке системы необходимо направлять по адресу info@techinnovations.ru или на персональную почту менеджера проекта, который выделяется на каждого Заказчика. Прием и обработка вопросов осуществляется по рабочим дням с 9:00 до 18:00 по Московскому времени».

7. ИНФОРМАЦИЯ О ПЕРСОНАЛЕ

ООО «Инновационные технологии» полностью укомплектовано необходимым персоналом для поддержки и администрирования поставляемого программного решения, для чего в компании предусмотрены следующие должности:

1. Руководитель отдела разработки программного обеспечения – 1 чел.;
2. Разработчик программного обеспечения – 2 чел.
3. Архитектор – 1 чел.;
4. Системный аналитик – 1 чел.
5. Тестировщик программного обеспечения – 1 чел.
6. Руководитель проектов – 1 чел.

Таким образом, специалисты ООО «Иновационные технологии» обладают необходимым набором знаний для работы со всеми компонентами, входящими в состав ПО, при решении прикладных задач, соответствующих функционалу программного обеспечения.