Функциональные и технические характеристики программного обеспечения «КИТ-Журнал»

1. Общие характеристики.

1.1. Архитектура программного обеспечения и состав компонентов.

- имеет клиент-серверную архитектуру, с возможностью добавления клиентских лицензий для дочерних организаций/филиалов;
- все компоненты программного обеспечения развертывают на серверах/компьютерах заказчика;
- наличие встроенной службы штампов времени, с применением электронной подписи для подтверждения подлинности штампов;
- наличие встроенной службы резервирования, с возможностью создания и редактирования собственных политик резервирования. Интерфейс службы резервирования позволяет создавать как полные копии, так и разностные с настройкой произвольного расписания;
- средство содержит встроенный типовой комплект журналов учета и документов по учету криптосредств. Типовой комплект журналов и документов по учету криптосредств включает следующие формы:
    - Типовая форма лицевого счета пользователя СКЗИ;
    - Типовая форма журнала поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
    - Типовая форма журнала учета хранилищ ключевых документов, дистрибутивов, технической и эксплуатационной документации к СКЗИ;
    - Типовая форма журнала поэкземплярного учета ключевых документов;
    - Типовая форма акта уничтожения СКЗИ, ключевой информации, эксплуатационной и технической документации СКЗИ;
    - Типовая форма журнала учёта хранилищ;
    - Акт установки и настройки СКЗИ
    - Акт деинсталляции (изъятия) СКЗИ;
- наличие в составе системы веб-приложения, обеспечивающего доступ к журналам и каталогам системы с помощью браузеров Chrome, Opera, Mozilla, Edge, Yandex с неограниченным числом одновременных подключений;
- для веб-приложения предусмотрена возможность группировки журналов в разделы, настройка видимости полей, фильтрации отображаемых записей в зависимости от учетной записи;
- наличие настраиваемой службы заданий и оповещений о событиях с возможностью отдельной настройки триггеров («По расписанию», «По состоянию записи», «По событию в журнале») и действий («Создать запись», «Изменить запись», «Отправить письмо по электронной почте», «Синхронизация», «PowerShell скрипт», «Удалить запись», «Печать», «Запуска триггера»);
- для службы заданий и оповещений предусмотрена возможность быстрого включения/отключения триггеров и действий, их внеочередного выполнения;
- возможность отложенного выполнения задач и формирования документов службой заданий;
- микросервис отправки почтовых сообщений с возможностью настройки параметров подключения к почтовому сервису;
- для службы заданий и оповещений предусмотрена возможность просмотра формируемых и сформированных системой документов, очереди формирования документов;

- наличие конфигуратора службы заданий и оповещений с возможностью создания неограниченного количества триггеров (с произвольным количеством условий) и действий, группировкой их в задачи;
- поддержка синхронизации со сторонними системами через CSV-файл;
- поддержка сертифицированных криптопровайдеров для создания электронной подписи (в том числе ViPNet CSP);
- поддержка шаблонов записей, для автоматического создания записей в журналах службой заданий и оповещений;
- централизованное управление журналами учета;
- наличие административной утилиты для создания и редактирования журналов и их полей, разделов системы, с прямым подключением к базе данных.
- административная утилита позволяет выполнять следующие операции:
    - Множественное изменение записей в журнале (одновременное изменение поля или нескольких полей во всех выделенных записях);
    - Импорт данных журналов из CSV файлов;
    - Экспорт данных журналов в CSV файлы;
    - Возможность дублирования схем журналов;
    - Настройка и редактирование шаблонов формируемых печатных форм журналов и документов;
    - Настройка автоматических подстановок значений для полей;
    - Формирование и редактирование справочников;
    - Создание/изменение/удаление журналов;
    - Перемещение в другое представление журналов, списанных под уничтожение, доступных только администраторам.

1.2. Подсистема разграничения прав доступа.
- поддерживается разграничение прав доступа пользователей к электронным журналам, полям, разделам системы;
- предусмотрены следующие права доступа к электронным журналам: чтение, изменение, удаление записей;
- поддержка групп пользователей;
- возможность создания сертификатов простой электронной подписи для пользователей;
- возможность управления учетными записями пользователей (создание, изменение, блокировка, разблокировка, удаление) с возможностью рассылки новым пользователям информационных сообщений с информацией об учетной записи и смене пароля;
- поддержка ролевой модели разграничения доступа с управлением ролями (создание, изменение, удаление) и политиками авторизации ролей при доступе к ресурсам;
- система позволяет настраивать роли с областями видимости записей для филиалов. Пользователь с ролью администратора филиала может видеть записи всех журналов, относящихся к текущему филиалу;
- в системе предусмотрена роль, позволяющая редактировать записи своего филиала. Предусмотрена возможность сокрытия записей чужих филиалов.

1.3. Характеристики интерфейса.
- возможность вывода электронных журналов на печать;
- возможность изменения форм;
- возможность импорта данных в журналы из CSV файлов, с возможностью включения/отключения кнопки импорта для отдельных журналов и разделов системы;
- наличие раздела для упрощенного импорта машинных носителей, СКЗИ/СЗИ и информации об их установке и выдаче из CSV файлов с автоматическим формированием записей в следующих журналах:

- Журнал регистрации СЗИ и СКЗИ (первичная постановка на учет);
- Журнал поэкземплярного учета выдачи /подключения /изъятия криптосредств (СКЗИ);
- Журнал поэкземплярного учета движения СКЗИ для Органа криптозащиты (ОКЗ);
- Журнал учета установки/изъятия средств защиты информации;

- наличие раздела для упрощенного импорта сведений об электронных подписях и фактах и выдачи из CSV файлов с автоматическим формированием записей в следующих журналах:

- Журнал поэкземплярного учета и выдачи ключевых документов (носителей);
- Журнал поэкземплярного учета ключевых документов и носителей ОКЗ;
- Журнал учета машинных носителей информации;
- Журнал выдачи/возврата машинных носителей информации.

- предусмотрена возможность настройки отображаемых полей журналов (видимость, параметр «только чтение», параметр «обязательное поле»);
- возможность генерации отчетных документов по данным в журналах в формате RTF, DOCX, PDF;
- наличие встроенных средств поиска и фильтрации в электронных журналах;
- возможность создания произвольных пользовательских фильтров для журналов, списков и таблиц;
- возможность загрузки файлов в поля журнала;
- поддержка перекрестных ссылок в журналах;
- поддержка технологий простой электронной подписи на базе паролей или PIN-кодов, а также средств квалифицированной электронной подписи;
- возможность пользователей подтверждать выполнение задач прямо из писем электронной почты, без авторизации и входа в программу (с помощью временных ссылок);
- возможность просмотра сводных списков задач и задач отдельных пользователей;
- журналы, разделы и поля снабжены подсказками;
- возможность изменения цветовых тем оформления интерфейса.

1.4. Прочие характеристики.

- программное обеспечение «КИТ-Журнал» зарегистрировано в государственном реестре программ и баз данных в соответствии с действующим законодательством;
- программное обеспечение внесено в Единый реестр российских программ для электронных вычислительных машин и баз данных;
- предусмотрена возможность распределения журналов по группам и подразделениям организации;
- бессрочная лицензия;
- возможность автоматизации дополнительных бизнес-процессов;
- **автоматический сбор электронных подписей для неподписанных записей в журналах;**
- возможность создания дочерних организаций/филиалов и учетных записей для них;
- реализация процессов передачи СКЗИ между органом криптозащиты и подведомственными(дочерними) организациями/филиалами (с автоматических созданием соответствующих записей в журналах);
- возможность авторизации в системе с помощью протокола LDAP.

2. Автоматизируемые с помощью программного обеспечения «КИТ-Журнал» процессы.

- Планирование и выполнение внутренних проверок по защите информации для информационных систем.

- Контроль проведения инструктажей по информационной безопасности, допуск к СКЗИ с возможностью автоматической проверки знаний сотрудников путем электронного тестирования.
- Автоматизированная рассылка обучающего материала по вопросам информационной безопасности.
- Автоматическое отслеживание прав доступа, носителей информации уволенных сотрудников.
- Формирование пакетов документов по учету криптосредств на основе данных в системе.
- Формирование пакетов документов ПДн/ГИС/КИИ на основе данных в системе.
- Автоматическое ведение журналов учета по информационной безопасности.
- Автоматическое определение уровня защищенности ПДн, класса ГИС, категорирование КИИ.
- Синхронизация данных с внешними источниками (через SQL-запрос для кадровых данных, через CSV-файл для других данных).
- Выполнение внешних приложений и скриптов (PowerShell).

3. Функциональные возможности программного обеспечения «КИТ-Журнал».

- список (каталог) организаций-контрагентов;
- список (каталог) филиалов;
- каталоги филиалов и организаций-контрагентов ведутся раздельно (в разных разделах);
- раздельный учет помещений контрагентов и филиалов Заказчика;
- электронный журнал учета машинных носителей информации;
- электронный журнал учета фактов выдачи/возврата машинных носителей информации;
- формирование оповещений для ответственных лиц в случае обнаружения фактов невозврата выданных носителей информации увольняемыми сотрудниками;
- автоматическое формирование акта уничтожения машинного носителя информации;
- автоматическое составление плана внутренних проверок состояния защиты информации;
- оповещение ответственных лиц по электронной почте о необходимости проведения проверки состояния защиты информации;
- автоматическое формирование протоколов по результатам выполненных проверок состояния защиты информации;
- электронный журнал периодического тестирования средств защиты информации;
- учет средств защиты информации, технических средств, программного обеспечения в привязке к компьютерам и информационным системам;
- электронный журнал учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств на компьютерах;
- автоматическое отслеживание изменений в статусе объектов и субъектов с формированием оповещений для ответственных лиц;
- оповещение ответственных лиц об окончании сроков действия сертификатов на средства защиты информации по электронной почте;
- автоматическое оповещение администратора об изменении статуса пользователя (увольнение, смена должности);
- автоматическое формирование оповещений в случае выявления изменений статуса пользователей;
- электронный перечень защищаемых ресурсов и их администраторов;
- список учетных записей пользователей защищаемых ресурсов;
- учет администраторов и пользователей защищаемых ресурсов индивидуально по каждому ресурсу;
- учет программного обеспечения, установленного на компьютеры информационных систем;

- автоматизированная процедура допуска пользователей к работе с СКЗИ, включающая:
  - направление пользователю обучающего материала по электронной почте;
  - внесение записи в журнал проведения инструктажей по факту завершения инструктажа;
  - автоматическое формирование заключения о допуске к работе с СКЗИ;
- возможность редактирования каталога инструктажей, загрузки материалов Заказчика, редактирования списка вопросов и билетов для тестирования пользователей;
- электронный журнал проведения инструктажей по информационной безопасности;
- электронный журнал заседания комиссий по допуску к СКЗИ;
- редактируемый каталог типов СЗИ и СКЗИ, с указанием сроков действия сертификатов соответствия;
- электронный журнал поэкземплярного учета выдачи/подключения/изъятия криптосредств (СКЗИ);
- электронный журнал регистрации выдачи/приема хранилищ (помещений, сейфов, пеналов, печатей, ключей);
- возможность включения проверки возможности выдачи СКЗИ/ключевых документов пользователю, с учетом сведений журнала регистрации выдачи/приема хранилищ;
- электронный журнал опечатывания (опломбирования) технических средств;
- электронный журнал поэкземплярного учета и выдачи ключевых документов (носителей);
- автоматическое оповещение ответственных пользователей о необходимости уничтожения ключевых документов при окончании их срока действия;
- автоматическое формирование акта уничтожения ключевых документов;
- возможность ведения аппаратного (технического) журнала для каждого СКЗИ;
- автоматическое ведение лицевых счетов пользователей СКЗИ;
- возможность формирования списка СКЗИ пользователя;
- формирование актов жизненного цикла СКЗИ (акт установки, изъятия, уничтожения) с автоматической нумерацией и возможностью комиссионного подписания электронной подписью (по электронной почте);
- формирование актов жизненного цикла ключевых документов (акт передачи, уничтожения) с автоматической нумерацией и возможностью комиссионного подписания электронной подписью (по электронной почте);
- формирование печатных форм всех журналов (форматы RTF, DOCX, PDF) с выводом сведения об электронных подписях.

Состав программного обеспечения «КИТ-Журнал»

Списки, перечни и каталоги

Общее

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).

Активы (ресурсы) и права пользователей

17. Перечень защищаемых ресурсов и их администраторов.
18. Каталог прав доступа для ресурсов.
19. Список прав доступа.
20. Учетные записи пользователей.

Внутренние проверки и проверки надзорных органов

21. Каталог внутренних проверок.

Персональные данные

22. Перечень обрабатываемых персональных данных и целей обработки.
23. Перечень баз данных ПДн.

КИИ

24. Перечень критических процессов в организации.

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

Общие 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.

СЗИ и СКЗИ

11. Журнал регистрации СЗИ и СКЗИ, эксплуатационной и технической документации к ним
12. Журнал поэкземплярного учета выдачи/подключения/изъятия криптосредств (СКЗИ).
13. Журнал учета установки/изъятия средств защиты информации.
14. Журнал учета хранилищ.
15. Журнал регистрации выдачи/приема хранилищ (помещений, сейфов, пеналов, печатей, ключей).
16. Журнал заседания комиссий по допуску к СКЗИ.
17. СКЗИ пользователя.
18. Журнал поэкземплярного учета и выдачи ключевых документов (носителей).
19. Журнал опечатывания (опломбирования) технических средств.
20. Технический (аппаратный) журнал СКЗИ.

Персональные данные

21. Журнал учета передачи персональных данных.
22. Журнал учёта обращений субъектов персональных данных и их законных представителей.

Учет активов (ресурсов), назначения прав, заявки

23. Журнал назначения прав пользователям.
24. Журнал учета МЧД (машиночитаемых доверенностей).

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).
21. Акт уничтожения персональных данных.

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 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.

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.