КИТ-Журнал

Выполнение требований регуляторов по защите информации и учету СКЗИ без бумаги и временных затрат

ООО «КИТ-Дистрибуция»

3 вакансии
2 специалиста

ПДн, ГИС, КИИ,
БФО, СКЗИ...

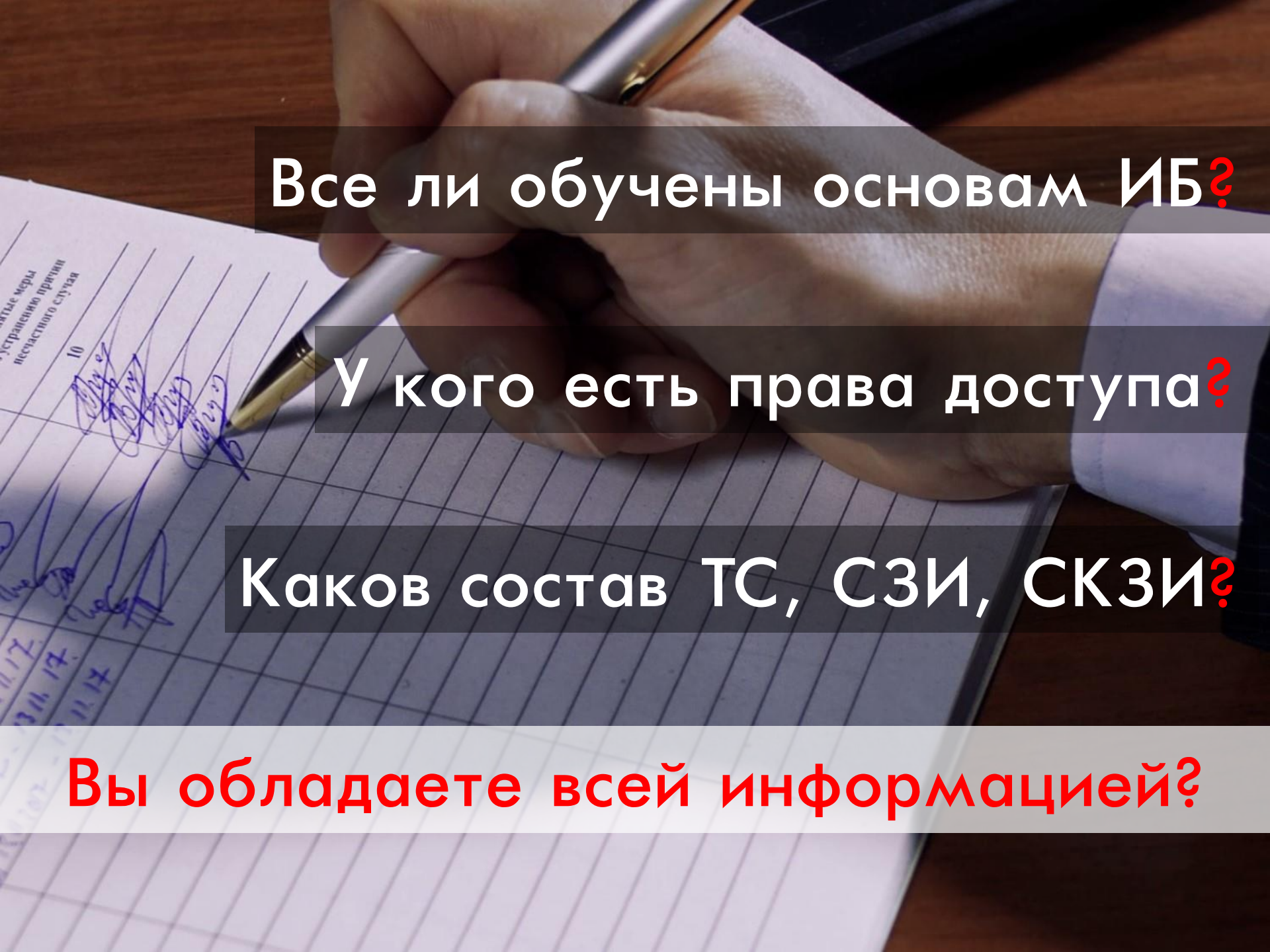
Халатный подход к организационным аспектам ИБ

...есть дела поважнее

...напечатал и забыл

...кто это читает?

Вы фиксируете все изменения и события в журналах учета?


Все ли обучены основам ИБ?
У кого есть права доступа?
Каков состав ТС, СЗИ, СКЗИ?
Вы обладаете всей информацией?

КИТ-Журнал

Платформа автоматизации процессов ИТ и ИБ

КИТ-Журнал

Автоматически ведутся 30 форм журналов и формируются 65 видов документов для всех подразделений.

Простая и квалифицированная подписи для всех действий и документов. Комиссионные подписания и оповещения по почте.

Формирование простой подписи средствами системы.

КИТ-Журнал

Основные функции КИТ-Журнал:

Автоматизация организационных процессов: платформа автоматизирует различные процессы информационной безопасности, включая рутинные задачи и рабочие процессы, связанные с управлением безопасностью и использованием криптосредств.

Обучение пользователей по вопросам информационной безопасности: инструктажи и тестирования для пользователей по различным вопросам информационной безопасности и использования СКЗИ / ЭП.

Управление документами и электронные подписи: возможность электронной подписи документов (актов, приказов, согласий и др.) может оптимизировать бизнес-процессы, сократить объем бумажной работы и повысить скорость транзакций.

Ведение всех журналов учета в электронном виде с электронными подписями.

Механизм назначения и отслеживания задач сотрудникам и пользователям с подтверждением исполнения.

КИТ-Журнал

Кому подойдет:

Отделы защиты информации: автоматизация организационных процессов информационной безопасности, проверки информационных систем, ведение журналов, формирование документов, соблюдение требований законов 152-ФЗ, 187-ФЗ, 63-ФЗ

Органы криптозащиты, отделы эксплуатирующие СКЗИ: автоматизация жизненного цикла эксплуатации СКЗИ, ключевых документов, носителей, хранилищ, соблюдение требований Приказа ФАПСИ 152, ПКЗ-2005.

Отделы ИТ: автоматизация учета парка компьютерной техники, используемых технических средств и программного обеспечения.

Основные пользователи:

Бюджетные учреждения и организации (Федеральные, государственные и местные органы власти, мед. учреждения, ВУЗы);

Крупные коммерческие организации (банки, заводы, госкорпорации с распределенной структурой, пищевые холдинги).

Преимущества

Сокращение ручного труда: автоматизация многих задач сократит потребность в ручном труде, сэкономив время и ресурсы.

Снижение эксплуатационных расходов: за счет оптимизации процессов и сокращения потребности в бумажной документации эксплуатационные расходы будут ниже.

Соответствие требованиям: платформа поможет организациям подготовиться к проверкам и пройти их, гарантируя, что все меры безопасности автоматизированы и документированы.

Адаптация новых сотрудников: с помощью платформы можно эффективно управлять обучением новых сотрудников вопросам информационной безопасности.

Внутренние проверки: планирование регулярных внутренних проверок ИТ-систем и процессов можно оптимизировать с помощью этой платформы.

КИТ-Журнал

Уникальные преимущества

1. Интерфейс оптимизирован для работы с большими массивами данных.

2. Встроенный выпуск сертификатов простой электронной подписи для пользователей - можно без доп. затрат обеспечить возможность сотрудникам подписывать записи журналов и документов.

3. Сбор подписей и выполнение задач пользователями по электронной почте - не нужно искать неподписанные записи, беспокоится о не заполненных полях или о необходимости формировать акты, система сама сделает и оповестит.

4. Полная юридическая значимость всех действий в системе - можно полностью отказаться от бумаги.

5. Настраиваемая система логирования ВСЕХ событий в системе можно задать регистрируемые параметры.

6. Автоматизированы ВСЕ журналы по информационной безопасности не нужно какие-то формы отдельно вести на бумаге.

7. Полная автоматизация учета СКЗИ в соответствии с инструкцией ФАПСИ (приказ 152) (все формы и журналы) - учтены все моменты от фиксации повреждений упаковки до контроля пломб.

8. Возможность настройки синхронизация с кадровой системой (через csv файлы либо SQL-запрос) - данные по сотрудникам всегда актуальны, не нужно вручную следить за актуальностью данных.

9. Гибкая подсистема разграничения доступа (настройка видимости разделов и полей) - можно реализовать произвольную модель разграничения прав доступа.

КИТ-Журнал

Сравнение с альтернативами

Параметр	КИТ-Журнал	Системы автоматизации процессов ИБ	Ручной способ, excel
Ввод данных	Импорт/синхронизация/SQL запросы	Импорт/интеграции (при наличии API).	Данные заполняются в электронных таблицах, не всегда достоверны.
Служба заданий и оповещений	Полностью управляемая, включение/отключение задач, создание своих задач и оповещений, исполнение скриптов.	В некоторых системах есть конструкторы процессов, возможности ограничены.	Самостоятельное планирование.
Подсистема ведения журналов	Все журналы (30 форм) с возможностью вывода печатных форм и электронными подписями.	Обычно только несколько журналов.	Собственно журналы ведутся на бумаге вручную. Часто ведутся не все нужные журналы.
Подсистема формирования актов и документов	65 видов документов, все могут быть подписаны электронными подписями. Есть возможность подписания комиссиями.	Документы формируются системой, но в основном без возможности подписать их непосредственно в системе электронной подписью (либо не для всех форм).	Документы готовятся в текстовых редакторах на основе шаблонов.
Подсистема инструктажей	3 инструктажа с возможностью загрузки учебного материала, 90 билетов по 10 вопросов. Все редактируется. Автоматическое планирование, привязка к должностям, рассылка тестов, формирование заключений, создание записей в журналах.	Присутствует, но механизм как правило не подразумевают автоматизации полного цикла.	Обучение, допуски проводятся вручную, либо с применением сторонних систем, либо проводятся формально.
Подсистема задач	Автоматическая постановка задач пользователям по всем аспектам ИБ и использованию СКЗИ, рассылка и исполнение задач по email.	Как правило работа внутри системы, либо отсутствует.	Задачи назначаются вручную.
Подсистема электронных подписей	Встроенный выпуск сертификатов простой подписи, использование криптопровайдеров для усиленной и квалифицированной подписей. Используется во всех разделах системы.	Используется ограничено, только в некоторых разделах.	Собственноручные подписи.
Подсистема разграничения доступа	Разграничение доступа вплоть до полей журналов. Области видимости для подразделений / филиалов. Управление сессиями, политики авторизации.	Присутствует, ограниченная функциональность.	Журналы и документы хранятся у ответственных.
Подсистема учета событий	Настраиваемая подсистема логирования произвольных событий в системе.	Присутствует, обычно набор регистрируемых событий ограничен.	Не применимо.

КИТ-Журнал

Как работает КИТ-Журнал?

1. Установка СУБД и приложений на сервер заказчика (дистанционно инженерами КИТ-Дистрибуция либо самостоятельно).

2. Настройка сервера, SMTP, LDAP, синхронизации с источниками данных. Загрузка/импорт начальных данных.

3. Настройка оповещений, ответственных. Выполнение разграничения доступа. Настройка логирования.

4. Выполнение действий в системе пользователями через браузер со своих рабочих мест. Пользователи используют учетные записи с настроенными ролями и областями видимости.

5. КИТ-Журнал выполняет автоматические задачи, планирует проведение инструктажей, создает записи в журналах, формирует документы.

6. Пользователям направляются оповещения с задачами, документами, инструктажами и тестами. Письма содержат ссылки на страницы подписания данных и выполнения задач.

7. Периодически выполняется синхронизация с кадровой системой. Система обновляет статусы сотрудников. При увольнении сотрудников, ответственные получают письма с перечнем необходимых действий (что нужно изъять/уничтожить). Новым сотрудникам автоматически назначаются инструктажи, процедуры допуска.

КИТ-Журнал

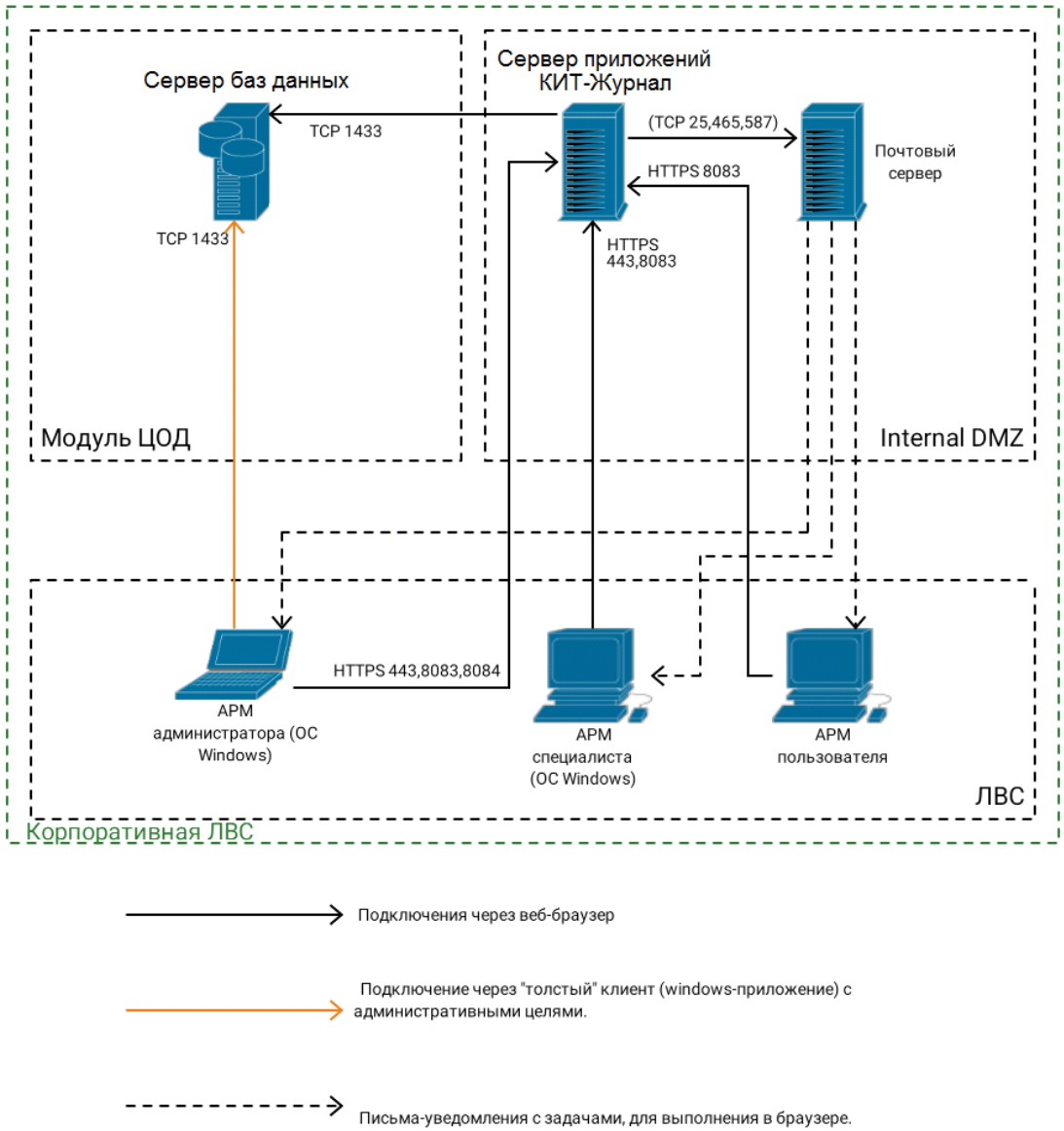


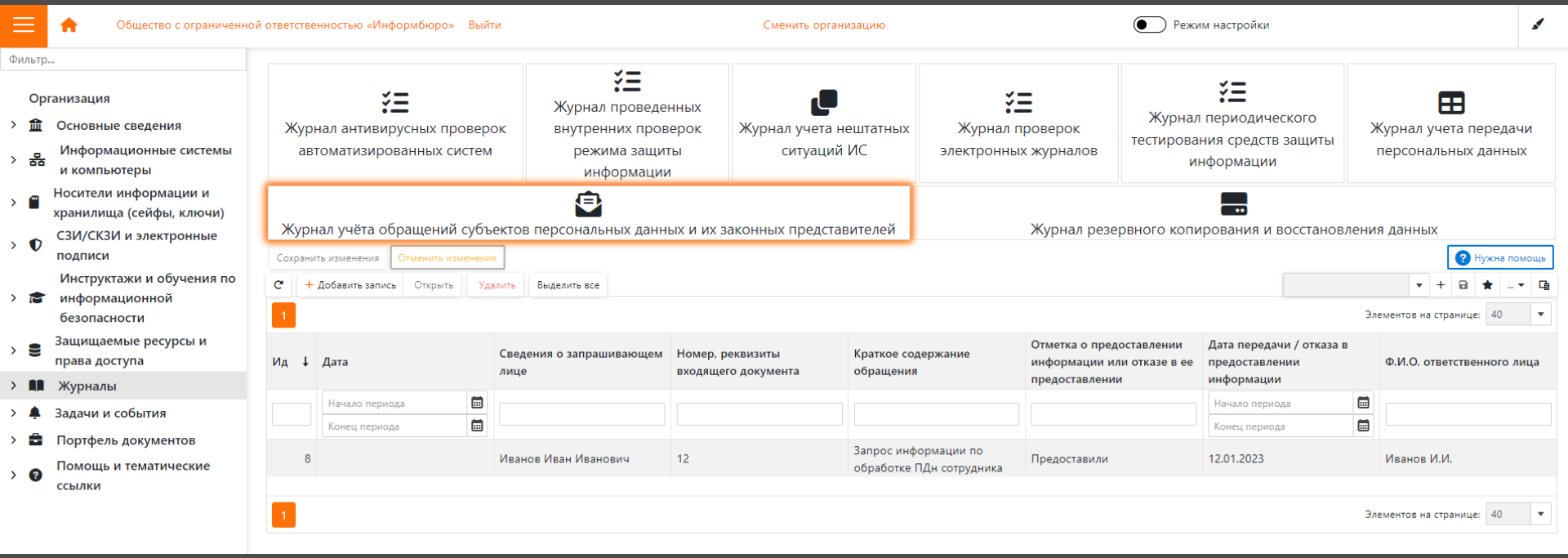
Схема подключений

Системные требования

Сервер:
- ОС РЕД ОС 8 с последними пакетами обновлений / ОС Windows 10/11/2012 Server или новее;
- СУБД PostgreSQL 16 (или новее) / Microsoft SQL Server 2014 (или новее);
- 16 ГБ оперативной памяти;
- 50 ГБ свободного места на диске;
- процессор 2-х/4-х ядерный серверный;
- постоянно подключен к сети организации.

Клиентское рабочее место:
- Браузер (Yandex, Firefox, Chrome, Opera, Edge) с плагином криптопровайдера;
- Криптопровайдер для подписания данных (КриптоПро CSP 5.0).

КИТ-Журнал



Все необходимые формы журналов и документов

КИТ-Журнал

Состав программного обеспечения КИТ-Журнал

Списки, перечни и каталоги

1. Список организаций (филиалов).
2. Список сотрудников.
3. Список подразделений.
4. Список должностей.
5. Список помещений.
6. Информационные системы и объекты.
7. Модели угроз.
8. Список компьютеров и устройств (СВТ).
9. Список программного обеспечения.
10. Журнал регистрации СЗИ и СКЗИ, эксплуатационной и технической документации к ним.
11. Каталог СЗИ.
12. Каталог инструктажей по информационной безопасности.
13. Комиссии по информационной безопасности.
14. Приказы по информационной безопасности.
15. Аттестации и работы по защите информации.
16. Учет и реагирование на инциденты ИБ (с формированием файлов НКЦКИ).
17. Контрагенты.

Активы (ресурсы) и права пользователей

1. Перечень защищаемых ресурсов и их администраторов.
2. Каталог прав доступа для ресурсов.
3. Список прав доступа.
4. Учетные записи пользователей.

Внутренние проверки и проверки надзорных органов

1. Каталог внутренних проверок.
   Персональные данные
2. Перечень обрабатываемых персональных данных и целей обработки.
3. Перечень баз данных ПДн.
   КИИ
4. Перечень критических процессов в организации.
5. План-график регламентных работ и проверок (СЗИ/СКЗИ).

Служебные журналы обеспечения процессов

1. Журнал задач.
2. Назначенные инструктажи и мероприятия.
3. Назначенные внутренние проверки.

Обеспечиваемые процессы

1. Планирование и выполнение внутренних проверок по защите информации для информационных систем.
2. Контроль проведения инструктажей по информационной безопасности, допуск к СКЗИ.
3. Автоматизированная рассылка обучающего материала и тестирование пользователей по вопросам информационной безопасности.
4. Автоматическое отслеживание прав доступа, носителей информации уволенных сотрудников.
5. Автоматическое формирование файлов для НКЦКИ и учет инцидентов информационной безопасности.
6. Формирование пакетов документов ПДн/ГИС/КИИ на основе данных в системе.
7. Автоматическое ведение журналов учета по информационной безопасности.
8. Формирование моделей угроз.
9. Автоматическое определение уровня защищенности ПДн, класса ГИС, категорирование КИИ.
10. Синхронизация данных с внешними источниками (через CSV файлы).
11. Выполнение внешних приложений и скриптов (PowerShell).

Журналы

1. Журнал учета машинных носителей информации.
2. Журнал выдачи/возврата машинных носителей информации.
3. Журнал периодического тестирования средств защиты информации.
4. Журнал учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн.
5. Журнал проверок электронных журналов.
6. Журнал антивирусных проверок автоматизированных систем.
7. Журнал проведенных внутренних проверок режима защиты персональных данных.
8. Журнал проведения инструктажа по информационной безопасности.
9. Журнал резервного копирования и восстановления данных.
10. Журнал учета актов.
11. Журнал учета МЧД (машиночитаемых доверенностей).
12. Журнал назначения прав пользователям.
13. Журнал учета передачи персональных данных.
14. Журнал учта обращений субъектов персональных данных и их законных представителей.
15. Журнал выдачи/возврата компьютеров.
16. Журнал учета фатов уничтожения персональных данных.
17. Журнал выполнения регламентных работ (СЗИ и СКЗИ).
18. Журнал задач.

СЗИ и СКЗИ

1. Журнал регистрации СЗИ и СКЗИ, эксплуатационной и технической документации к ним
2. Журнал поэкземплярного учета выдачи/подключения/изъятия криптосредств (СКЗИ).
3. Журнал учета установки/изъятия средств защиты информации.
4. Журнал учета хранилищ.
5. Журнал регистрации выдачи/приема хранилищ (помещений, сейфов, пеналов, печатей, ключей).
6. Журнал заседания комиссий по допуску к СКЗИ.
7. СКЗИ пользователя.
8. Журнал поэкземплярного учета и выдачи ключевых документов (носителей).
9. Журнал опечатывания (опломбирования) технических средств.
10. Технический (аппаратный) журнал СКЗИ.
11. Журнал поэкземплярного учета движения СКЗИ для Органа криптозащиты (ОКЗ).
12. Журнал поэкземплярного учета ключевых документов и носителей для Органа криптозащиты (ОКЗ).

КИТ-Журнал

Состав программного обеспечения КИТ-Журнал

Формируемые документы

Общие документы по организации

1. Акт классификации информационной системы (на ГИС и на ГИС с обработкой ПДн).
2. Модель угроз безопасности информации (документ формируется на каждую информационную систему).
3. Технический паспорт (документ формируется на каждую информационную систему).
4. Приказ/распоряжение/постановление о комиссии по определению класса ГИС и уровня защищенности ПДн.
5. Приказ/распоряжение/постановление об ответственном за защиту информации, не содержащей сведения, составляющие государственную тайну.
6. Приказ/распоряжение/постановление об утверждении перечня ИС, обрабатывающих защищаемую информацию, и перечня защищаемой информации, обрабатываемой в ПК, входящих в состав ИС.
7. Приказ/распоряжение/постановление о сотрудниках, осуществляющих обработку защищаемой информации, и имеющих доступ к обрабатываемой защищаемой информации.
8. Приказ/распоряжение/постановление о сотрудниках, которым разрешены действия по внесению изменений в базовую конфигурацию информационных систем и системы защиты информации.
9. Приказ/распоряжение/постановление о сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них.
10. Приказ/распоряжение/постановление о сотрудниках, имеющих доступ к содержанию электронного журнала сообщений
11. Приказ/распоряжение/постановление об обеспечении безопасности материальных носителей защищаемой информации.
12. Приказ/распоряжение/постановление об обеспечении безопасности помещений, в которых размещены ИС и сохранности носителей защищаемой информации.
13. Приказ/распоряжение/постановление об утверждении форм документов, необходимых в целях выполнения требований законодательства в области защиты информации.
14. Приказ/распоряжение/постановление об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации при ведении журнала учета посетителей.
15. Приказ/распоряжение/постановление о системе разграничения доступа в ИС.
16. Приказ/распоряжение/постановление о комиссии по уничтожению защищаемой информации (документ формируется при наличии соответствующей комиссии).
17. Приказ/распоряжение/постановление о введении в эксплуатацию системы видеонаблюдения (документ формируется при наличии системы видеонаблюдения)
18. Положение по организации и проведению работ по обеспечению безопасности защищаемой информации, при ее обработке в ИС.
19. Приказ/распоряжение/постановление об ответственном за планирование и контроль мероприятий по обеспечению информационной безопасности.
20. Приказ/распоряжение/постановление об ответственном за управление (администрирование) подсистемой безопасности (системой защиты информации).

Комплект документов по эксплуатации СКЗИ

1. Приказ/распоряжение/постановление об утверждении мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты информации.
2. Список допущенных к работе с ключами СКЗИ.
3. Заключение о готовности к работе с СКЗИ.
4. Перечень допущенных в помещения с ключами СКЗИ.
5. Акт уничтожения криптографических ключей.
6. Акт установки СКЗИ.
7. Акт изъятия СКЗИ.
8. Акт приема-передачи СКЗИ/КД.
9. Акт повреждения упаковки СКЗИ/КД.
10. Акт возврата (обратной передачи) СКЗИ.

Документы ПДн

1. Список работников, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных, необходим для выполнения их служебных обязанностей
2. Приказ/распоряжение/постановление об ответственном за организацию обработки ПДн.
3. Приказ/распоряжение/постановление об ответственном за обеспечение безопасности ПДн в ИС.
4. Приказ/распоряжение/постановление об утверждении перечня ПДн.
5. Политика в отношении обработки персональных данных.
6. Положение по организации и проведению работ по обеспечению безопасности защищаемой информации, при их обработке в ИС.
7. Порядок хранения, использования и передачи ПДн сотрудников.
8. Акт оценки вреда, который может быть причинен субъектам ПДн.
9. Акт определения уровня защищенности ПДн при их обработке в ИС (на ИСПДн).
10. Согласие на обработку ПДн
11. Согласие на поручение обработки ПДн
12. Согласие на передачу ПДн
13. Согласие на включение ПДн в общедоступные источники
14. Уведомление о намерении осуществлять обработку ПДн
15. Информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку ПДн
16. Информационное письмо о прекращении обработки ПДн.
17. Акт уничтожения персональных данных.

Документы КИИ

1. План мероприятий по реализации требований Федерального закона от 26 июля 2017 г. 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации и принятых в соответствии с ним нормативных правовых актов.
2. Приказ/распоряжение/постановление об утверждении Положения о комиссии по категорированию объектов КИИ.
3. Приказ/распоряжение/постановление о комиссии по категорированию объектов КИИ.
4. Приказ/распоряжение/постановление об утверждении перечня объектов КИИ, подлежащих категорированию (в том числе форма отправки сведений во ФСТЭК России).
5. Акт категорирования объекта КИИ.
6. Сопроводительное письмо в ФСТЭК с перечнем объектов КИИ, подлежащих категорированию.
7. Форма утверждения перечня объектов КИИ с ФСТЭК.
8. Сопроводительное письмо в ФСТЭК с результатами категорирования объектов КИИ.
9. Сведения о результатах присвоения объекту КИИ категории значимости (документ формируется на каждый объект).
10. Приказ/распоряжение/постановление о назначении администратора безопасности значимых объектов КИИ.
11. Приказ/распоряжение/постановление об ответственном за обеспечение безопасности КИИ.
12. Приказ/распоряжение/постановление о силах обеспечения безопасности значимых объектов КИИ.

Лицензирование

Бессрочные лицензии.

Включена техническая поддержка 1 год и дистанционная установка.

Услуги по внедрению: от 0% до 100% от стоимости лицензий (в зависимости от необходимости интеграций, индивидуальных адаптаций и т.п.).

Стоимость типовых лицензий от 185 000 р.

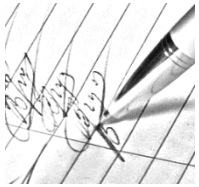
Стоимость индивидуальных конфигураций от 582 000 р.

Стоимость проектов для распределенных организаций с филиалами и интеграциями от 1 500 000 р.

Три пакета технической поддержки со второго года (базовый 25%, расширенный 40%, максимальный 75%).

Для точного составления спецификаций рекомендуется заполнять опросный лист!

КИТ-Журнал



Все виды подписей

ViPNet CSP

КРИПТОПРО

Минкомсвязь России

В реестре Российского ПО

Индивидуальные конфигурации

КИТ-Дистрибуция

Разработчик решений для автоматизации процессов учета и формирования документов.

55 партнеров во всех федеральных округах.

Некоторые пользователи продуктов КИТ-Журнал:

РУСАГРО

Министерство труда и социальной защиты Российской Федерации

Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Территориальный Фонд Обязательного Медицинского Страхования Свердловской области

KIA

ИВТЭ

Электрощит Самара

Петропавловск

РЕГИС Научно-производственная геологическая фирма

Газпром проектирование

Крокус Банк

ЛУКОЙЛ

Газпром газораспределение Барнаул

ЧНК

Сочи международный аэропорт

Краснодар международный аэропорт

Получите пробный доступ!

info@kit-URAL.RU

Спасибо!