КСБ-СОФТ

Кибербезопасность медицинских организаций

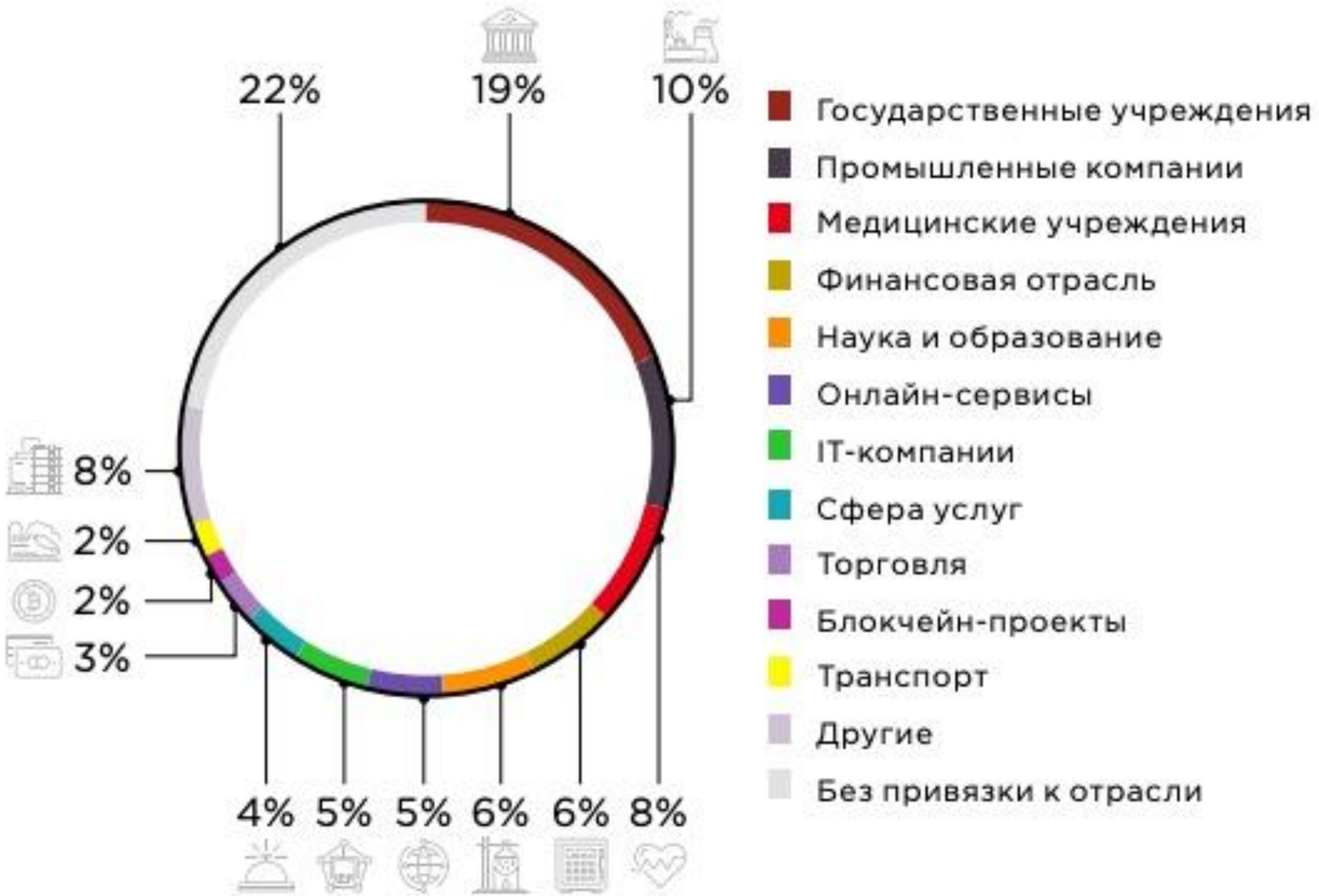
Федоров Иван

Заместитель генерального директора по развитию

ООО «КСБ-СОФТ», CISM, CGEIT, MBA

Актуальность

Сводная статистика по категориям атакуемых юридических лиц

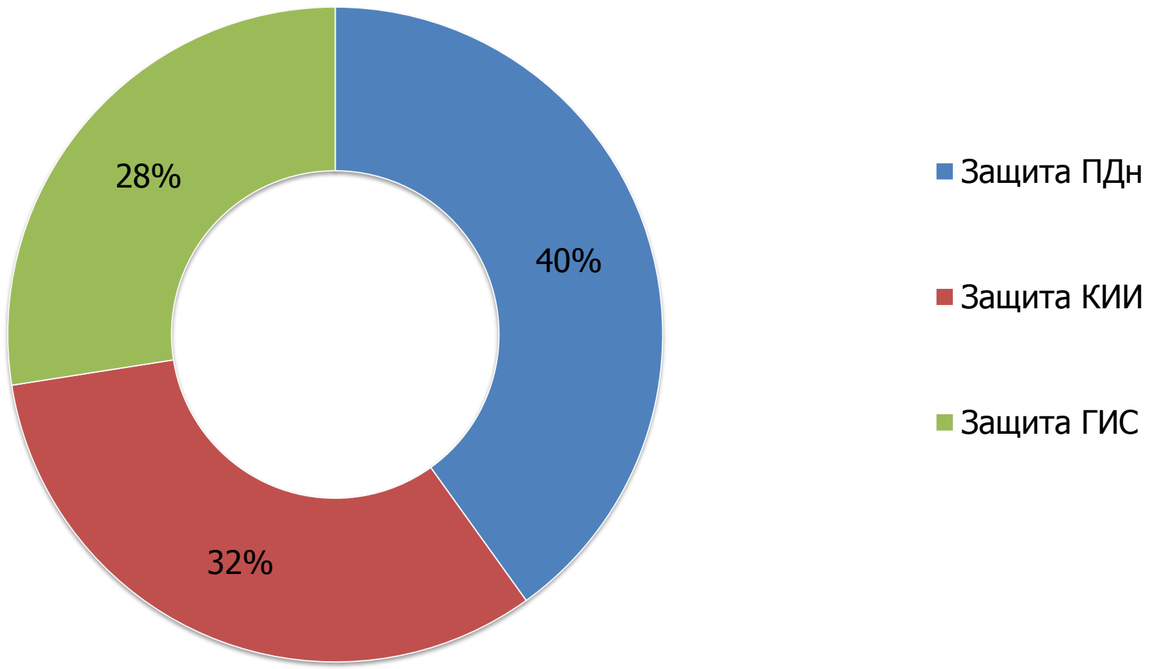


*По данным отчета компании Positive Technologies «Актуальные киберугрозы: II квартал 2019 года»

Актуальность

Результаты опроса

Аспекты, влияющие на актуальность вопросов информационной безопасности



КСБ-СОФТ

Безопасность персональных данных

Выполнение основных требований законодательства

- Назначение ответственных лиц
- Установление перечня ПДн
- Определение перечня сотрудников, имеющих доступ к ПДн
- Выполнение требований 687 ПП (при неавтоматизированной обработке ПДн)
- Выполнение требований 211 ПП (для операторов - госорганов)
- Ведение плана внутренних проверок режима обработки и защиты ПДн
- Формирование Политики в отношении обработки ПДн
- Определение уровня защищенности ПДн при их обработке в ИСПДн
- Определение угроз безопасности ПДн при их обработке в ИСПДн
- Отправка уведомления/информационного письма в Роскомнадзор
- Ознакомление работников с положениями законодательства о ПДн
- Наличие сертифицированных средств защиты информации и формуляров на них
- Выполнение комплекса мер по физической защите технических средств и носителей ключевой информации

Наиболее часто встречающие замечания

- ✓ Неопубликование оператором документа, определяющего Политику в отношении обработки ПДн

  РЕКОМЕНДАЦИЯ: выкладывайте Политику в отношении обработки ПДн на сайт организации на видное место, в т.ч. если используется сбор ПДн через онлайн-формы

- ✓ Отсутствие уведомления об обработке ПДн; Представление в уполномоченный орган уведомления об обработке персональных данных, содержащего неполные или недостоверные сведения; непредставление / несвоевременное предоставление сведений об изменении информации

  РЕКОМЕНДАЦИЯ: вовремя актуализируйте уведомление об обработке ПДн, отправляйте информационное письмо в Роскомнадзор в течение 10 рабочих дней с момента внесения изменений

Наиболее часто встречающие замечания

- ✓ Отсутствие условий соблюдения конфиденциальности ПДн в договорах с третьими лицами, а также требований к защите обрабатываемых ПДн

  РЕКОМЕНДАЦИЯ: в договоре должно быть прописано: с какой целью передаются ПДн другой компании, какие действия она будет совершать с ними, обязанность компании обеспечивать конфиденциальность и безопасность полученных ПДн. (см. ч.3 ст.6 ФЗ-152)

- ✓ Отсутствие у оператора места (мест) хранения ПДн (материальных носителей), перечня лиц, осуществляющих обработку ПДн, либо имеющих к ним доступ

  РЕКОМЕНДАЦИЯ: обеспечьте раздельное хранение документов, содержащих ПДн разных физических лиц; обеспечьте контролируемый доступ в помещения, в которых обрабатываются ПДн. В конце рабочего дня документы должны быть убраны в запираемые шкафы, сейфы

Наиболее часто встречающие замечания

- ✓ Невыполнение требований по обучению и ознакомлению сотрудников с порядком обработки, хранения ПДн и ответственностью за нарушение требований законодательства при обработке ПДн

  РЕКОМЕНДАЦИЯ: соберите все необходимые подписи сотрудников, которые работают с ПДн. Они должны ознакомиться под роспись с Политикой, положением, инструкцией ответственного, подписать обязательство о соблюдении конфиденциальности, согласие на обработку их ПДн

КСБ-СОФТ

Безопасность КИИ

Нормативно-правовые акты (для КИИ)

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Категорирование:

- Постановление Правительства РФ от 8 февраля 2018 г. № 127;
- Приказ ФСТЭК России от 22 декабря 2017 г. № 236;
- Информационное сообщение ФСТЭК России от 24 августа 2018 г. № 240/25/3752.

Взаимодействие с ГосСОПКА:

- Приказ ФСБ России от 24 июля 2018 г. № 367;
- Приказ ФСБ России от 24 июля 2018 г. № 368;
- Приказ ФСБ России от 06 мая 2019 № 196.

Обеспечение информационной безопасности:

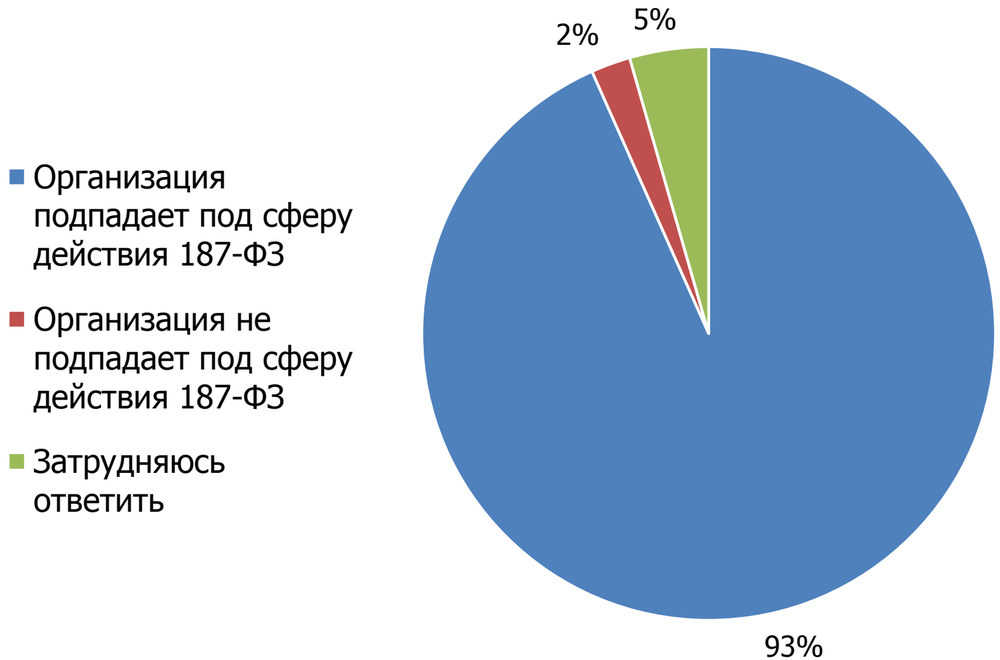
- Приказ ФСТЭК России от 21 декабря 2017 г. № 235;
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239.

Перечень потенциальных сфер объектов КИИ

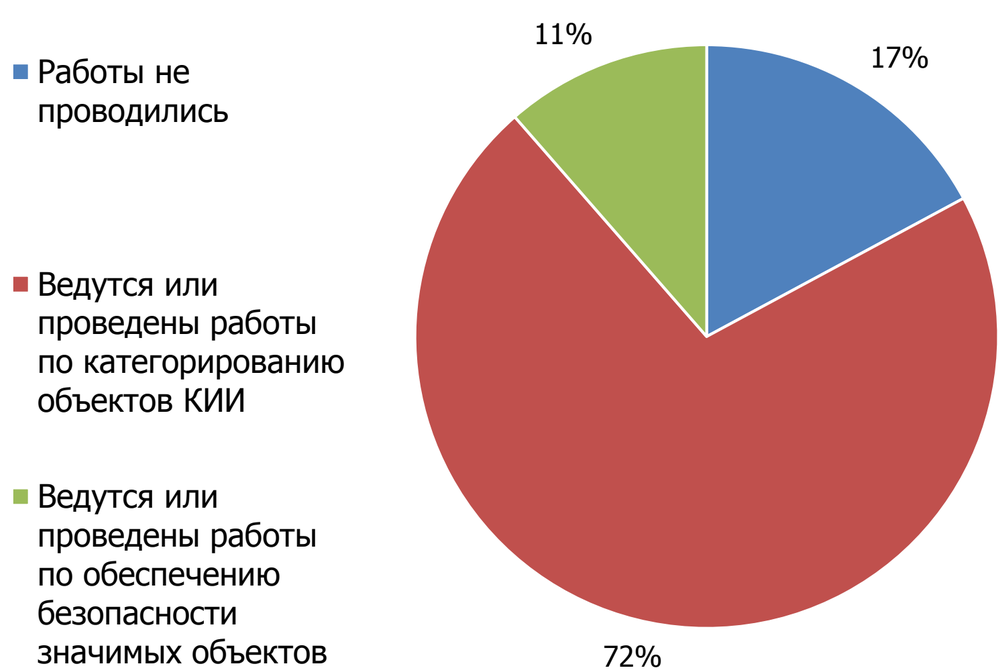
Потенциальные сферы объектов КИИ
• **здравоохранение**
• наука
• транспорт
• связь
• энергетика
• банковская и иные сферы финансового рынка
• топливно-энергетический комплекс
• атомная энергия
• оборонная и ракетно-космическая промышленность
• горнодобывающая, металлургическая и химическая промышленность

Результаты опроса

Организации, признавшие себя субъектами КИИ



Проведение работ, предусмотренных 187-ФЗ



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?

Особенности категорирования

- Уровень детализации процесса не регламентирован
- ФСТЭК России не согласовывает перечень объектов, подлежащих категорированию
- Для организаций с филиальной структурой перечень объектов предоставляется головной организацией
- По показателям нужны конкурентные значения, которые получаются в ходе расчетов
- Результаты категорирования нескольких объектов КИИ могут быть оформлены одним актом
- Рассматриваются наихудшие сценарии, учитывающие проведение целенаправленных компьютерных атак
- Сведения во ФСТЭК России направляются в печатном и электронном виде
- Объекту КИИ может быть не присвоена ни одна из категорий
- Акт категорирования рекомендуется формировать с учетом Приказа ФСТЭК России от 22 декабря 2017 г. № 236

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

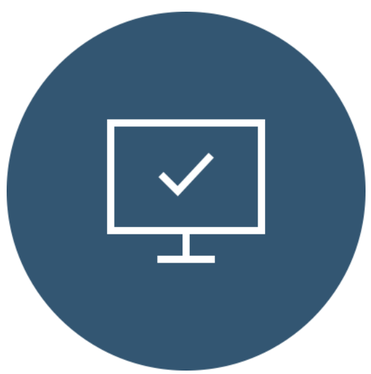
2 **Разработка организационных и технических мер**
- ✓ Моделирование угроз (по требованиям ФСТЭК)
- ✓ Проектирование системы безопасности
- ✓ Разработка эксплуатационной документации

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**

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 .

Взаимодействие с ГосСОПКА

Взаимодействие с ГосСОПКА

В случае самостоятельного подключения к ГосСОПКА:

- Обеспечить взаимодействие с НКЦКИ;
- Выполнить организационные и технические требования в соответствии с нормативными правовыми актами и методическими рекомендациями;
- Развернуть специализированные системы взаимодействия с технической инфраструктурой НКЦКИ (для значимых КИИ обязательно, остальным опционально).

В случае подключения через сторонний корпоративный сегмент:

- Заключить соглашение с корпоративным центром;
- Уведомить НКЦКИ о включении своих информационных ресурсов в зону ответственности корпоративного центра.

КСБ-СОФТ

Безопасность ГИС

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.

Жизненный цикл ГИС

Согласно 676-ПП

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;

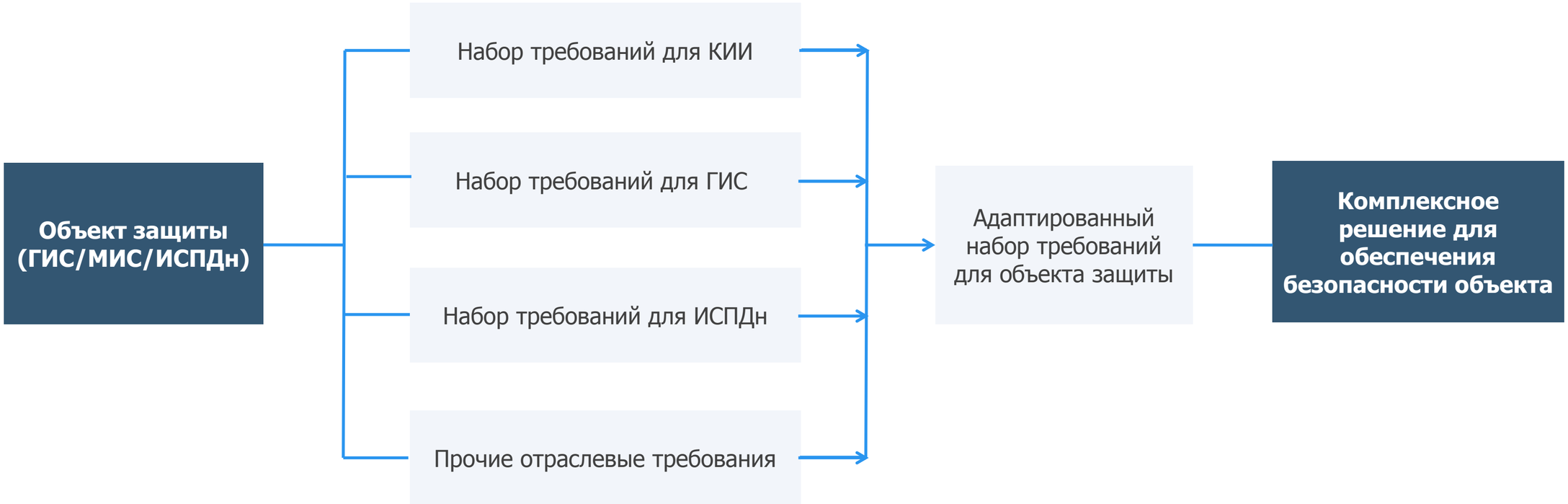
б) отсутствия в реестре территориального размещения объектов контроля, предусмотренном ПП № 675 (внесение реестровой записи согласно Приказу Министерства связи и массовых коммуникаций РФ от 7 декабря 2015 г. № 514 «Об утверждении порядка внесения сведений в реестр территориального размещения технических 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»).

Приказ ФСТЭК России № 17 от 11.02.2013

- Класс защищенности ГИС не должен быть выше класса защищенности ЦОД (дополнение в пункте 14.2)
- При моделировании угроз ГИС необходимо учитывать угрозы ЦОД (дополнение в пункте 14.3)
- При создании ГИС необходимо сформировать требования по защите информации в инфраструктуре ЦОД (дополнение в пункте 14.4)
- При проектировании системы защиты ГИС необходимо учитывать меры защиты информации, принятые в инфраструктуре ЦОД (дополнение в пункте 15.1)
- Средства защиты информации (СЗИ), устанавливаемые в ГИС, должны быть совместимы между собой, а также с СЗИ, установленными в ЦОД (дополнение в пункте 16.1)
- ЦОД должен быть аттестован на соответствие требованиям приказа ФСТЭК России № 17 не ниже класса защищенности, установленного для ГИС (уточнение в пункте 17.6)
- Главное изменение в части аттестации — срок действия аттестата — теперь он выдается на весь срок эксплуатации ГИС. Однако это не освобождает оператора от необходимости поддерживать систему защиты и инфраструктуру ГИС в соответствии с аттестатом, об этом говорится в пункте 17.4.
- Пункт 17.2 был дополнен замечанием о том, что, по решению заказчика (оператора ГИС), аттестационные испытания можно совместить с проведением приемочных испытаний информационной системы
- Появился новый пункт 18.6 об информировании и обучении персонала. Требования к обучению персонала теперь формализованы и установлена их периодичность: не реже 1 раза в 2 года
- С 1 июня 2020 года вступит в силу пятый абзац пункта о том, что используемые при проектировании ГИС СЗИ должны иметь сертификат ФСТЭК России по оценочному уровню доверия (ОУД)

Система защиты медицинских информационных систем (МИС)



Спасибо за внимание!
Вопросы?

ООО «КСБ-СОФТ»

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