GIS ГАЗИНФОРМ СЕРВИС

SafeERP

Информационная безопасность 1С: как предотвратить утечки данных и атаки на корпоративную систему

Санкт-Петербург. 2025 г.

www.gaz-is.ru

УТЕЧКИ В ERP СИСТЕМАХ

SafeERP

51 % утечки конфиденциальной информации

44 % нарушение основной деятельности

24 % больше новых уязвимостей

67 % избегают публичных высказываний

2025

www.tadviser.ru

ЯНВАРЬ	ФЕВРАЛЬ	МАРТ	АПРЕЛЬ	МАЙ	ИЮНЬ	ИЮЛЬ	АВГУСТ	СЕНТЯБРЬ
Ритейл	Девелопмент	IT	IT	IT	Банки	Ритейл	Туризм	ТЭК

Отрасли

УЯЗВИМОСТИ ERP

SafeERP

- данные клиентов
- инженерная информация
- номера банковских счетов
- персональные данные сотрудников
- интеллектуальная собственность
- проведение финансовых транзакций

ПРОБЛЕМАТИКА

SafeERP

Платформа

Код

Приложения

DevSecOps + compliance

- Дороговизна
- Отсутствие экспертности
- Человеческий фактор
- Долгий временной цикл
- Экспорт данных

ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

- Указ Президента РФ: №166 (технологический суверенитет)
- ФЗ: №149, 152, 187 (ЗИ, ИСПДн, КИИ)
- Стандарт ГОСТ: Р 57580.1-2017
- Приказы: ФСТЭК №17, 21, 31, 239 (ГИС, ЗИ, ИСПДн, КИИ):

  ИАФ: Идентификация и аутентификация субъектов доступа и объектов доступа
  УПД: Управление доступом субъектов доступа к объектам доступа
  РСБ: сбор, запись и хранение информации о событиях безопасности в части событий назначений политик доступа
  АУД: аудит безопасности
  АНЗ: контроль правил генерации и смены паролей

- ГОСТ. Защита информации. Разработка безопасного программного обеспечения.

КОМПЛЕКСНЫЙ МОНИТОРИНГ И ИНСТРУМЕНТЫ БЕЗОПАСНОЙ РАЗРАБОТКИ

SafeERP

EXTENSION MODULE CODE / PLATFORM

Комплексная защита 1С

- Поиск уязвимостей 1С-кода;
- Контроль настроек 1С.

1

EXTENSION MODULE +

Инструменты безопасной разработки

- Статический анализ кода SAST: SQLScript, XS, XML, JS, Python, C#, XSJS, XAML, Java;
- Анализ безопасности приложений методом DAST;
- Сканер сети и эксплуатация уязвимостей методом пентеста;
- SCA.

2

КЕЙСЫ EXTENSION MODULE

Контроль настроек 1С: неограниченный доступ к режиму технического специалиста

АНОМАЛИИ

- данные о поставках;
- настройки маршрутов;
- изменения в заказах.

расследование

мошенник

ИСПОЛЬЗОВАНИЕ

Учетная запись сотрудника техподдержки

АКТИВАЦИЯ

Режим технического специалиста

Роль: администратор системы

- модификация бизнес-логики систем;
- внедрение скриптов для перехвата информации;
- создание скрытых баз данных для дальнейшего шантажа.

ПОТЕНЦИАЛЬНЫЕ ПОСЛЕДСТВИЯ:

- **финансовые потери** из-за манипуляций с отчетностью и хищений;
- **крупная утечка данных**, угрожающая репутации и соблюдению регуляторных требований;
- **остановка операционной деятельности** из-за повреждения конфигурации 1С.

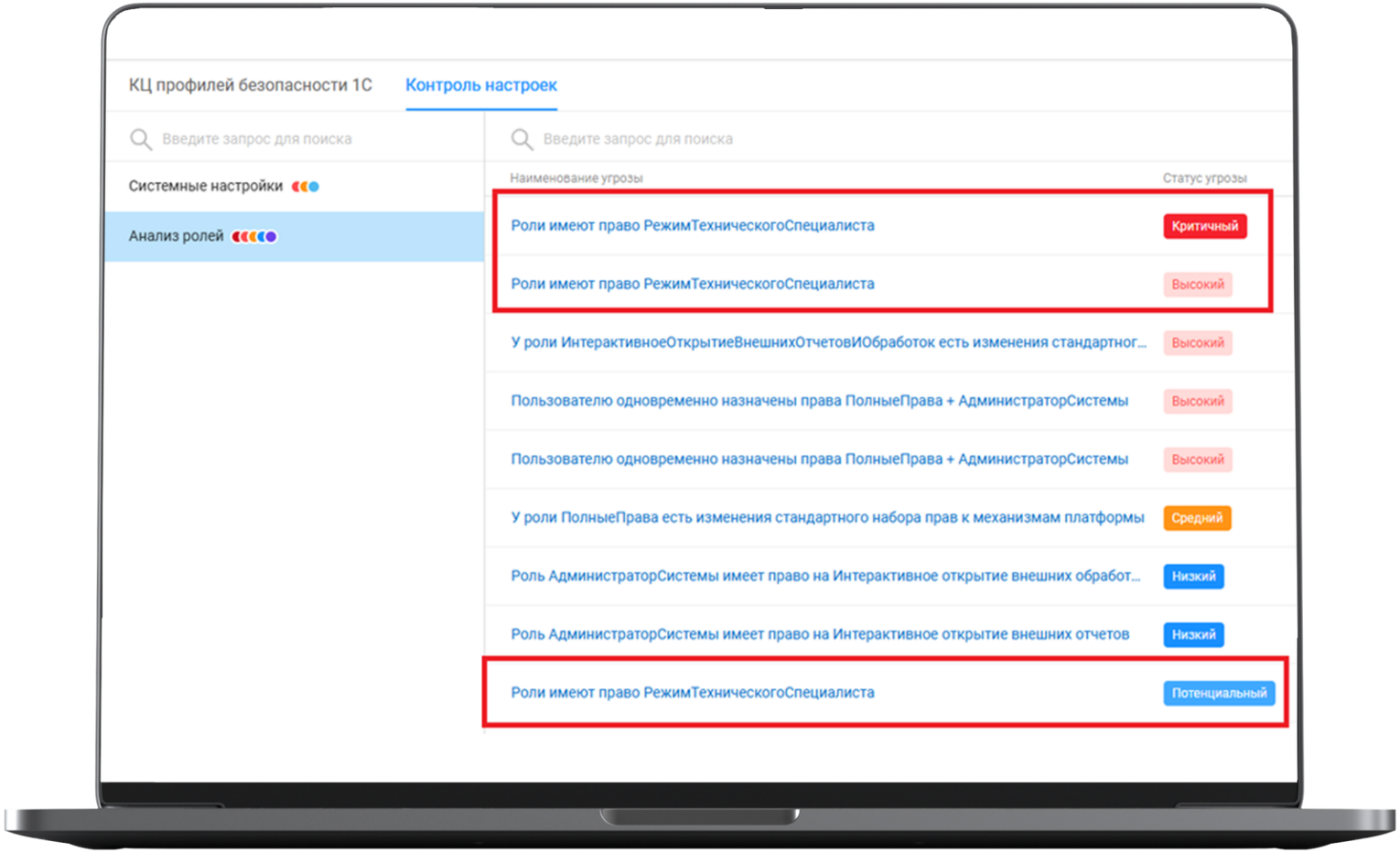
КЕЙСЫ EXTENSION MODULE

Контроль настроек 1С: неограниченный доступ к режиму технического специалиста

Применение SafeERP

Меры:

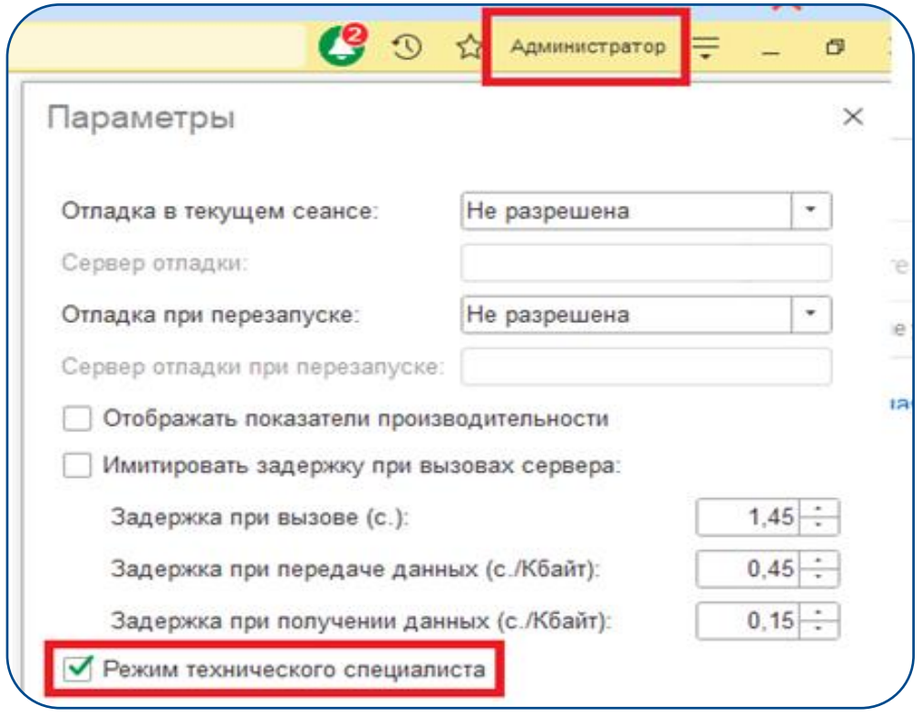
- перераспределение привилегий: отдельная роль с временным доступом, актив через запрос;
- исключение из стандартных ролей: право удалено из ролей; «Администратор системы»;
- регулярный контроль: выполнение регулярных проверок через SafeERP для выявления несоответствия.



КЕЙСЫ EXTENSION MODULE

Контроль настроек 1С: неограниченный доступ к режиму технического специалиста

Применение SafeERP



ИТОГИ:

- **устранение уязвимости** в кратчайшие сроки: доступ к критическим функциям ограничен, активность злоумышленника заблокирована;
- **снижение рисков** несанкционированного вмешательства в конфигурацию 1С;
- **сохранение репутации:** утечка данных предотвращена, клиенты не пострадали.

КЕЙСЫ EXTENSION MODULE

SafeERP

Возможность открытия внешних отчетов и обработок из режима конфигуратора 1С

ПОТЕНЦИАЛЬНЫЕ ПОСЛЕДСТВИЯ:

Массовое заражение рабочих станций вирусами-шифровальщиками, простой бизнеса, утечка персональных данных клиентов, включая платежные реквизиты, финансовые манипуляции.

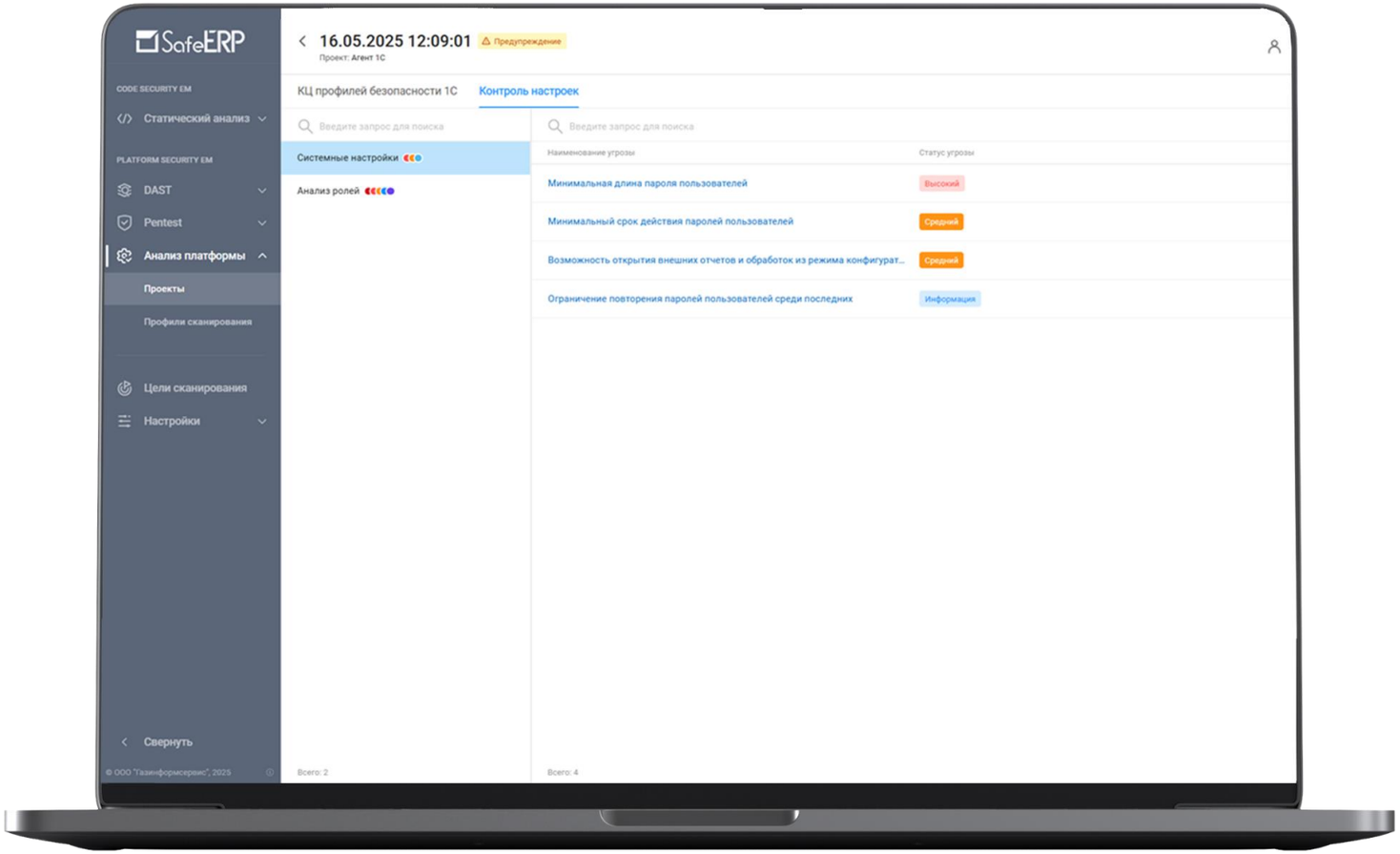
КЕЙСЫ EXTENSION MODULE

Возможность открытия внешних отчетов и обработок из режима конфигуратора 1С

Применение SafeERP

Меры:

- Блокировка опасных настроек: отключена возможность запуска внешних файлов;
- Централизированное управление отчетами: через защищенный корпоративный портал после проверки ИБ;
- Обучение сотрудников: тренинги по кибергигиене;
- Автоматизация контроля: SafeERP настроен на ежедневную проверку параметров безопасности.



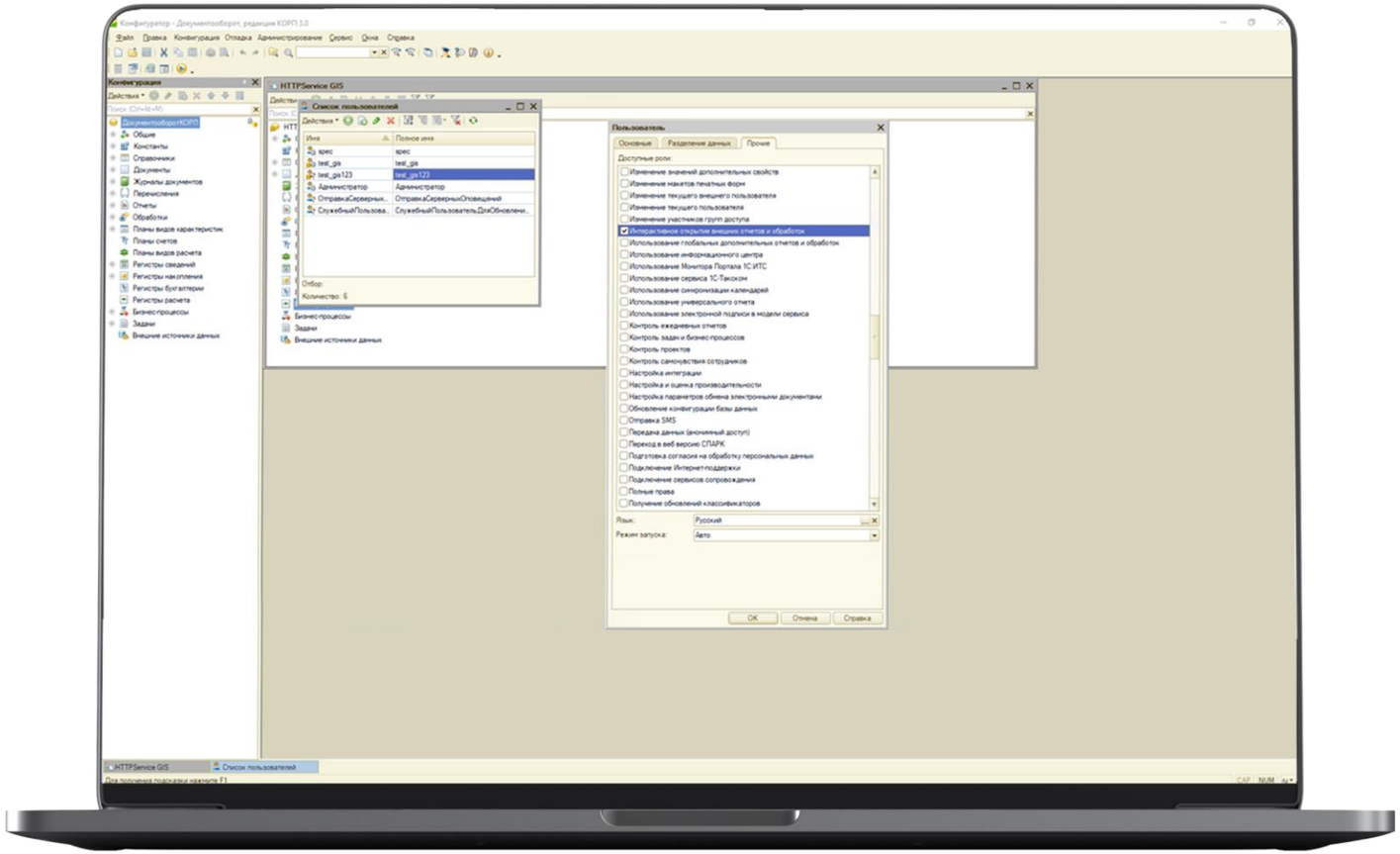
КЕЙСЫ EXTENSION MODULE

Возможность открытия внешних отчетов и обработок из режима конфигуратора 1С

Применение SafeERP

Итоги:

- **угроза нейтрализована**: запуск внешних файлов из конфигуратора заблокирован, инцидент с вредоносным кодом устранен;
- **повышение уровня защиты**: данные клиентов и финансовая отчетность изолированы от несанкционированного доступа;
- **проактивная защита**: регулярные проверки SafeERP PS EM исключают повторение сценария.



КЕЙСЫ EXTENSION MODULE

SafeERP

Контроль целостности профилей безопасности 1С

Обновление 1С

АНОМАЛИИ

- изменение в накладных;
- самопроизвольные перезагрузки сервера 1С;
- попытки подключения к внешним ip-адресам из системы.

расследование

АКТИВИРОВАНЫ НАСТРОЙКИ:

- полный доступ к файловой системе сервера;
- доступ к COM-объектам и внешним компонентам;
- профиль безопасности инфобазы 1С и внешних компонентов;
- доступ к привилегированному режиму и функциям криптографии.

мошенник

вредоносный код

УЯЗВИМОСТЬ:

- подмена реквизитов поставщиков в платежных документах;
- сбор данных о запасах сырья для передачи конкурентам;
- блокировка выполнения критических задач с требованием выкупа.

ПОТЕНЦИАЛЬНЫЕ ПОСЛЕДСТВИЯ:

Полная остановка производства, утечка коммерческой тайны, финансовые манипуляции, нарушение compliance: несоответствие требованиям ФСТЭК, ГОСТ Р и отраслевым стандартам

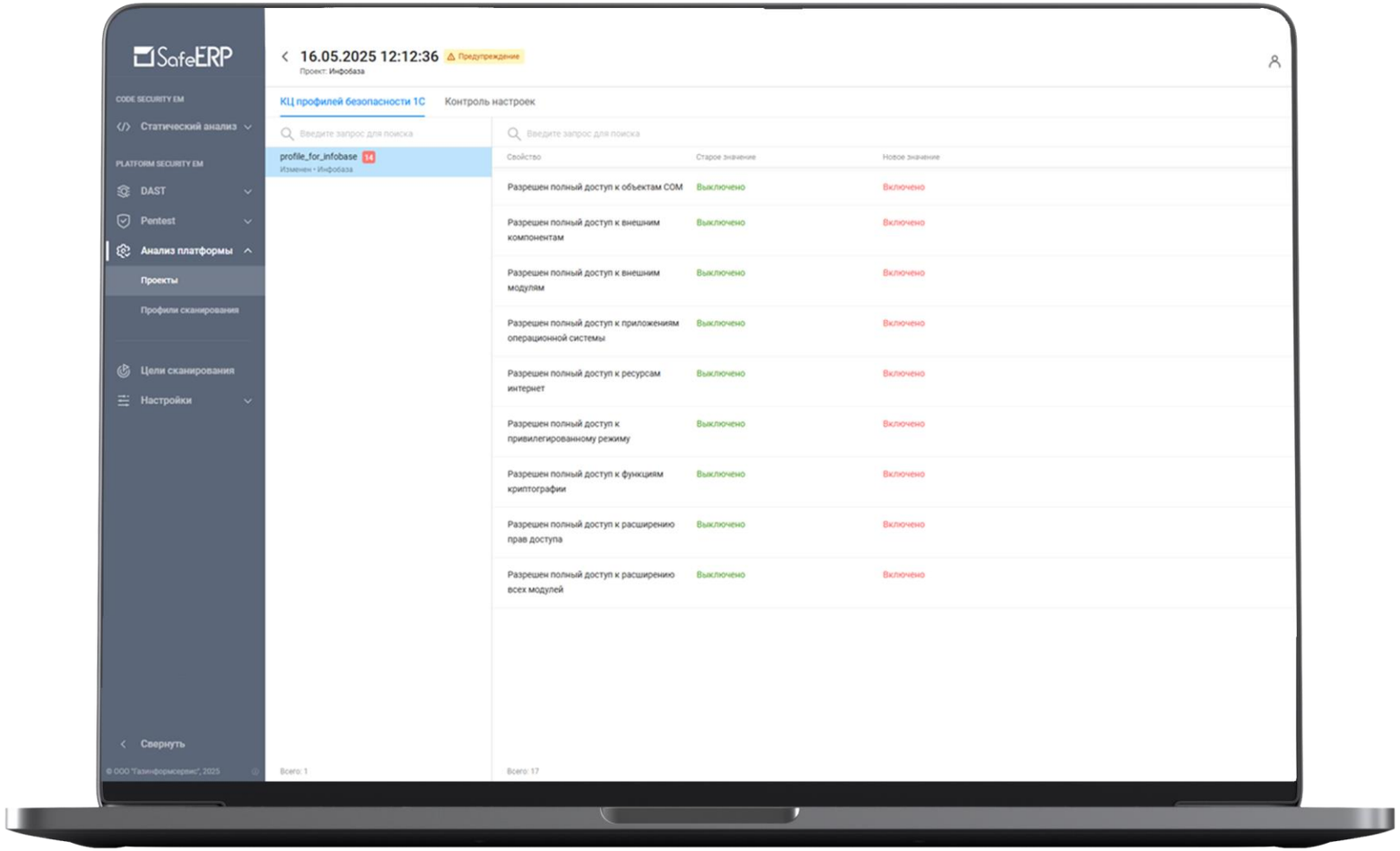
КЕЙСЫ EXTENSION MODULE

Контроль целостности профилей безопасности 1С

Применение SafeERP

Меры:

- экстренный откат настроек: все опасные параметры переведены в положение «выключено»;
- сегментация прав: отдельные профили для разработчиков, администраторов и пользователей;
- аудит конфигураций: все обновления 1С теперь проходят проверку через SafeERP.



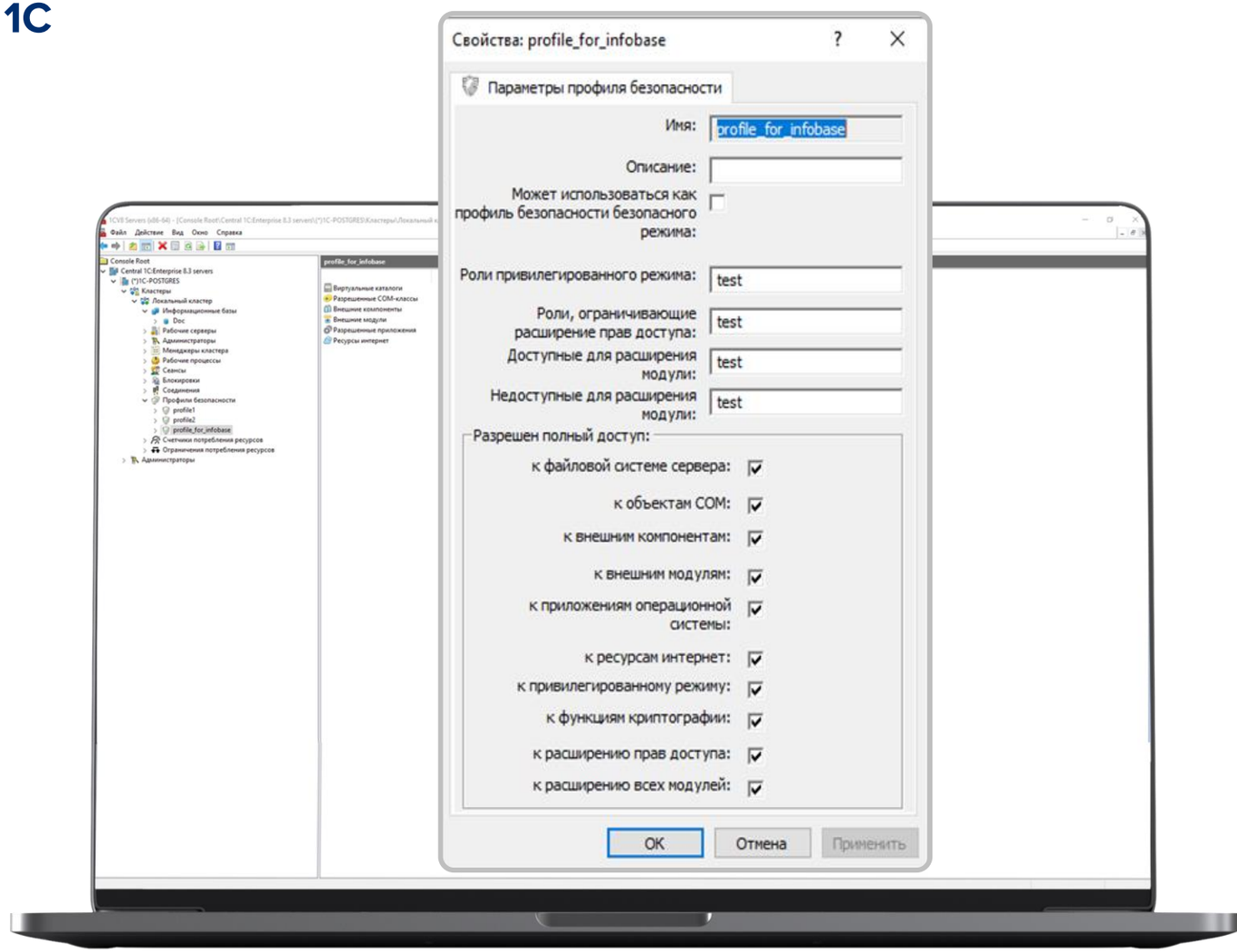
КЕЙСЫ EXTENSION MODULE

Контроль целостности профилей безопасности 1С

Применение SafeERP

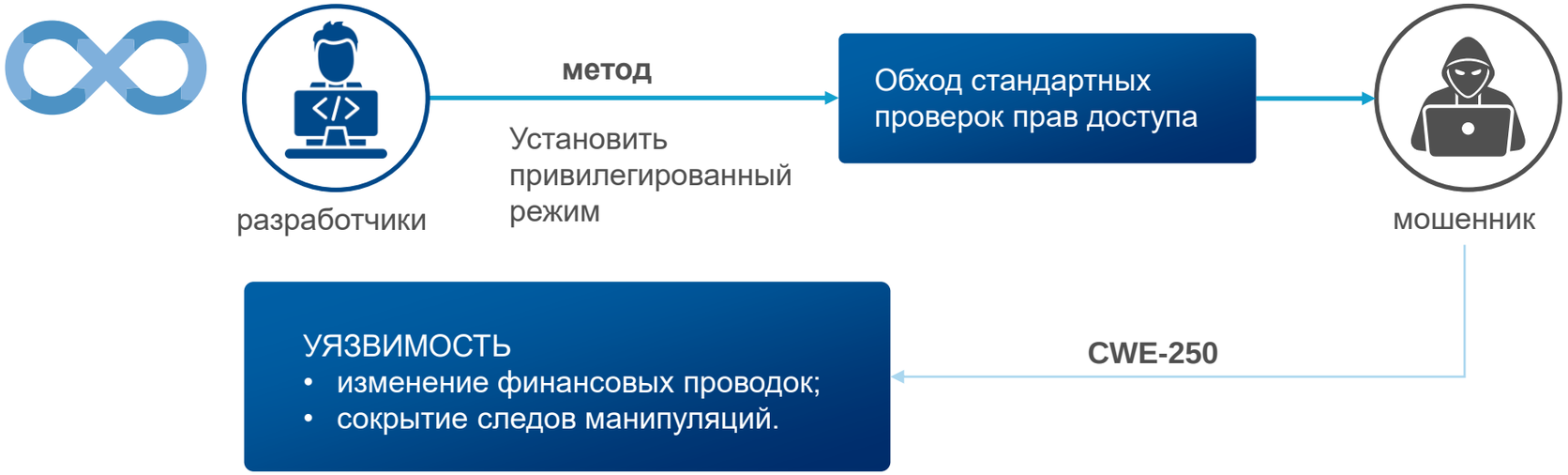
Итоги:

- **угроза устранена за сутки**: вредоносный код удален, настройки безопасности восстановлены;
- **снижены риски:** исключен доступ к критическим ресурсам ОС и внешним компонентам;
- **проактивная защита**: регулярные проверки SafeERP PS EM исключают повторение сценария.



КЕЙСЫ EXTENSION MODULE

Привилегированный режим 1С



Пример небезопасного кода:

```
&НаСервере
Функция ПроверитьСпособДоставки(Рассылка, Знач
ПараметрыДоставки)

    УстановитьПривилегированныйРежим(Истина);
```

ВОЗМОЖНЫЕ УГРОЗЫ:

- эскалация привилегий;
- обход системы авторизации;
- выполнение бизнес-логики от имени пользователя в привилегированном режиме.

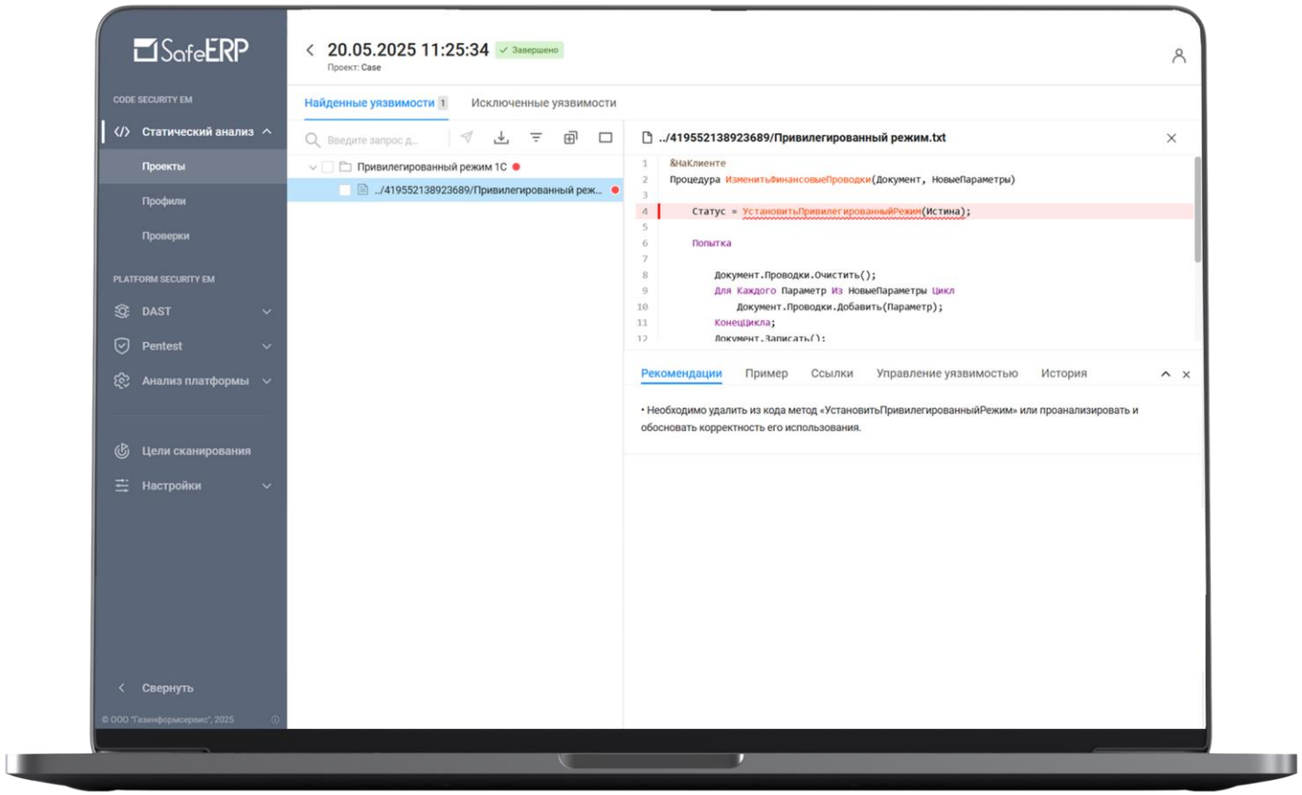
КЕЙСЫ EXTENSION MODULE

Привилегированный режим 1С

Применение SafeERP

Итоги проекта:

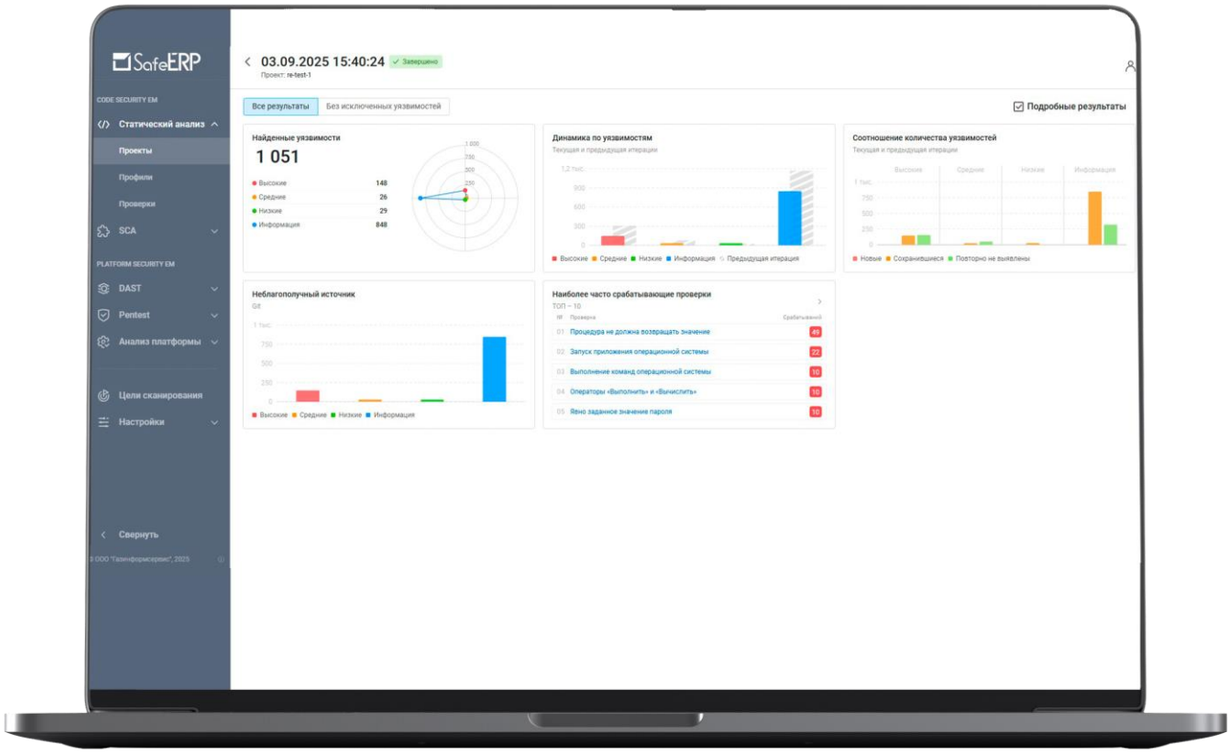
- статический анализатор кода позволяет выявить в программном коде системы «1С:Предприятие» использование метода УстановитьПривилегированныйРежим();
- в системах разработки разработчик может самостоятельно проверять написанный код.



ЗАДАЧИ, КОТОРЫЕ РЕШАЕТ EXTENSION MODULE

SAST 1С и контроль настроек 1С

- Позволяет выявить уязвимости и недекларированные возможности в коде 1С
- Максимальное количество выявленных уязвимостей за счет анализа исходного кода
- Выявление потенциально небезопасных настроек профилей безопасности 1С
- Обнаружение потенциально небезопасных настроек 1С конфигураций
- Возможность отделения расширений и внешних обработок
- Возможность инкрементального сканирования
- Выявление уязвимостей на ранних этапах разработки
- Возможность создания собственных сценариев проверки кода
- Генерация отчета, содержащего полную информацию



EXTENSION MODULE

SafeERP

Функциональные возможности

PLATFORM SECURITY EM

- Контроль целостности (КЦ) профилей безопасности 1С (регистрация изменений в БД)
- Контроль настроек (КН) 1С (анализ ролей, настройки конфигурации, системные настройки)
- Более 70 проверок на контроль платформы 1С, с возможностью создавать собственные

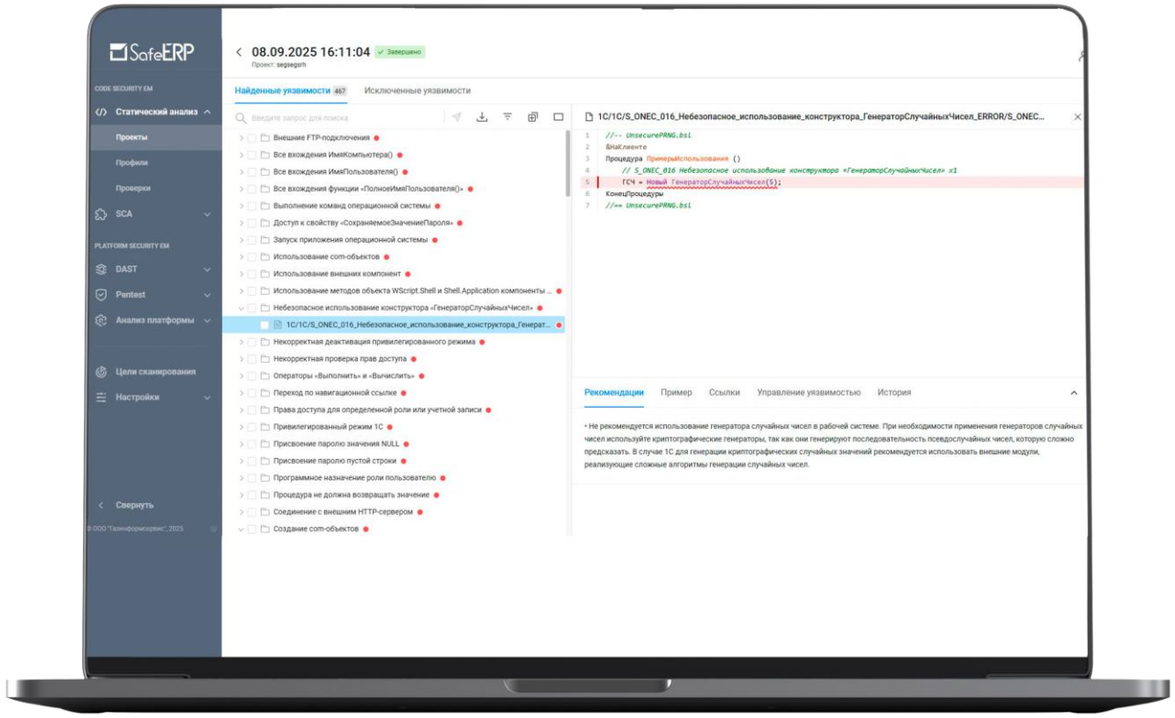
CODE SECURITY EM

- Автоматическая выгрузка кода из БД 1С, конфигурации 1С, хранилища 1С и GIT
- Выявление небезопасного кода 1С во внешних обработках и расширениях в режиме автоматического отделения от основной конфигурации
- Оперативная информация об изменении части программного кода 1С
- Более 50 проверок на анализ кода 1С, с возможностью создавать собственные
- Плагин для среды разработки 1С:EDT

ДОПОЛНИТЕЛЬНЫЕ

- Параметры критичности уязвимости
- Рекомендации по устранению найденных уязвимостей
- Анализ и контроль защищенности в режиме промышленной эксплуатации или по заданному расписанию, отчеты, дашборды, уведомления и сравнительный анализ итераций проверок
- Управление найденными уязвимостями

ИНТЕРФЕЙС EXTENSION MODULE

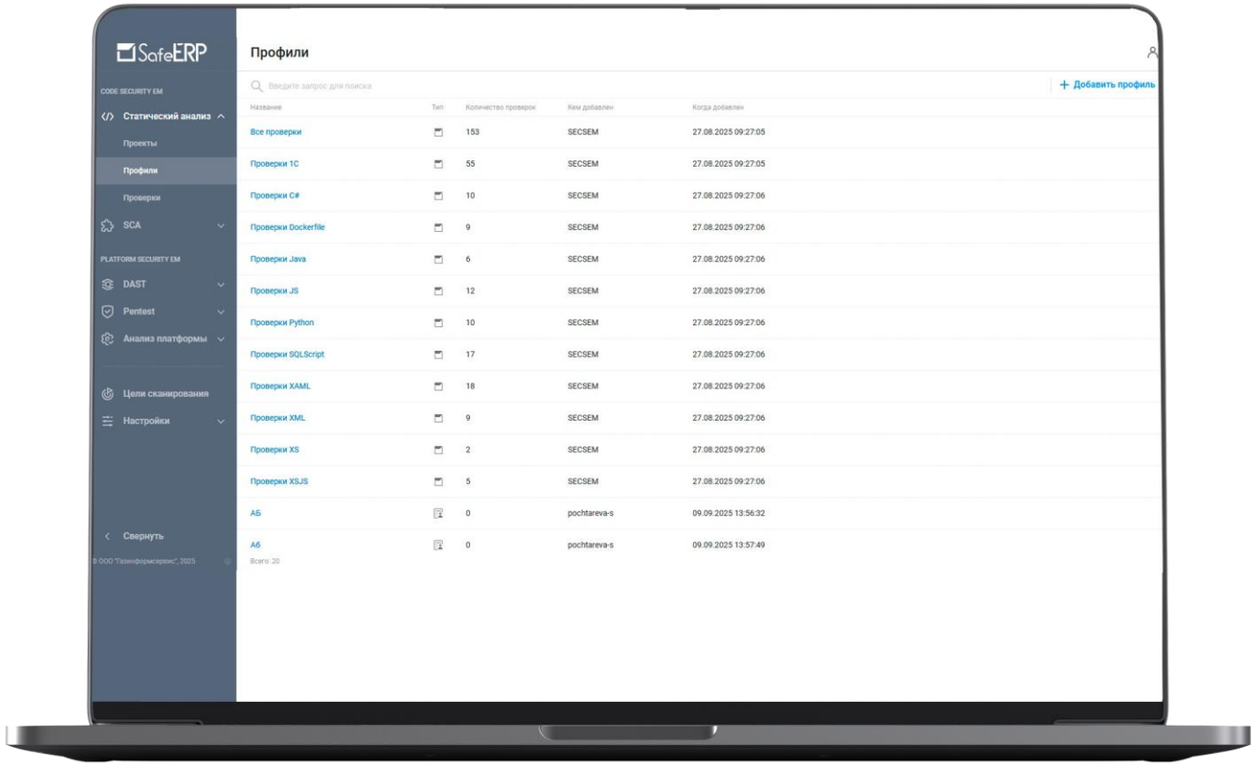


- Перечень потенциально небезопасных конструкций кода
- Рекомендации по исправлению, ссылки на полезные ресурсы
- Запуск по расписанию, уведомления на почту
- Дашборды по проектам анализа кода: сравнительный анализ итерации проверок
- Детальные отчеты по уязвимостям выявление изменений профилей безопасности 1С по более 70 сценариям проверок;
- Выявление небезопасных настроек в кластере 1С – отслеживание изменения критически важных настроек;
- Возможность создания пользовательских сценариев проверок настроек 1С.
- Конструктор профилей сценариев проверок кода 1С
- Управление найденными уязвимостями
- Кастомный отчет
- Создание собственных проверок анализа кода 1С
- Гибкая настройка источников: GIT (CI/CD), БД 1С, Хранилище 1С, Конфигурация 1С
- Сканирование zip-архивов с файлами, содержащими исходный код, поддерживаемых языков, в т.ч. с внешними обработками (*.epf) и файлов с внешними отчетами (*.erf).
- Гибкая ролевая политика

ЗАДАЧИ, КОТОРЫЕ РЕШАЕТ EXTENSION MODULE+

SAST, DAST и пентест

- Позволяет выявить уязвимости и недекларированные возможности в коде приложений, разрабатываемых на языках программирования: SQLScript, XS, XML, JS, Python, C#, XSJS, XAML, Java
- Позволяет выявить уязвимости непосредственно при выполнении программы
- Имитирует вредоносные внешние атаки, использующие распространенные уязвимости для компрометации приложения
- Проверка доступности целевых хостов и открытых портов для компрометации сервисов с применением подготовленных пентестов
- Использование при отсутствии исходного кода и без привязки к языкам программирования
- Возможность встраивания анализатора в pipepline (CI/CD GIT)
- Возможность создания собственных сценариев проверки кода
- Генерация отчета, содержащего полную информацию



EXTENSION MODULE+

SafeERP

Функциональные возможности

PLATFORM SECURITY EM

- Сканирование любых веб-приложений методом динамического анализа
- Анализ защищенности информационных систем и приложений методом пентест с применением эксплойтов
- Собственная БДУ
- Эксплойты для различных приложений и SAP

CODE SECURITY EM

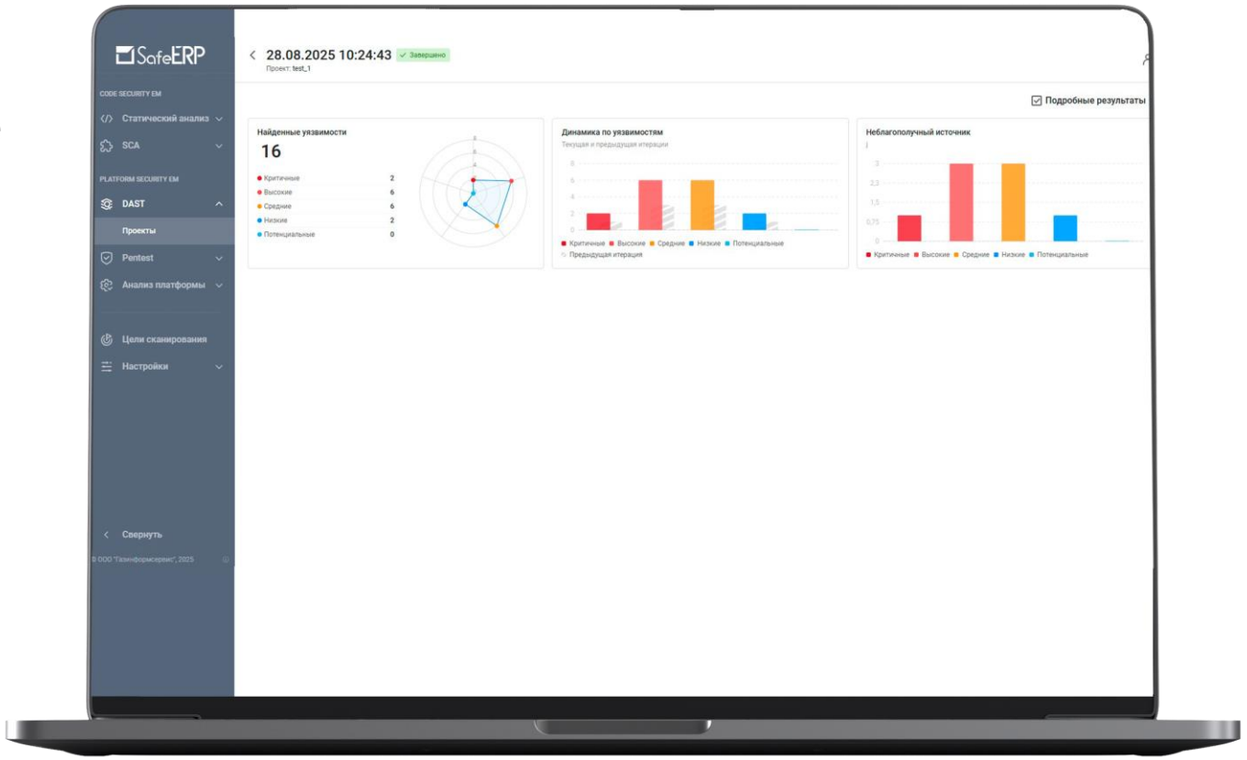
- Перечень потенциально небезопасных конструкций кода различных языков программирования: SQLScript, XS, XML, JS, Python, C#, XSJS, XAML, Java
- Автоматическая выгрузка кода из GIT.
- Сканирование архивов
- CI/CD GIT
- Возможность анализа только редактируемого кода
- Более 200 проверок на анализ кода различных языков программирования, с возможностью создавать собственные

ДОПОЛНИТЕЛЬНЫЕ

- Параметры критичности уязвимости
- Рекомендации по устранению найденных уязвимостей
- Интеграции с поддерживаемым ПО
- Анализ и контроль защищенности в режиме промышленной эксплуатации или по заданному расписанию, отчеты, дашборды, уведомления и сравнительный анализ итераций проверок
- Управление найденными уязвимостями

ИНТЕРФЕЙС EM +

- Генерация отчетов о выявленных уязвимостях с рекомендациями по их устранению
- Дашборды
- DAST: выявление ссылок на целевом хосте; − формирование структуры веб-приложения; − выполнение поиска веб-директорий методом «фаззинга»; − выявление http cookies, не соответствующих критериям безопасности
- предоставление возможности просмотра найденных уязвимостей по категориям в отдельном окне
- Pentest: выявление уязвимостей и эксплойтов ПО;
- Проведение тестов на проникновение;
- Перечень потенциально небезопасных конструкций кода
- Рекомендации по исправлению, ссылки на полезные ресурсы
- Запуск по расписанию, уведомления на почту
- Гибкая ролевая политика
- CI/CD GIT
- Кастомные сценарии проверок кода



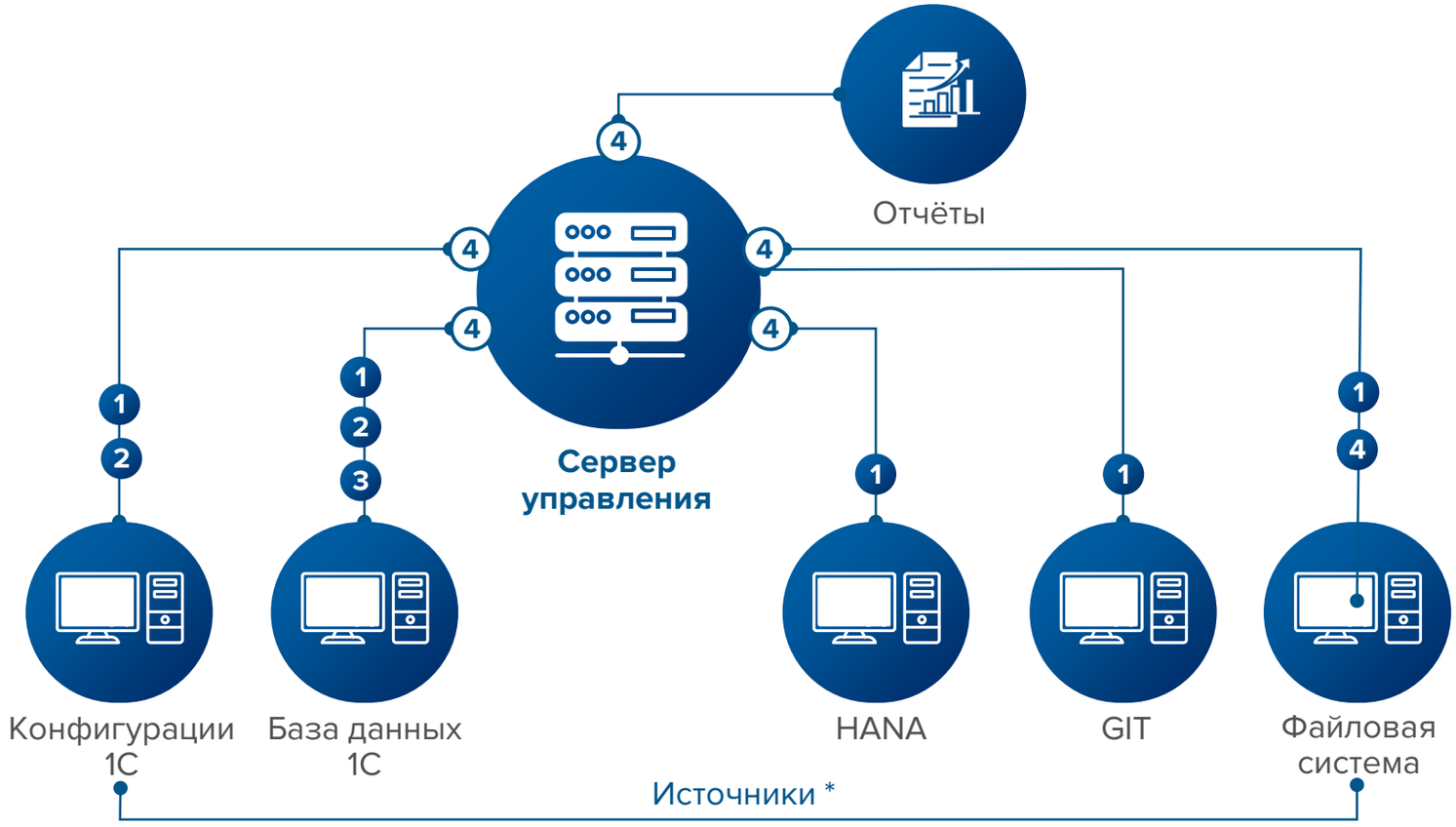
CODE SECURITY EXTENSION MODULE

SafeERP

Архитектура

- Сервер управления
- Источники
  - База данных 1С
  - Конфигурация 1С
  - GIT
  - SAP HANA
  - Файловая система

* Количество источников рассчитывается исходя из опросного листа



1. Анализ кода
2. Анализ изменённого кода
3. Анализ расширений и внешних обработок
4. Автоматизация процесса

ИСТОЧНИКИ (ПОДКЛЮЧЕНИЕ КЛИЕНТОВ) В CODE SECURITY EXTENSION MODULE

SafeERP

01	База данных 1С	1С Database	При подключении к базе данных 1С может анализироваться исходный код, в том числе с возможностью отделения расширений и внешних обработок, сравнения текущего uuid (уникальных идентификаторов) конфигурации с ранее сохраненными (сравнение и проверка измененного кода) и проверкой программных модулей, доступных для изменений (проверка доступного для изменения кода).	Прямое подключение к базе данных 1С. При подключении источника типа 1С Database необходимо использовать конструкцию «драйвер:СУБД», т.е. «jdbc:postgresql» (или иной СУБД)
02	Конфигурация 1С	1С Designer	Выгрузка кода происходит напрямую из конфигурации 1С с возможностью отделения расширений 1С от основной конфигурации.	Подключение к конфигуратору 1С через клиент 1cv8 (не входит в состав SafeERP CS EM). Версия клиента должна совпадать с версией на подключаемой конфигурации 1С. Функционал получения кода напрямую с конфигурации 1С работает начиная с версии платформы 1С 8.3.
03	GIT	Git	Выгрузка кода происходит из проектов GIT для проверки 1С и других языков программирования (SQLScript, XS, XML, JS, Python, C#, XSJS, XAML, Java) и возможностью встроиться в CI/CD.	Подключение происходит по протоколу http (через логин и пароль) или ssh (по ключу).
04	Архив	Файлы	Возможна проверка zip-архивов с файлами, содержащими исходный код, поддерживаемых языков, в т.ч. с внешними обработками (*.epf) и файлов с внешними отчетами (*.erf).	Методом ручной загрузки. Встроен в сервер управления CS EM (подключение источника не требуется).

АРХИТЕКТУРА PLATFORM SECURITY EM

- Анализ безопасности кластера 1С: статус «выкл» небезопасные настройки

- Контроль настроек 1С по более 50 сценариям проверок

DAST веб-приложений:

- БДУ ГИС
- url сканер, поиск доменов/поддоменов, фаззинг, анализ SSL сертификата, поиск http cookies, sql injection, поиск XSS уязвимостей;

- 13 эксплойтов для ИС и приложений и 18 эксплойтов для SAP
    - Brute-Force
    - Apache Tomcat
    - PostgreSQL

УНИКАЛЬНЫЕ ПРЕИМУЩЕСТВА CODE SECURITY EXTENSION MODULE

SafeERP

- Извлечение кода из кластера 1С для проверки напрямую из интерфейса анализатора
- Анализ расширений и внешних обработок 1С
- Возможность создания собственных проверок анализа
- Возможность выбрать конкретные объекты 1С для анализа кода
- Возможность анализа только редактируемого кода
- Доработки под требования
- Скорость и качество проверки (сценарии на ИБ и качество кода)

Аналоги

positive technologies

Ростелеком

sonarqube

ПОКАЗАТЕЛИ CODE SECURITY EXTENSION MODULE

SafeERP

- Автоматизация выявления уязвимостей в процессе разработки
- Оптимизация процесса обработки событий ИБ
- Снижение трудозатрат на мониторинг и обработку событий ИБ
- Снижение затрат на устранение уязвимостей, найденных на ранних этапах разработки ПО
- Сокращение сроков и расходов на внедрение ПО

УНИКАЛЬНЫЕ ПРЕИМУЩЕСТВА PLATFORM SECURITY EM

SafeERP

- Анализ безопасности и контроль настроек 1С
- Более 50 сценариев на контроль настроек 1С
- Мониторинг состояния безопасности настроек 1С в режиме одного окна
- Поиск известных эксплойтов для найденных уязвимостей
- Собственная БДУ GIS: обновление каждый день

Аналоги

positive technologies

WIRESHARK

NMAP

ПОКАЗАТЕЛИ PLATFORM SECURITY EM

- Автоматизация процесса получения информации о состоянии защищенности веб-приложений и смежных систем с точки зрения внешнего нарушителя
- Оптимизация процессов обработки полученной информации
- Снижение трудозатрат на мониторинг и проведение аудита защищенности информационных систем
- Сокращение сроков и расходов на проведение тестирования на проникновение веб-приложений

SafeERP

GIS ГАЗИНФОРМ СЕРВИС

Следующие шаги:

Демонстрация продукта

Пилотное внедрение

Договор на поставку

GIS ГАЗИНФОРМ СЕРВИС

Спасибо за внимание!

+7 (812) 677-20-53
safeerp.gaz-is.ru
sales@gaz-is.ru

Кулешова Римма
менеджер продукта