КЕЙСИСТЕМС 15 лет

19-21 ноября 2018 г.
г. Москва

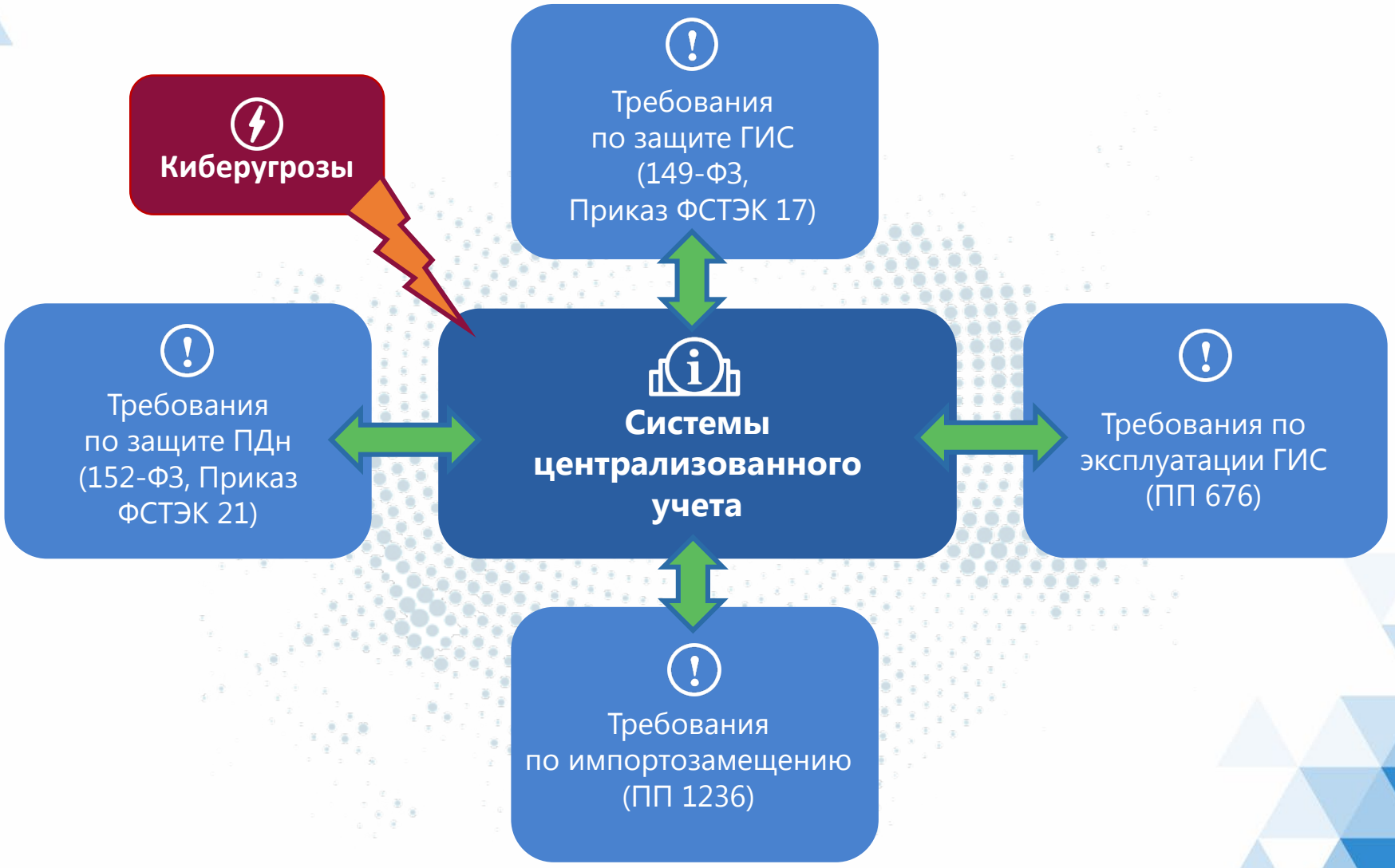
Вопросы информационной безопасности в системах централизованного бухгалтерского учета

Докладчик:

Фёдоров Иван Александрович

Заместитель генерального директора
компании «КСБ-СОФТ»

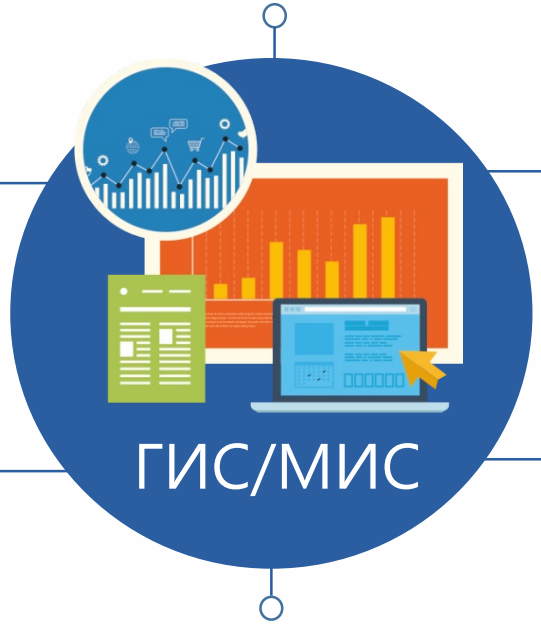
Выполнение требований законодательства



ГИС или не ГИС (149-ФЗ; ПП от 06.07.2015 N676)?

Создаются в целях обеспечения обмена информацией между государственными органами

Создаются в целях реализации полномочий государственных органов



Создаются на основе статистической и иной документированной информации

Создаются на основании федеральных законов, законов субъектов РФ

Создаются на основании правовых государственных актов

Создаются с учетом требований, предусмотренных законодательством РФ о контрактной системе в сфере закупок

Если иное не установлено решением о создании государственной (муниципальной) информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы

ГИС. Случай из практики

- В ходе выездной проверки учреждения было выявлено нарушение: непредоставление сопроводительных документов в электронной форме во ФГИС, учреждение оштрафовано
- Учреждение подало апелляцию в арбитражный суд, в которой было указано отсутствие информации о создании и вводе в эксплуатацию ФГИС
- В ходе рассмотрения дела было установлено отсутствие на официальном сайте федерального органа власти правового акта о вводе ФГИС в эксплуатацию (ПП 676), сведения о размещении технических средств ФГИС в реестре территориального размещения технических средств информационных систем отсутствуют (ПП 675), что «препятствует использованию ФГИС в установленных целях»
- Решение: у учреждения «не имелось правовых оснований для использования ФГИС», вина учреждения не установлена

Постановление Тринадцатого арбитражного апелляционного суда от 10 ноября 2017 г. N 13АП-23356/17

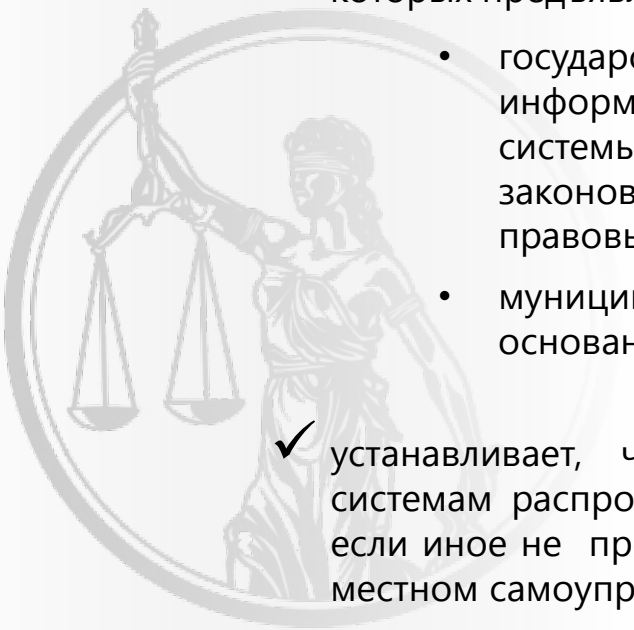
ГИС. Еще один случай

- Был инцидент ИБ с информационными системами Правительства Оренбургской области, по инициативе УМВД и УФСБ было проведено расследование
- Виновные лица установлен не были, но привлекли к ответственности операторов информационных систем (заказчика и оператора, п.6 ст.13.12)
- Операторы все это время считали «Электронную почту» «продуктом ИТС», а официальные веб-порталы – просто ИС, системы не внесены в реестр ГИС
- ФСБ считает, что это ГИС (информация структурируется, используется для обмена)
- Суд решил, что информационные системы не отнесены ГИС, но имеют их признаки (созданы в рамках выполнения НПА области, предназначены для реализации полномочий ОГВ и обеспечения обмена информацией

Решение Ленинского районного суда г. Оренбург от 5 октября 2016 года № 12-933/2016

Нормативные требования по защите информации в государственных информационных системах (ГИС)

Федеральный закон от 27 июля 2006г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»:



- ✓ определяет понятия информационных систем, к обеспечению безопасности в которых предъявляются специальные требования (статьи 13,14):
  - государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых государственных актов;
  - муниципальные информационные системы – созданные на основании решения органа местного самоуправления.
- ✓ устанавливает, что требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении;
- ✓ определяет, что требования о защите информации, содержащейся в государственных информационных системах, устанавливаются ФСБ России и ФСТЭК России.

Нормативные требования по защите персональных данных (ПДн)

Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»:

- ✓ определяет Меры по обеспечению безопасности персональных данных при их обработке (статья 19)
- ✓ устанавливает, что требования по обеспечению безопасности ПДн распространяются на все организации, которые осуществляют обработку ПДн
- ✓ определяет, что требования по обеспечению безопасности ПДн, устанавливаются ФСТЭК России и ФСБ России в пределах их полномочий

Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

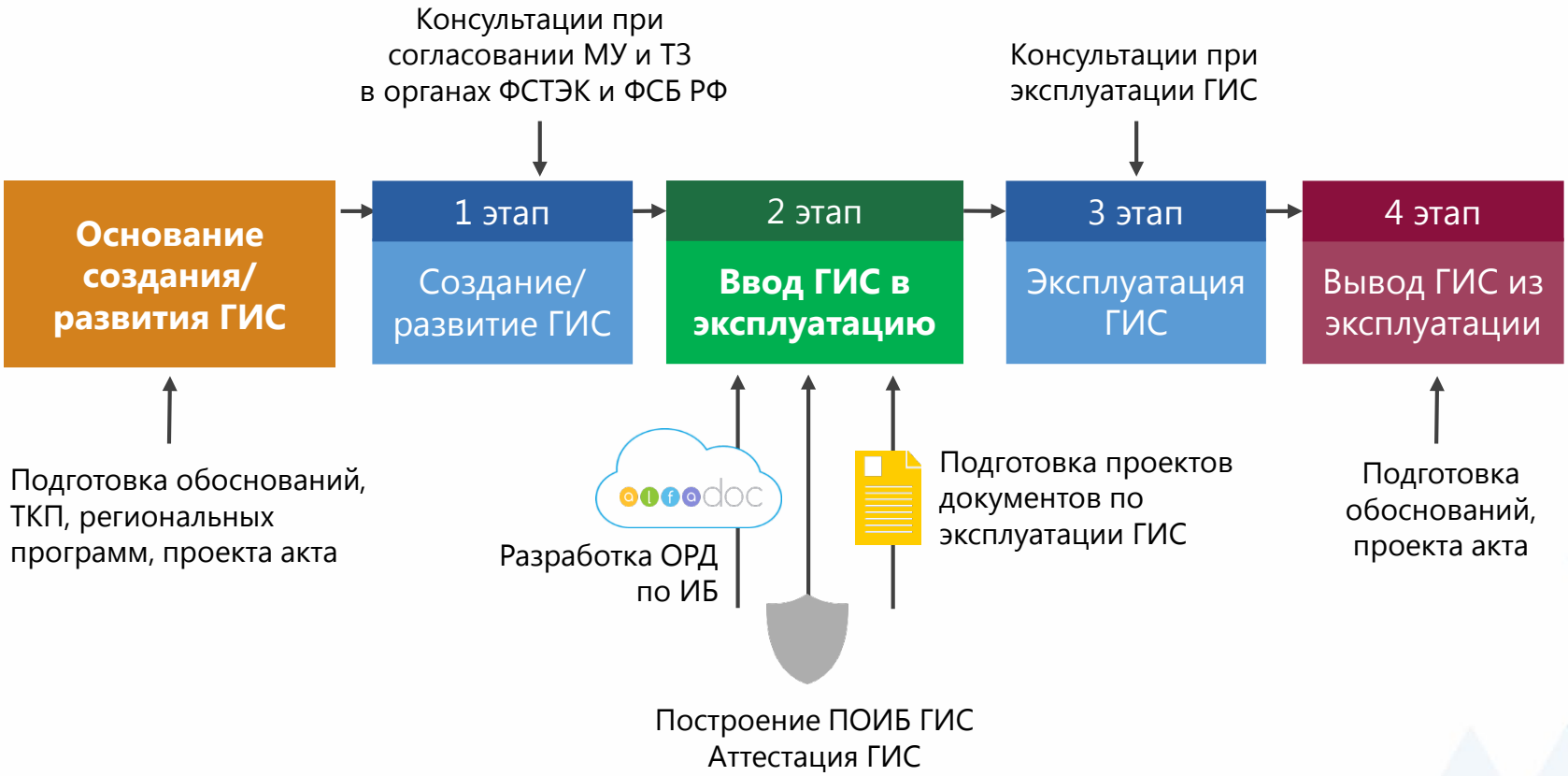
Нормативные требования по защите персональных данных (ПДн)

Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

Порядок создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации ГИС

(жизненный цикл ГИС согласно ПП 676)



Жизненный цикл ГИС. Особенности формирования требований

Учитывать изменения актуальной редакции приказа 17 ФСТЭК России

- Пункт 14.3, связь требований с банком данных угроз безопасности информации (bdu.fstec.ru)

Учитывать изменения в положении ФСТЭК России о системе сертификации СЗИ

- Срок действия сертификата соответствия – до 5 лет, средство защиты может применяться по окончании срока действия сертификата соответствия – с реестра СЗИ уже удалены сроки действия сертификатов

Жизненный цикл ГИС. Особенности ввода в эксплуатацию

Учитывать изменения актуальной редакции приказа 17 ФСТЭК России

- Пункт 17, «Проведение аттестационных испытаний информационной системы должностными лицами, осуществляющими проектирование и (или) внедрение системы защиты информации информационной системы, не допускается»
- Пункты 16.6, 17.2, анализ уязвимостей при опытной эксплуатации системы защиты
- Пункт 17.3, «аттестация сегментов»
- Пункт 17.4, аттестат на 5 лет
- Пункт 17.6, аттестация ЦОДов: «центр обработки данных должен быть аттестован по классу защищенности не ниже класса защищенности, установленного для создаваемой информационной системы»

Централизованная бухгалтерия

- Защита и аттестация ИС (ПДн), организация взаимодействия со своей ИС
- Выполнение требований по взаимодействию с региональной ИС
- Оператор цифрового документооборота

Муниципальный орган (ГРБС)

Централизованная бухгалтерия

Финансовый орган МО или субъекта

Планирование

Исполнение

Отчётность

- Выполнение требований по взаимодействию с федеральными ИС
- Защита и аттестация ИС (ПДн, ГИС, КИИ), организация защищенного взаимодействия со своими ИС

- Цифровой документооборот (абонент)
- Выполнение требований по взаимодействию с централизованной ИС

Учреждение (АУ, БУ, КУ)

Оператор

Руководитель

Централизованная бухгалтерия

Защита на уровне финоргана субъекта или МО

- Аудит и разработка **комплекта документации*** по защите информации в ЦБ финоргана, регламентация применения ЭП
- Техническая защита серверов и аттестация ЦБ ФО
- Разработка требований по подключению к ЦБ ФО
- Выполнение требований по подключению к ФИС

Защита на уровне ГРБС, муниципалитета

- Аудит и разработка **комплекта документации*** по защите информации в ЦБ ГРБС, регламентация применения ЭП
- Техническая защита серверов и аттестация ЦБ ГРБС

- Выполнение требований по подключению к ЦБ финоргана

Защита в учреждении (АУ, БУ, КУ)

- Аудит и разработка **комплекта документации*** по защите информации в МИС, регламентация применения ЭП

- Выполнение требований по подключению к ЦБ ФО или ЦБ ГРБС

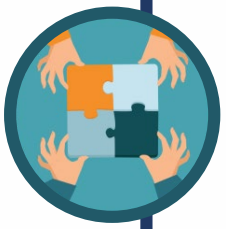
Информационная безопасность. Сервисный подход

Аудит и консалтинг

- Организационный и технический аудит
- Разработка организационных мер
- Проектирование

ИТ-безопасность

Применение надежных и стабильных средств технической защиты



Сервисы сопровождения

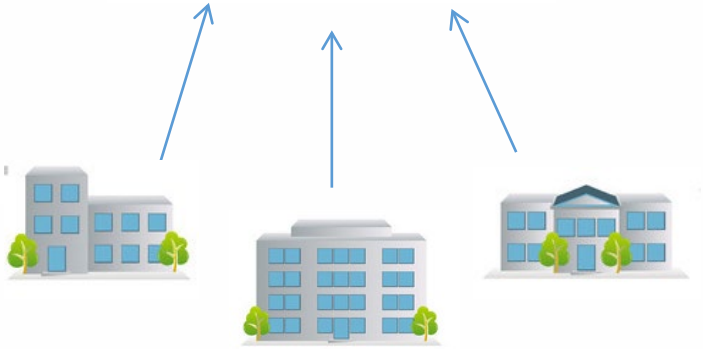
- Техническое сопровождение
- Реагирование на инциденты, взаимодействие с ГосСОПКА
- Консультации, сопровождение проверок

Оценка соответствия

- Аттестация по требованиям безопасности
- Контроль эффективности

ИТ-коннектор

Государственная информационная система



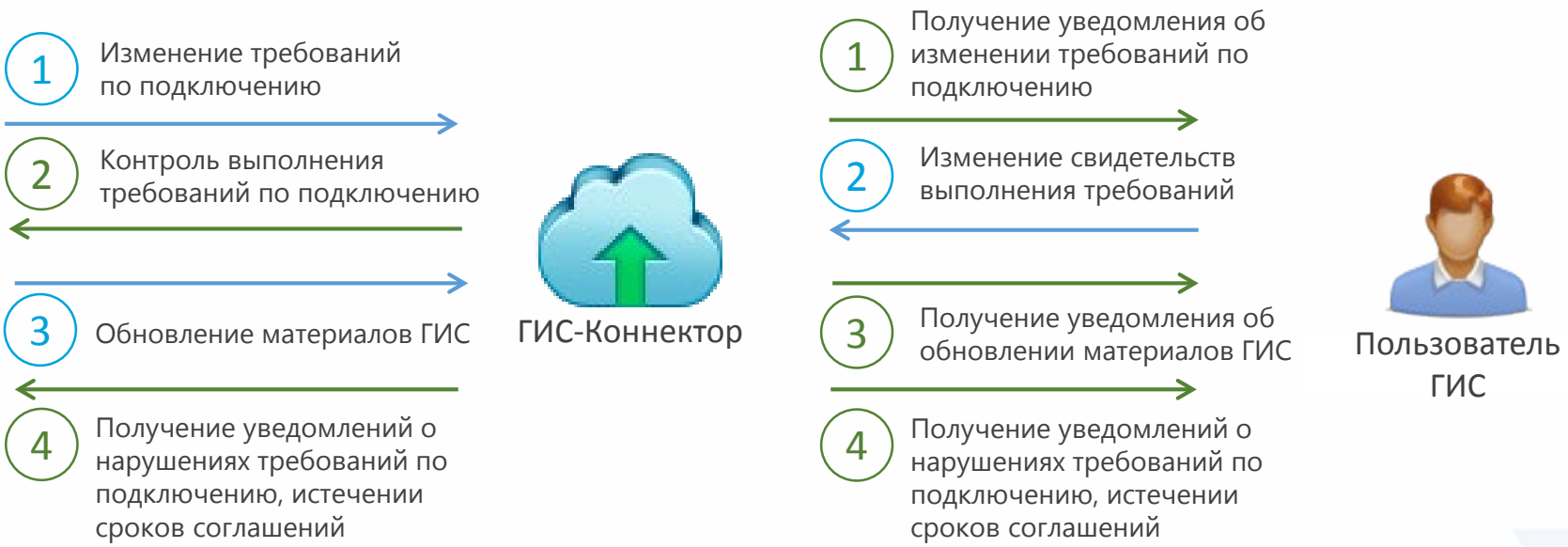
Пользователи ГИС

1. Разработка и трансляция потенциальным пользователям требований по подключению к ГИС
2. Организация приема заявок на подключение к ГИС
3. Обработка заявок: контроль выполнения требований
4. Подключение к ГИС пользователей, выполнивших требования
5. Постоянный контроль выполнения требований по подключению

ИТ-коннектор. Начало работы с ГИС

ИТ-коннектор. Начало работы с ГИС

ИТ-коннектор. Эксплуатация ГИС



Типовой сценарий проекта

Полезные советы

Создайте надежную основу для всех инициатив (среднесрочная программа ИБ), учитывайте все требования для оптимизации затрат

Планируйте мероприятия по ИБ на каждом этапе жизненного цикла ИС (создание, модернизация, передача другому оператору, вывод из эксплуатации), не забывайте про эксплуатационную документацию

Учитывайте сильную взаимосвязь с иными ИС, регламентируйте информационное взаимодействие (распределение ответственности)

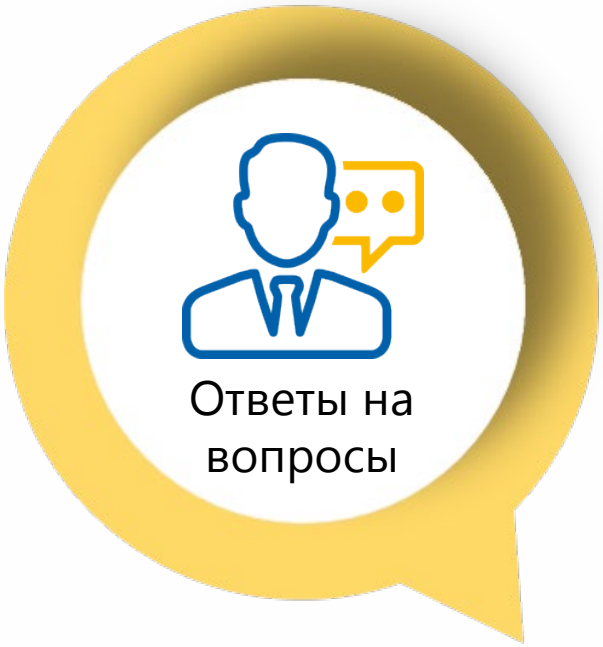
Сохраните возможности развития аттестованных ИС

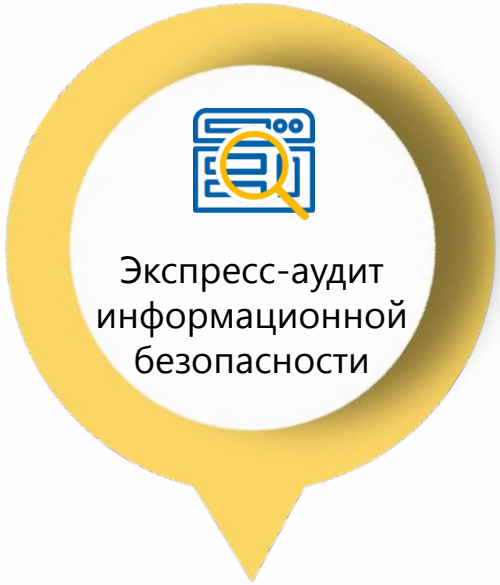
Выводите ИС из эксплуатации правильно

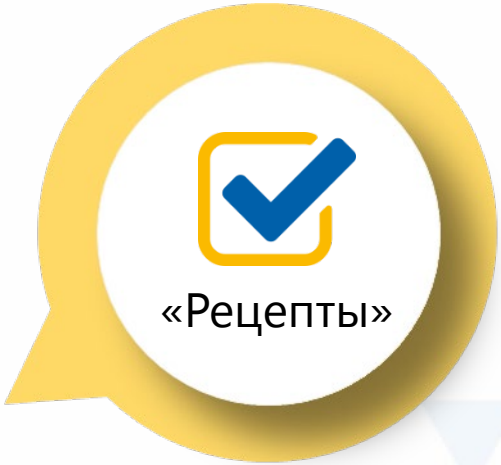
Полезные советы

- Создайте надежную основу для всех инициатив (среднесрочная программа ИБ), учитывайте все требования для оптимизации затрат
- Планируйте мероприятия по ИБ на каждом этапе жизненного цикла ИС (создание, модернизация, передача другому оператору, вывод из эксплуатации), не забывайте про эксплуатационную документацию
- Учитывайте сильную взаимосвязь с иными ИС, регламентируйте информационное взаимодействие (распределение ответственности)
- Сохраните возможности развития аттестованных ИС
- Выводите ИС из эксплуатации правильно

Клуб







ИТ-Проектор

Спасибо
за внимание!

ООО «КСБ-СОФТ»
8 (8352) 322-322
ksb-soft.ru
sec@keysystems.ru