КСБ-СОФТ

Комплексный подход к обеспечению безопасности информационных систем

Михаил Шипицын

Начальник отдела управления проектами

ООО «КСБ-СОФТ», CISA

Нормативно-правовые акты (для ГИС)

- Федеральный закон от 27 июля 2006 года № 149 «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства РФ от 6 июля 2015 г. № 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 6 июля 2015 г. № 675 «О порядке осуществления контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 Федерального закона «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства РФ от 11 мая 2017 г. № 555 «О внесении изменений в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
- Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Государственные информационные системы (ГИС)

Согласно ст. 2, 13, 14 149-ФЗ

- **Информационная система —** совокупность баз данных, а также технологий и технических средств для их обработки.
- **Государственные информационные системы** — федеральные и региональные информационные системы, созданные на основании федеральных и региональных законов и правовых актов государственных органов.

Создаются, модернизируются и эксплуатируются:

- в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами;
- с учетом требований законодательства о контрактной системе в сфере для государственных и муниципальных нужд;
- на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

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.

Зачем защищать ГИС

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	→	676-ПП
4. Отраслевые требования		
5. Киберугрозы		

Жизненный цикл ГИС

Согласно 676-ПП

Решение по обеспечению жизненного цикла ГИС

Консультации при согласовании МУ и ТЗ в органах ФСТЭК и ФСБ РФ

Консультации при эксплуатации ГИС

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

Подготовка обоснований, ТКП, региональных программ, проекта акта

Разработка ОРД по ИБ

Построение ПОИБ ГИС, аттестация ГИС

Подготовка проектов документов по эксплуатации ГИС

Подготовка обоснований, проекта акта

Постановление Правительства № 676

п. 15, разд. III «Требования к порядку ввода системы в эксплуатацию»

Ввод системы в эксплуатацию не допускается в случаях:

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

б) отсутствия в реестре территориального размещения объектов контроля, предусмотренном ПП № 675 (внесение реестровой записи согласно Приказу Министерства связи и массовых коммуникаций РФ от 7 декабря 2015 г. № 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) невыполнения требований ПП № 676 в ходе осуществления контроля согласно ПП № 675 (внесение реестровой записи согласно Приказу Министерства связи и массовых коммуникаций РФ от 11 августа 2016 г. № 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»).

Нормативно-правовые акты (для КИИ)

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Постановление Правительства РФ от 08 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
- Приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Приказ Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 №236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;
- Приказ Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 г. № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Информационное сообщение Федеральной службы по техническому и экспортному контролю от 4 мая 2018 г. № 240/22/2339 «О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации».

Перечень потенциальных сфер объектов КИИ

Потенциальные сферы объектов КИИ
• здравоохранение
• наука
• транспорт
• связь
• энергетика
• банковская и иные сферы финансового рынка
• топливно-энергетический комплекс
• атомная энергия
• оборонная и ракетно-космическая промышленность
• горнодобывающая, металлургическая и химическая промышленность

Что означает «категорирование объектов КИИ»?

1. **Определить процессы, осуществляемые в рамках вида деятельности**
2. **Выявить критические процессы**
3. **Определить объекты КИИ**
4. **Сформировать перечень объектов, подлежащих категорированию**
5. **Произвести оценку в соответствии с показателями критериев значимости**
6. **Определить для объекта КИИ категорию значимости**

С кем осуществляется взаимодействие при категорировании объектов КИИ?

Система безопасности значимого объекта КИИ

Реализация требований к ИБ включает в себя 5 базовых шагов:

1 **Формирование перечня применимых требований**
Включает в себя категорирование объекта КИИ (в соответствии с Постановлением Правительства № 127 от 08.02.2018 г.), а также требования по обеспечению безопасности, включаемые в ТЗ

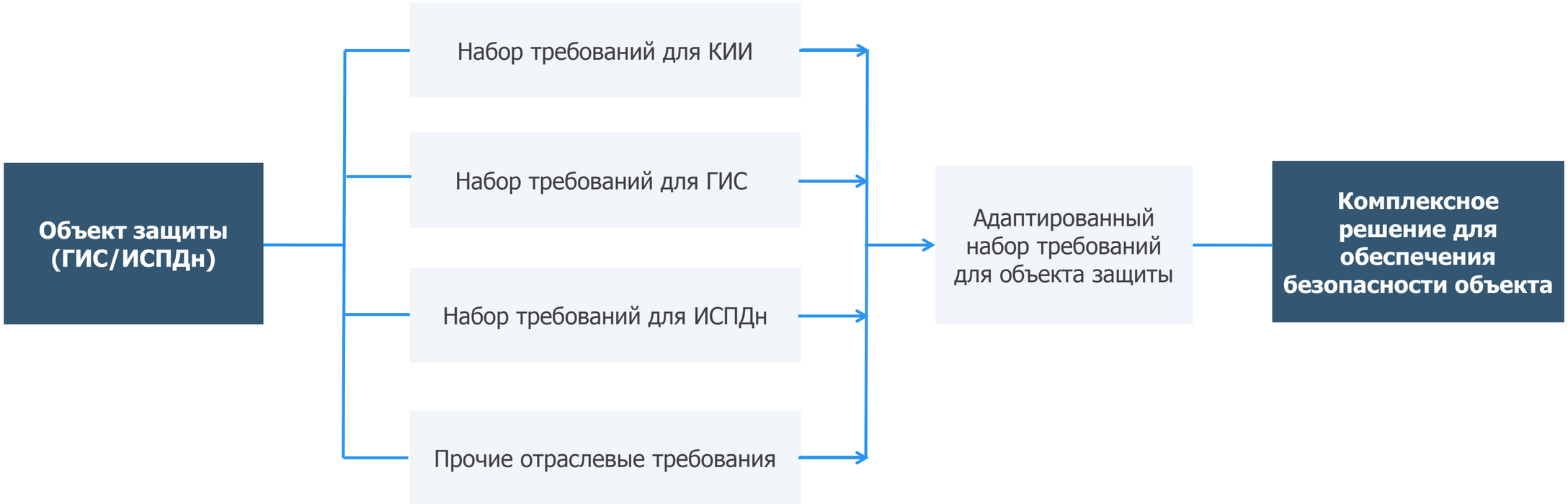
2 **Разработка организационных и технических мер**
- ✓ Моделирование угроз (по требованиям ФСТЭК)
- ✓ Проектирование системы безопасности
- ✓ Разработка эксплуатационной документации

3 **Внедрение организационных и технических мер по обеспечению безопасности**
- ✓ Установка и настройка средств защиты
- ✓ Разработка документов по безопасности объекта
- ✓ Предварительные испытания
- ✓ Опытная эксплуатация
- ✓ Выявление уязвимостей
- ✓ Приемочные испытания (для ГИС проводится аттестация)

4 **Обеспечение безопасности во время эксплуатации** + **Подключение к ГосСОПКА**

5 **Обеспечение безопасности при выводе из эксплуатации**

Система защиты ИС



КСБ-СОФТ

Организационное обеспечение юридически значимого документооборота

Внедрение модуля цифрового документооборота

Внедрение решения «Альфа-ЦДО» обеспечивает:

1. **централизацию электронного документооборота на уровне ведомства**
2. **обеспечение механизмов долговременного хранения электронных документов**
3. **взаимодействие с внешними системами доставки документов до адресата**
4. **интеграцию с системами бухгалтерского и управленческого учета**
5. **реализацию требований законодательства к системам электронного документооборота и системам хранения электронных документов в архивах государственных органов**

Возможности и результаты внедрения «Альфа-ЦДО»

- сопровождение документа метаданными о факте движения с подписью сервера;
- возможность усовершенствования усиленной квалифицированной электронной подписи (УКЭП);
- поддержка ряда сертифицированных клиентских и серверных криптопровайдеров и хранилищ ключей электронной подписи;
- возможность разбора конфликтных ситуаций для существующих ЭП;
- механизм визуализации формализованных и неформализованных документов;
- подсистема индексирования и полнотекстового поиска документов;
- предоставление информации по запросу контролирующих органов;
- подготовка рекомендаций по оптимизации документооборота.
- минимизация объема бумажного документооборота:
  - автоматизированный поиск необходимого документа;
  - ведение электронного каталога документов;
  - высвобождение площади, занимаемой архивом;
- повышение уровня достоверности и защиты данных, обрабатываемых в информационных системах финансового органа;
- снижение временных и финансовых затрат, связанных с документооборотом.

КСБ-СОФТ

SOC как инструмент для бесперебойной эксплуатации информационных систем

Что такое SOC

Security Operation Center (SOC) — комплекс решений и процессов, нацеленный на мониторинг, детектирование и оперативное реагирование на инциденты.

Что такое SOC

Security Operation Center (SOC) решает следующие проблемы:

- предотвращение киберпреступлений;
- выявление внутренних нарушений, связанных с халатностью или преднамеренными действиями сотрудников;
- повышение общего уровня защищенности инфраструктуры за счет выявления слабых и уязвимых мест;
- понимание общей картины инфраструктуры и её недостатков, инвентаризация активов;
- выполнение нормативных требований в области защиты информации;
- снижение репутационных, юридических и экономических рисков для организации .

Особенности работы SOC

Взаимодействие составляющих Security Operation Center (SOC):

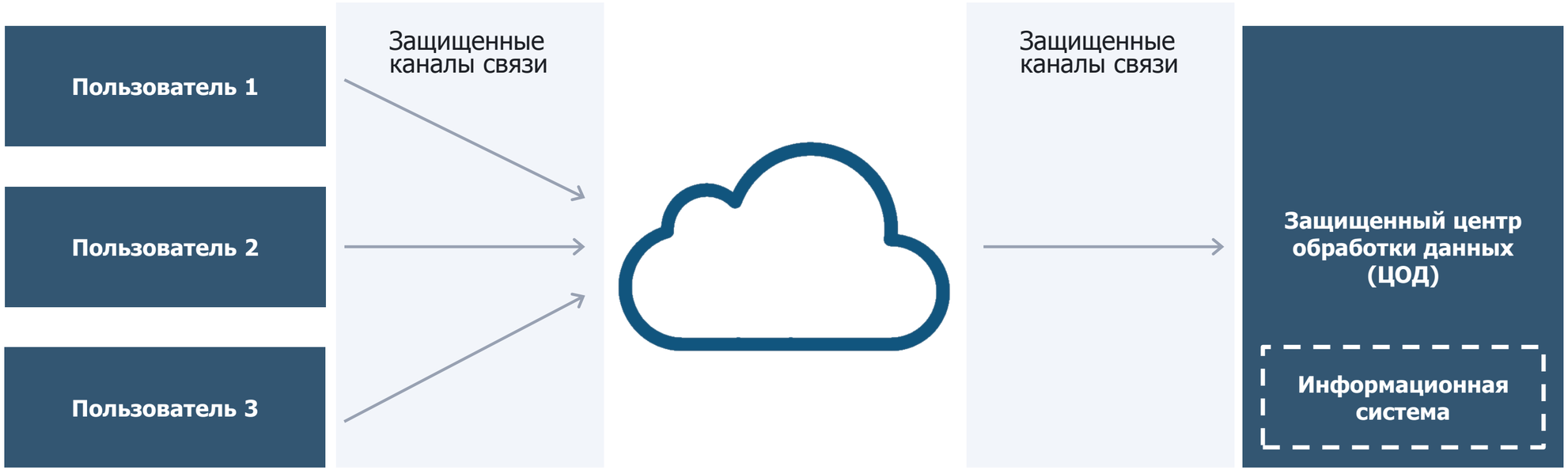
+ Периодическое тестирование безопасности
+ Периодическая отчетность по инцидентам
+ Координация действий службы ИБ организации

SOC как услуга

Преимущества использования «готовых» SOC:

- Экономия бюджетных средств;
- Выполнение требований законодательства в части обеспечения защиты информации и объектов КИИ;
- Реализация комплексных мер по обеспечению защиты информации в организации;
- Подключение объектов КИИ к ГосСОПКА.

Услуга отказоустойчивого защищенного ЦОД



+ Защищенная инфраструктура
+ Обслуживающий персонал
+ Резервирование технических средств
+ Бесперебойность
+ Стандартизированные регламенты обслуживания

Услуги для обеспечения безопасности ИС

В соответствии с Постановлением Правительства РФ от 28 ноября 2013 года № 1091 «О единых требованиях к региональным и муниципальным информационным системам в сфере закупок…» при создании и эксплуатации региональных и муниципальных систем должны выполняться требования по защите информации, обеспечению бесперебойной эксплуатации, а также требования в области использования электронной подписи, электронного документооборота, долговременного хранения информации.

Группа компаний «Кейсистемс» предлагает следующие продукты и услуги для решения данных задач:

- услуги по приведению государственных (муниципальных) информационных систем в соответствие с требованиями законодательства в области информационной безопасности;
- услуги по бесперебойной эксплуатации информационных систем (с возможностью предоставления услуг отказоустойчивого защищенного центра обработки данных);
- услуги по организационному обеспечению юридически значимого документооборота;
- внедрение модуля цифрового документооборота с возможностью долговременного хранения информации и интеграции с региональными информационными системами бухгалтерского (бюджетного) учета /облачными операторами электронного документооборота.

Спасибо за внимание!
Вопросы?

ООО «КСБ-СОФТ»

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