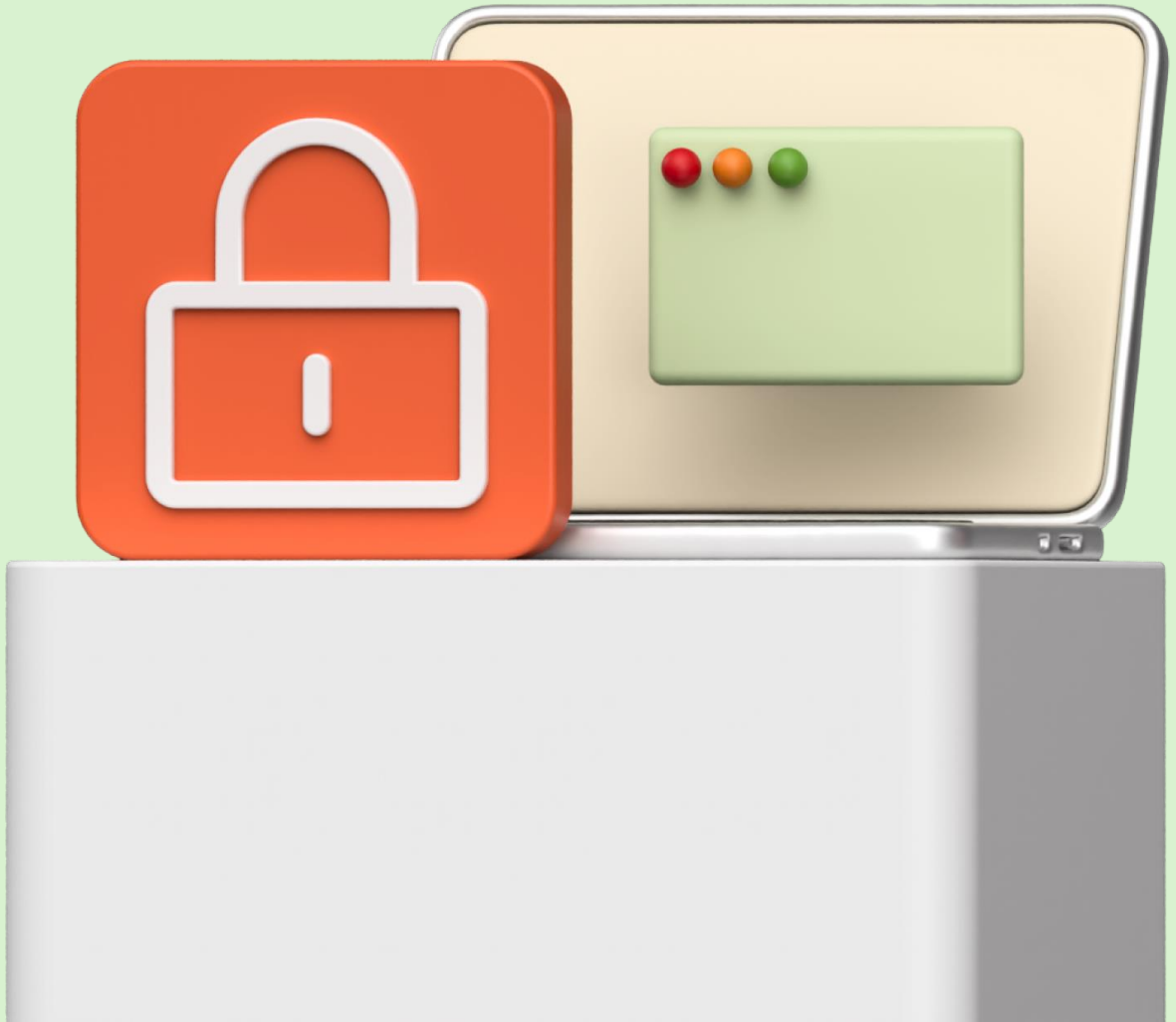
ЦВД × Directum

Решение ЦВД

«Информационная безопасность» для Directum RX

Централизованное управление ИБ
в единой экосистеме: от инцидентов
до обучения персонала



Почему ЦВД

Генеральный партнер

Центр сертифицированного обучения

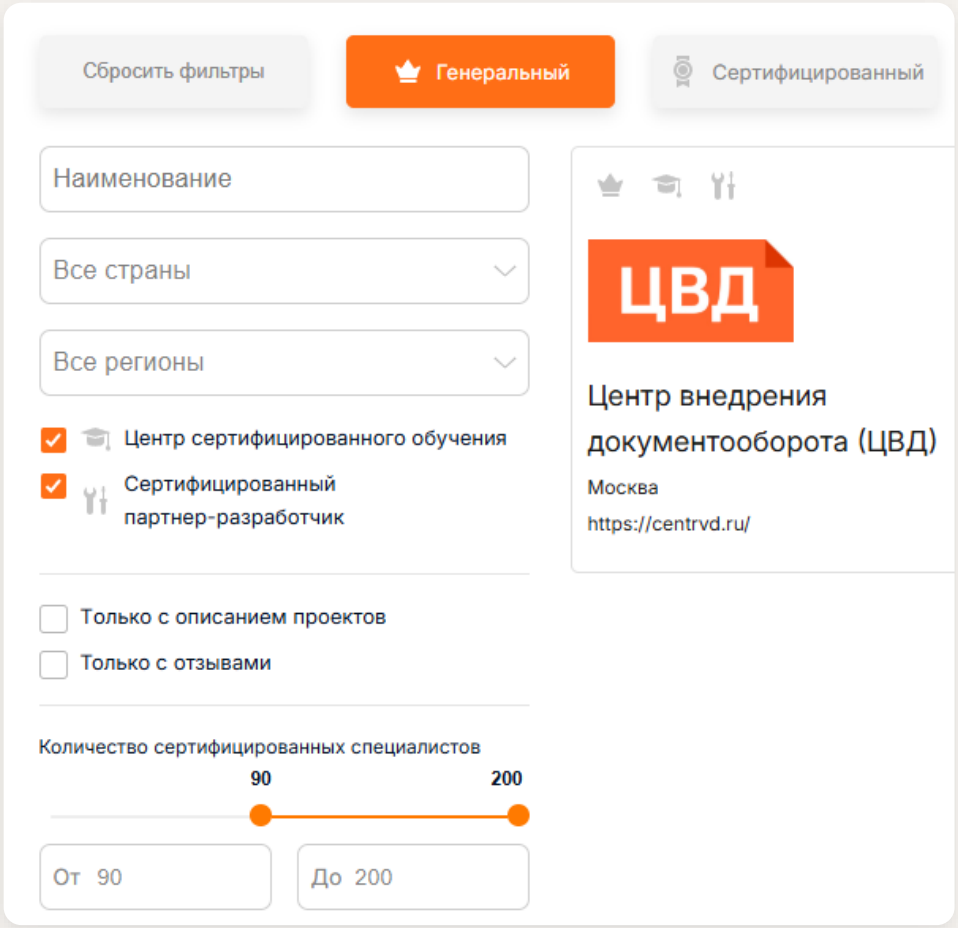
Сертифицированный партнер-разработчик DIRECTUM

Масштаб на рынке: Самая крупная команда среди партнеров Directum — **более 90 профессионалов**

Динамика развития: За 4 последние года закрыли контракты на **1,2 млрд руб.**

Глубокая экспертиза с 2008 года: Генеральный партнер, разработчик и учебный центр Directum «все в одном»

Специализация: Сложная разработка



Карточка «ЦВД» на сайте Directum

Более 170 клиентов

ЦВД

От хаоса к порядку — ключевые проблемы ручного управления ИБ

ЦВД

Разрозненные процессы

Инциденты, уязвимости, нарушения фиксируются в разных системах — сложно увидеть полную картину

Ручной труд

Специалисты тратят часы на регистрацию событий и сопоставление данных из SIEM, Wazuh, Gophish

Нет прослеживаемости

Непонятно, кто, когда и какие меры принял — отсутствует единая история

Сложность с регуляторами

Подготовка отчетов для ФСТЭК, 152-ФЗ и 187-ФЗ требует ручного сбора данных днями

Два модуля для разных категорий пользователей

ЦВД

Модуль «Информационная безопасность» — для специалистов

Управление инцидентами, уязвимостями, СЗИ, проверками, обучением, отчетами

Модуль «Запросы ИБ» — для всех сотрудников

Создание и отслеживание заявок на мероприятия, обучение, проверки

Централизованная среда для специалистов и руководителей ИБ

ЦВД

Управление безопасностью и планирование

Проверки, аудиты, мероприятия

Инциденты и уязвимости

Реестр, расследование, связь с нарушениями

Управление активами

Информационные системы, реестр СЗИ

Нормативные документы

Реестр ОРД, регламенты и стандарты

Обучение и осведомленность

Курсы, фишинговые кампании

Отчетность и аналитика

Прозрачность процессов ИБ

Полный цикл обработки инцидентов и управления уязвимостями

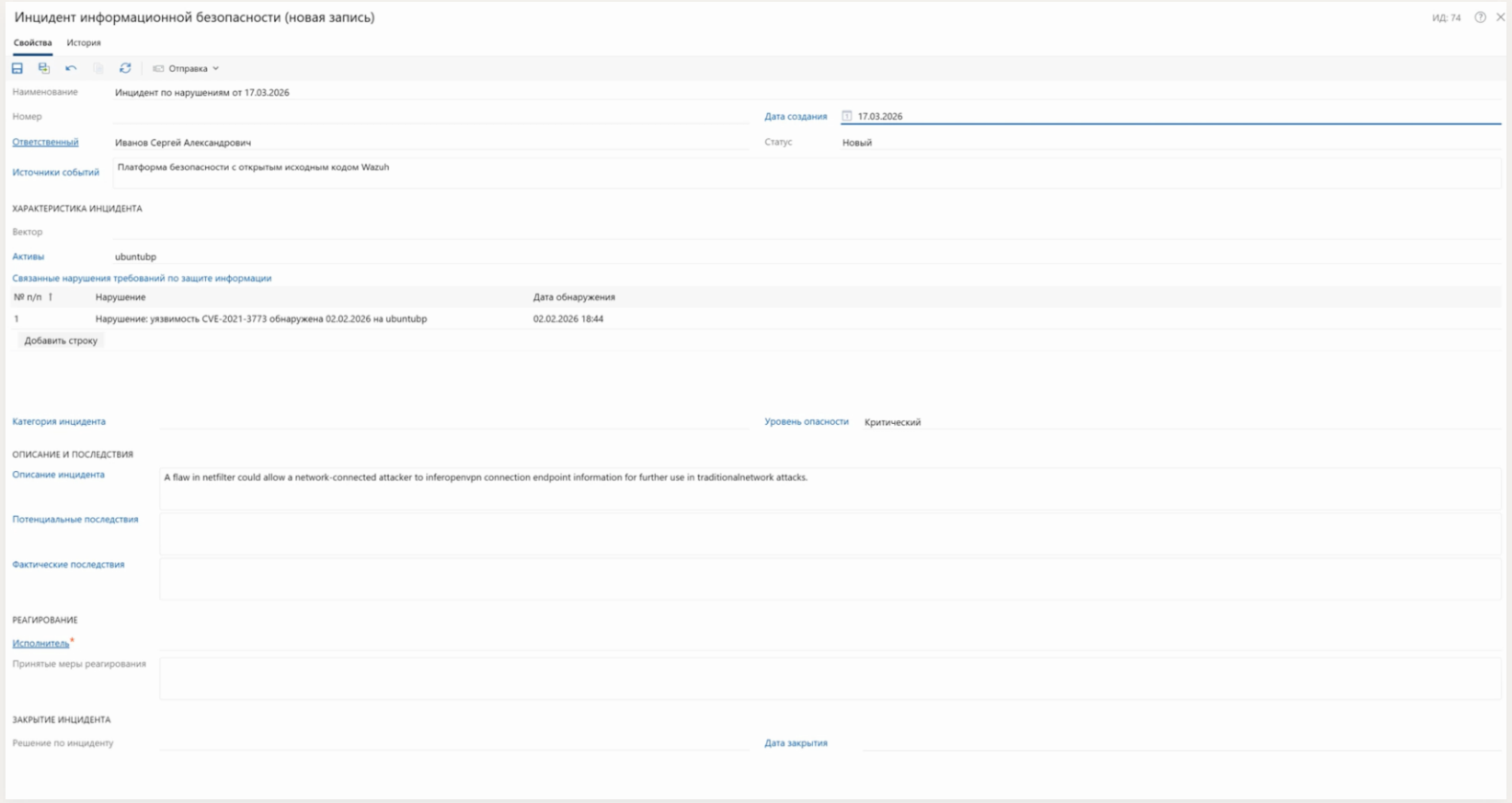
Регистрация инцидентов: (вручную или автоматически из SIEM/Wazuh)

Расследование: статусы, ответственные, сроки, описание последствий

Закрытие: итоговое заключение, решение по инциденту, связь с нарушениями

Уязвимости: реестр с CVE, CVSS, критичностью, интеграция с БДУ ФСТЭК

Связь: инциденты → нарушения → уязвимости → мероприятия по устранению



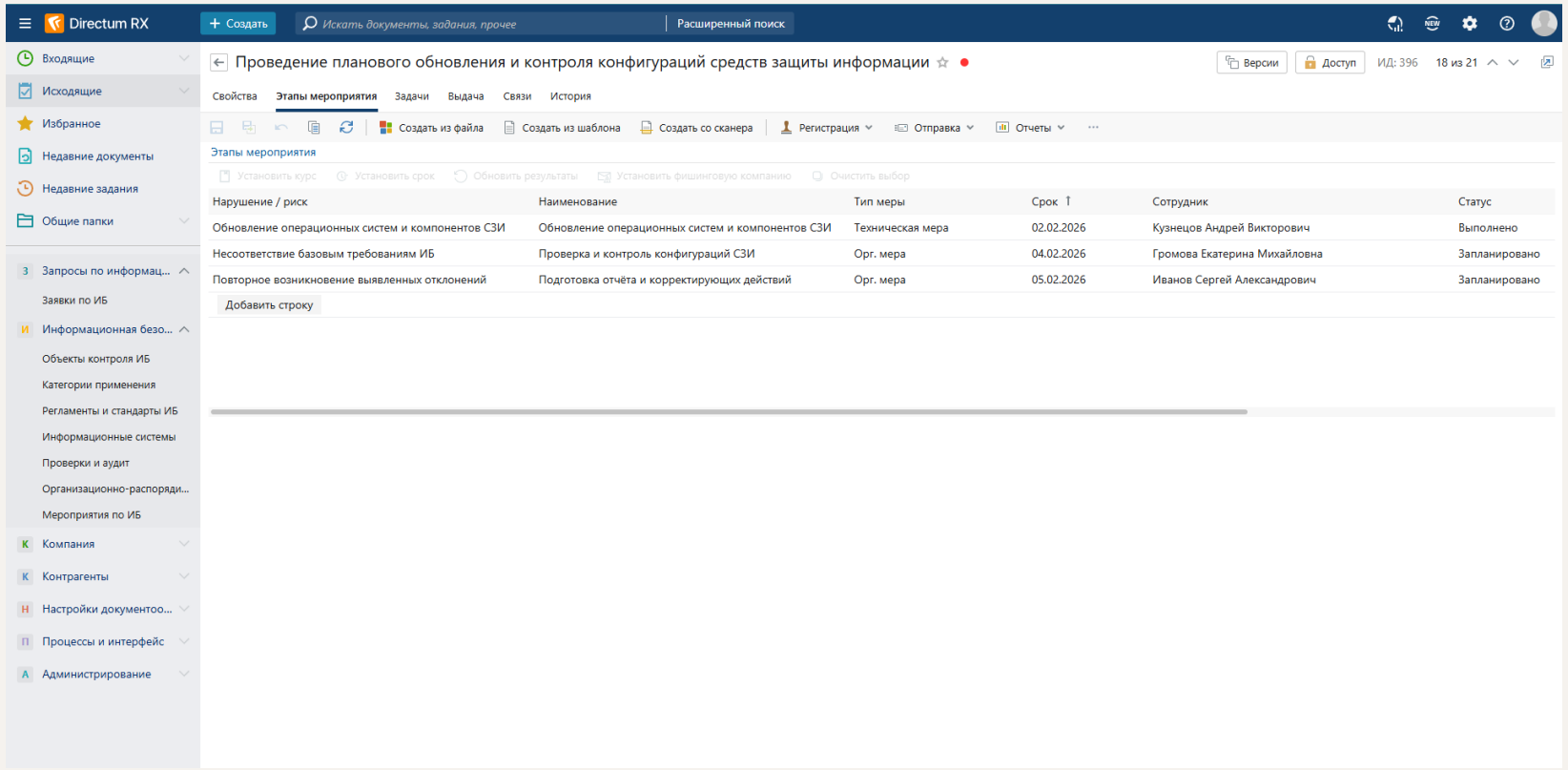
Планирование и контроль безопасности

Проверки и аудит: внутренние, внешние, целевые, внеплановые. Чек-листы, нормативная база, фиксация нарушений

Мероприятия по ИБ: плановые, внеплановые, корректирующие. Назначение ответственных, статусы, сроки

Акты: автоматическое формирование актов по результатам проверок и мероприятий

Связь: мероприятия привязаны к нарушениям, инцидентам, регламентам



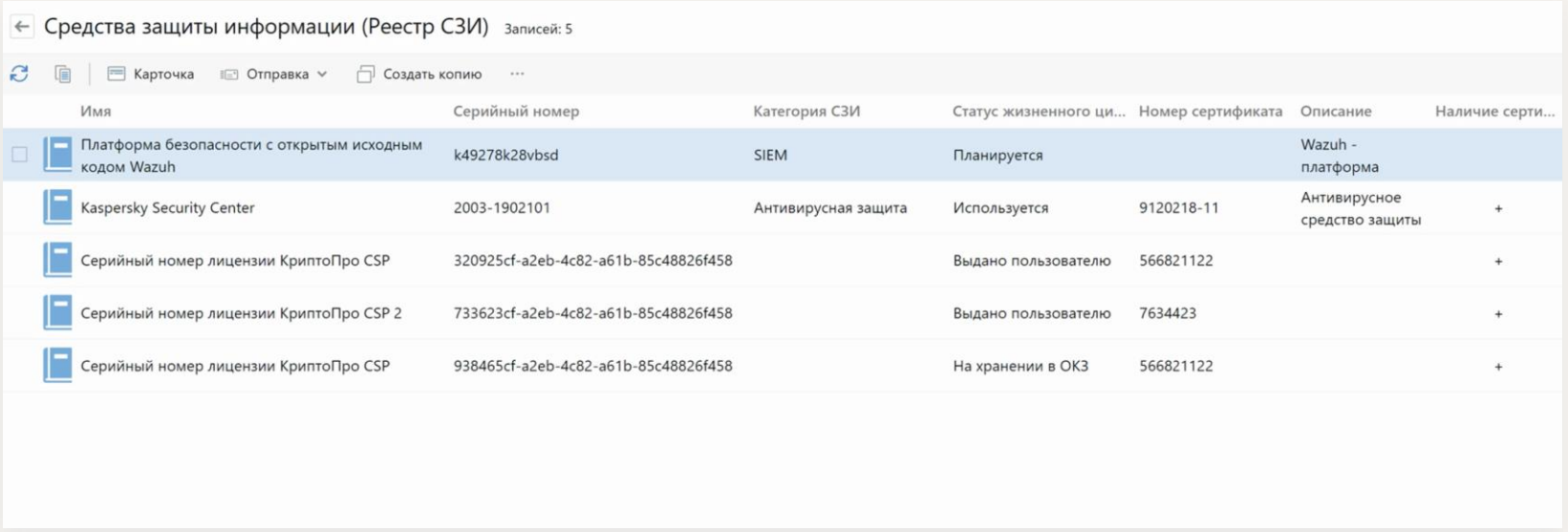
Полный реестр информационных систем и средств защиты

Информационные системы: владельцы, критичность, архитектура, среда эксплуатации, обработка ПДн

Реестр СЗИ: все средства защиты, их характеристики, статус жизненного цикла, сертификаты

Контроль сертификатов: отслеживание сроков действия, автоматическое напоминание

Операции с СЗИ: выдача, установка, изъятие, уничтожение — с формированием актов



Имя	Серийный номер	Категория СЗИ	Статус жизненного ци...	Номер сертификата	Описание	Наличие серти...
Платформа безопасности с открытым исходным кодом Wazuh	k49278k28vbsd	SIEM	Планируется		Wazuh - платформа	
Kaspersky Security Center	2003-1902101	Антивирусная защита	Используется	9120218-11	Антивирусное средство защиты	+
Серийный номер лицензии КриптоПро CSP	320925cf-a2eb-4c82-a61b-85c48826f458		Выдано пользователю	566821122		+
Серийный номер лицензии КриптоПро CSP 2	733623cf-a2eb-4c82-a61b-85c48826f458		Выдано пользователю	7634423		+
Серийный номер лицензии КриптоПро CSP	938465cf-a2eb-4c82-a61b-85c48826f458		На хранении в ОКЗ	566821122		+

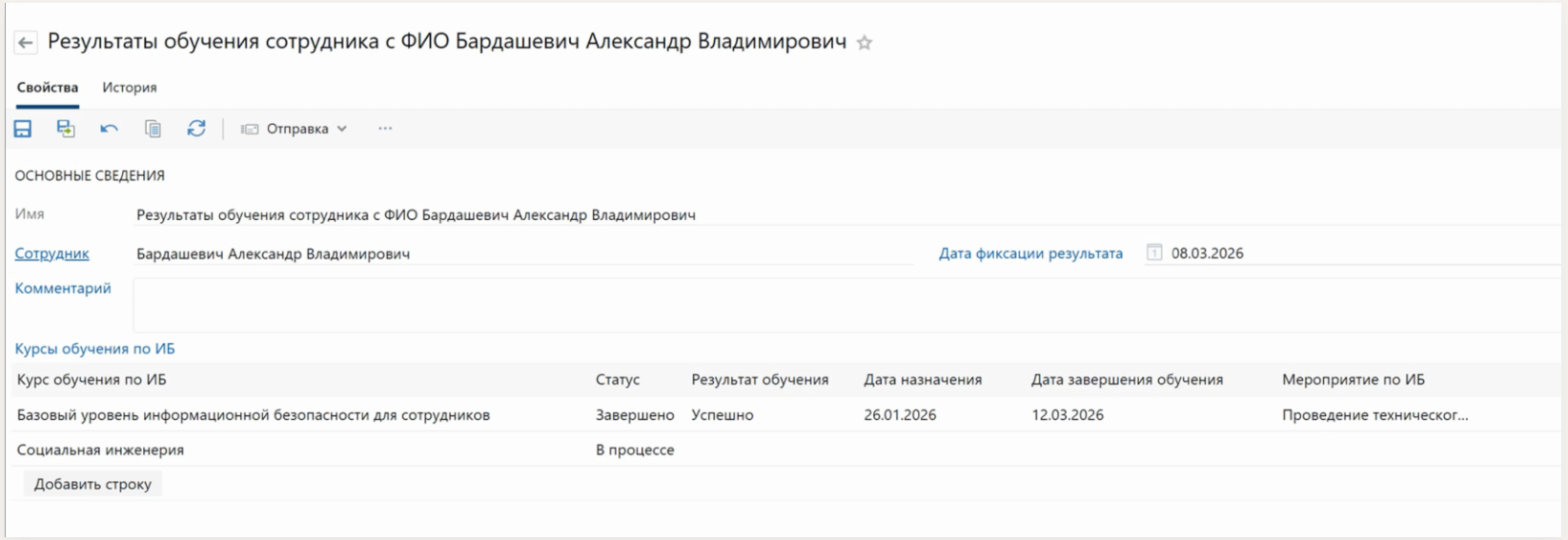
Управление обучением персонала и фишинговые симуляции

Курсы и обучение: справочник курсов, назначение сотрудникам, контроль прохождения (интеграция с WikiDS)

Фишинговые кампании: автоматический импорт кампаний из Gophish, отслеживание действий пользователей (открыл, перешел, ввел данные, сообщил)

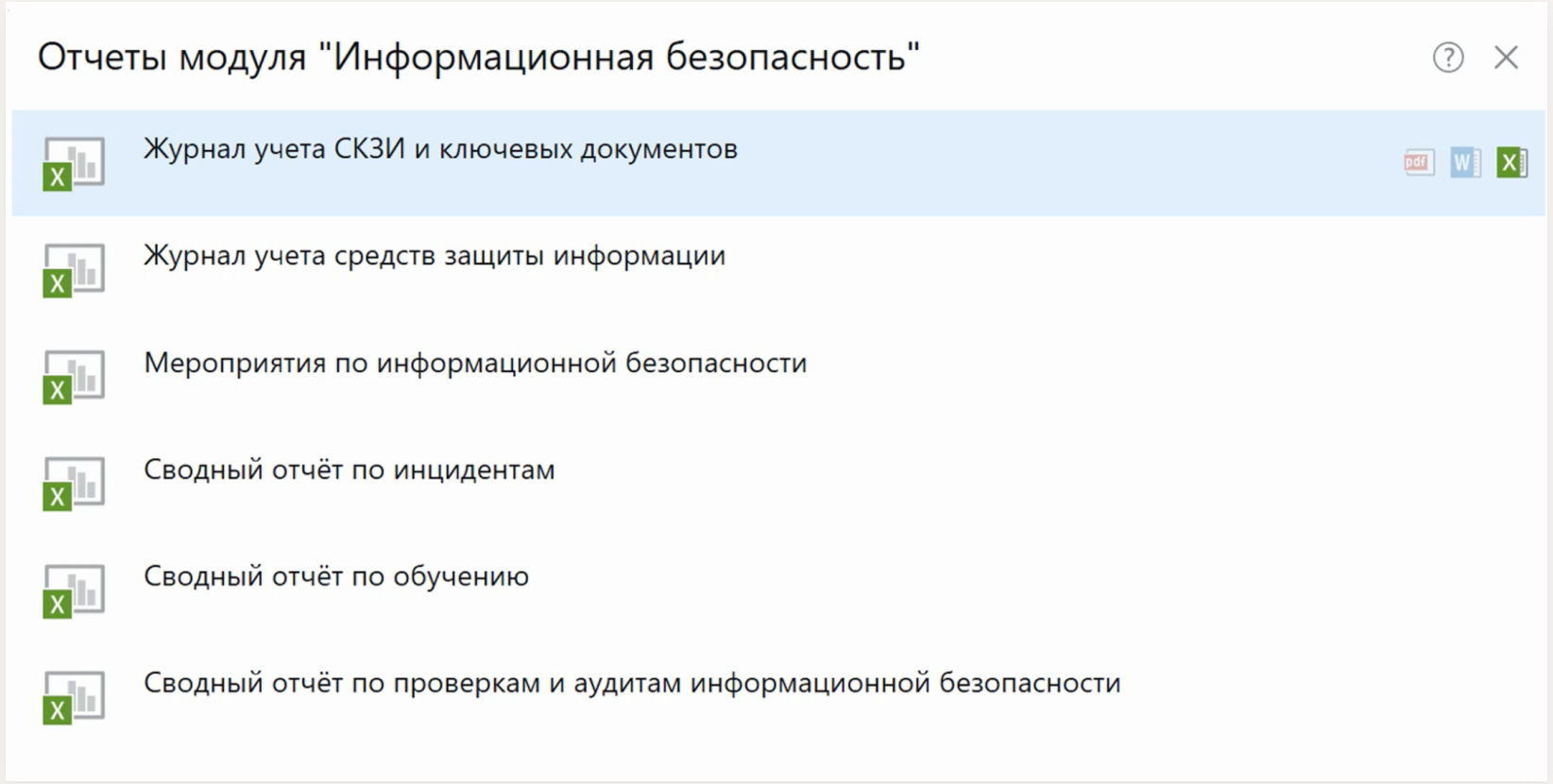
Результаты обучения: единый реестр статусов и результатов, связь с мероприятиями по ИБ

Отчетность: сводные отчеты по обучению и результатам сотрудников для регуляторов



Готовые шаблоны отчетов

- Сводный отчет по инцидентам
- Сводный отчет по проверкам и аудитам
- Журнал учета СКЗИ и ключевых документов
- Журнал учета средств защиты информации
- Отчет по обучению и осведомленности

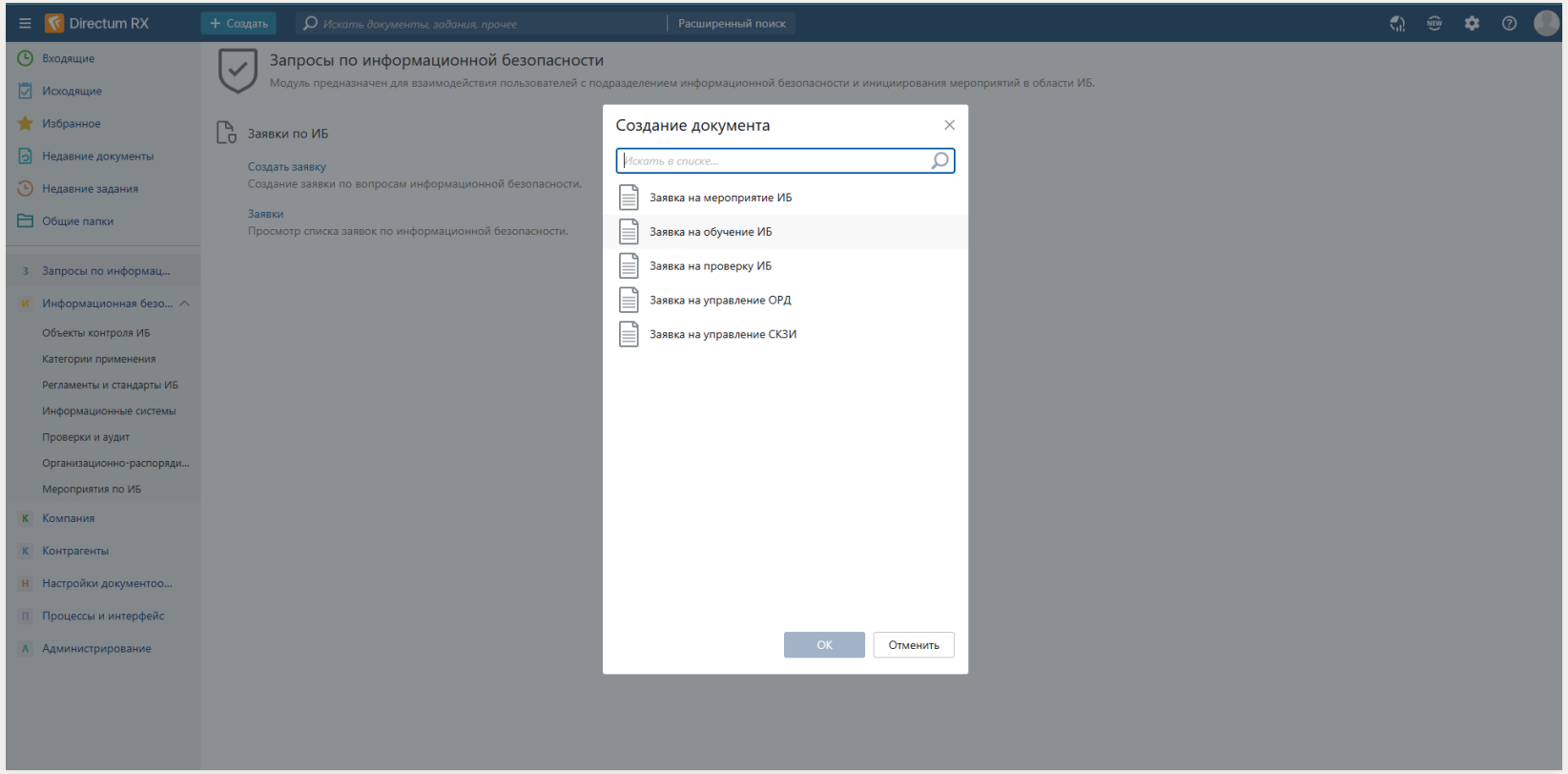


Простое взаимодействие со службой безопасности

Создание заявок на:

- Мероприятие по ИБ
- Обучение по ИБ
- Проверку ИБ
- Управление ОРД
- Управление СКЗИ

Просмотр статуса заявок в едином списке



Автоматическое наполнение данными из внешних источников

ЦВД

SIEM

LLM платформы

Инструменты симуляции фишинговых атак

Почему это решение — правильный выбор

ЦВД

Глубокая интеграция с экосистемой Directum RX

Единая среда для документооборота и безопасности

Автоматизация рутины

Интеграции с Wazuh, WikiDS, Gophish

Полная прослеживаемость

От события до закрытия, от инцидента до отчета

Готовность к регуляторам

Встроенные шаблоны отчетов

Гибкая настройка без программистов

Справочники настраиваются через интерфейс

Кому подходит решение

ЦВД

Специалистов и руководителей ИБ — для эффективного управления

ИТ-директоров — для единой системы управления рисками

Всех сотрудников — через модуль «Запросы ИБ»

Компаний любых отраслей, работающих с регуляторами (ПДн, КИИ, ФСТЭК)

ЦВД

Свяжитесь с нами, чтобы обсудить внедрение и получить демо-доступ

- Сокращение трудозатрат ИБ-отдела на 40–60% за счет автоматизации
- Полная прослеживаемость каждого инцидента и нарушения
- Готовность к регуляторным проверкам в любой момент
- Повышение осведомленности персонала через автоматизированное обучение

centrvd.ru
cvd@centrvd.ru