КСБ-СОФТ

Кибербезопасность региональных информационных систем закупок в контексте цифровой экономики

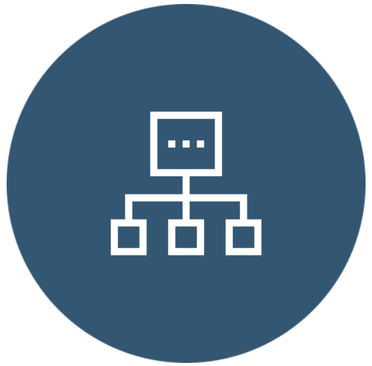
Владислав Николаев

Начальник отдела регионального развития

ООО «КСБ-СОФТ»

Региональные и муниципальные информационные системы

в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд



Как правило, создаются и эксплуатируются уполномоченными государственными органами. По всем признакам такие системы можно отнести к государственным информационным системам (ГИС). К таким признакам относятся:

а) такие системы создаются в целях реализации полномочий государственного органа и обеспечения обмена информацией между различными государственными органами

← Часть 1 статьи 14 ФЗ № 149-ФЗ от 27.07.2006

б) в таких системах обрабатывается информация, предоставляемая государственными органами и органами местного самоуправления

← Часть 3 статьи 14 ФЗ № 149-ФЗ от 27.07.2006

в) дополнительно, следует отметить, что такие системы обрабатывают ПДн. Хотя и данные ПДн являются общедоступными, данный факт не отменяет регламентацию обработки ПДн

← Постановление Правительства № 1119 от 11.01.2012

Нормативно-правовые акты

- Федеральный закон от 27 июля 2006 года N 149 «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства РФ от 6 июля 2015 г. N 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
- Постановление Правительства РФ от 28 ноября 2013 г. N 1091 "О единых требованиях к региональным и муниципальным информационным системам в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд"
- Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
- 152-ФЗ
  1119 ПП
  378 приказ ФСБ
  21 приказ ФСТЭК
  и т.д.

Особенности защиты ИС в сфере закупок

- В таких системах как правило обрабатывается общедоступная информация. Для таких систем необходимо обеспечить целостности обрабатываемой информации и ее доступность
- Такие системы открыты для широкого круга лиц
- Такие системы построены на базе веб-технологий, что вызывает потребность в использовании специализированных средств защиты веб-приложений

Оператор ГИС

Согласно ст. 2, 13, 14 149-ФЗ

Оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

- Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы;
- Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы.

Источники

1. Требования по защите ГИС	→	149-ФЗ Приказ ФСТЭК N 17
2. Требования по защите ПДн	→	152-ФЗ Приказ ФСТЭК N 21, Приказ ФСБ N 378
3. Требования по эксплуатации ГИС	→	Постановление Правительства № 676
4. Отраслевые требования	→	Постановление Правительства № 1091
5. Киберугрозы		

Жизненный цикл ГИС для Торгов

Общий порядок согласно 676-ПП

Комплексный подход. Сервисная модель

Аудит и консалтинг

- Организационный и технический аудит;
- Разработка организационных мер;
- Проектирование.

Сервисы сопровождения

- Техническое сопровождение;
- Реагирование на инциденты;
- Консультации, сопровождение проверок.

ИТ-безопасность

- Внедрение надежных и стабильных средств технической защиты.

Оценка соответствия

- Аттестация по требованиям безопасности;
- Контроль эффективности.

Решение по обеспечению жизненного цикла ГИС

План мероприятий проекта по обеспечению комплексной информационной безопасности

1. Аудит информационной безопасности	
2. Организационные меры	
3. Технические меры	
4. Аттестация информационной системы	
5. Сопровождение аттестованной информационной системы	

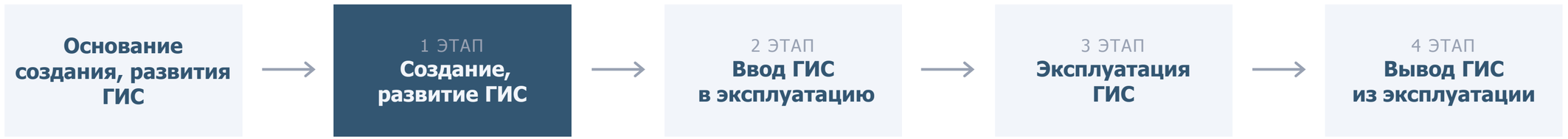
Жизненный цикл ГИС

Особенности

- Обязанность ОИВ по созданию системы, предусмотренная НПА;
- Решение ОИВ о создании системы с целью обеспечения реализации возложенных на него полномочий.

Жизненный цикл ГИС

Особенности



- Модель угроз и техническое задание согласуются с ФСТЭК России и ФСБ России;
- Техническое задание на создание и развитие системы должно включать требования по защите.

Жизненный цикл ГИС

Особенности

Основание создания, развития ГИС → 1 ЭТАП **Создание, развитие ГИС** → 2 ЭТАП **Ввод ГИС в эксплуатацию** → 3 ЭТАП **Эксплуатация ГИС** → 4 ЭТАП **Вывод ГИС из эксплуатации**

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»

Пункты 16.6, 17.2. Анализ уязвимостей при опытной эксплуатации системы защиты

Правовой акт о вводе системы в эксплуатацию должен включать мероприятия по подготовке должностных лиц к эксплуатации системы

Срок начала эксплуатации системы не может быть ранее срока окончания последнего мероприятия, предусмотренного правовым актом о вводе системы в эксплуатацию

Заявка на регистрацию должна содержать сведения об акте ввода в эксплуатацию и аттестации ИС. Одновременно с Заявкой представляются сами документы или их копии

Ввод ГИС в эксплуатацию

Особенности

Ввод системы в эксплуатацию не допускается в случаях:

а) невыполнение установленных законодательством РФ требований о защите информации, включая отсутствие действующего аттестата соответствия требованиям безопасности информации;

б) отсутствие в реестре территориального размещения объектов контроля, предусмотренном ПП675 (внесение реестровой записи согласно Приказу Министерства связи и массовых коммуникаций РФ от 7 декабря 2015 г. N 514 «Об утверждении порядка внесения сведений в реестр территориального размещения технических средств информационных систем и формы акта о выявленных несоответствиях сведений, содержащихся в реестре»);

в) невыполнение требований ПП N 676 в ходе осуществления контроля согласно ПП N 675 (внесение реестровой записи согласно Приказу Министерства связи и массовых коммуникаций РФ от 11 августа 2016 г. N 375 «Об утверждении порядка внесения сведений о выполнении требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, а также состава сведений, которые подлежат внесению, и срока их представления»).

Жизненный цикл ГИС

Особенности

Основание создания, развития ГИС → 1 ЭТАП **Создание, развитие ГИС** → 2 ЭТАП **Ввод ГИС в эксплуатацию** → 3 ЭТАП **Эксплуатация ГИС** → 4 ЭТАП **Вывод ГИС из эксплуатации**

Эксплуатация системы осуществляется в соответствии с рабочей документацией;

Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

Жизненный цикл ГИС

Особенности

Основание создания, развития ГИС → 1 ЭТАП **Создание, развитие ГИС** → 2 ЭТАП **Ввод ГИС в эксплуатацию** → 3 ЭТАП **Эксплуатация ГИС** → 4 ЭТАП **Вывод ГИС из эксплуатации**

Основания для вывода из эксплуатации

Завершение срока эксплуатации, если такой срок был установлен правовым актом о вводе системы в эксплуатацию;

Нецелесообразность эксплуатации (низкая эффективность, изменение правового регулирования, принятие управленческих решений);

Финансово-экономическая неэффективность.

Спасибо за внимание!
Вопросы?

Владислав Николаев

+7 (8352) 322-322 / доб. 187
+7 (917) 650-00-99
toptull@keysystems.ru

ООО «КСБ-СОФТ»

+7 (8352) 322-322
sec@keysystems.ru
ksb-soft.ru