Правовые аспекты ИБ с точки зрения специалиста по ИБ

ЗАДАНИЕ:

Задание является ситуационным, т.е. необходимо описать действия и инструкции для человека, попавшего в подобную ситуацию.

1. Опишите действия специалиста по Информационной безопасности, устроившегося на работу в государственную компанию, деятельность которой связана с медицинскими услугами (будем считать - что этот специалист - единственный специалист по ИБ в организации).

   Описать необходимо с точки зрения правовых аспектов!!! (что проверить, Что сделать в первую очередь, что во вторую, и т.д.)

   Данные о компании:

   В компании около 500 сотрудников
   Есть своя серверная, хранение критических данных происходит как на сетевом хранилище, так и на компьютерах пользователей.
2. Нарисовать схему взаимодействия специалиста ИБ с регуляторами ИБ. Отразить - какие документы необходимо предоставить специалисту в случае проверки организации

ОТВЕТ:

Если организация уже подключена к ГИС, то меры и средства защиты информации в ней проходили аттестацию согласно Приказу ФСТЭК РФ № 17 от 11.02.2013. Соответственно, специалисту по ИБ необходимо проверить соблюдаются ли эти меры с помощью локальных нпа, определённых законами и подзаконными актами.

При подготовке ГИС к аттестации был проведён следующий комплекс мероприятий (если организация ещё не подключалась к ГИС и наш специалист по ИБ первый сотрудник в этой компании, обеспечивающий осуществление требований законодательства в области защиты информации, то первым делом он выполняет данный комплекс действий):

- анализ информации и определение данных, подлежащих защите (здесь же определяем классы защищённости ИС);
- создание модели угроз;
- разработка технического задания с целью формирования конкретных требований к защите данных;
- исполнение требований законодательства в области защиты информации на объектах КИИ (согласно 187-ФЗ “О безопасности критической информационной инфраструктуры Российской Федерации” данная организация функционирует в сфере здравоохранения, а значит относится к объектам КИИ):
    - проведение категорирования объектов КИИ;
    - обеспечение интеграции в ГИС систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА) (согласно ПП РФ от 17.02.2019 №162 “Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ”);
    - принятие организационных мер по обеспечению безопасности объектов КИИ.

- исполнение требований законодательства в области защиты персональных данных;
- проектирование средств зи;
- непосредственная реализация защитных мер: построение сетевой структуры, защиты серверных и АРМ;
- разработка соответствующей правовой документации, включая приказы, распоряжения и акты по ГИС с целью ознакомления сотрудников с требованиями мер безопасности;
- аттестация.

ОБЪЕКТ КИИ:

Для того, чтобы выполнить требования 187-ФЗ, нужно:

- создать комиссию по категорированию (Приказ о создании комиссии в данном предприятии по категорированию объектов КИИ);
- определить и направить в ФСТЭК перечень объектов КИИ, утверждённый Информационным сообщением ФСТЭК от 24.08.2018 №240/25/3752 (Перечень объектов КИИ, подлежащих категорированию);
- провести анализ актуальных угроз;
- провести категорирование в соответствии с ПП №127 “Об утверждении Правил категорирования объектов критической информационной структуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений;
- составить акт результатов категорирования;
- направить сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Далее разрабатываются (или проверяются) следующий комплект документов (согласно 152-ФЗ, Приказы ФСТЭК №17,№21):

- правила учёта машинных носителей информации, содержащей ПДн;
- правила выявления информационных инцидентов и типовые правила реакции на них, приказ о создании группы реагирования на инциденты безопасности;
- правила резервирования и восстановления данных;
- приказ об уровнях допуска к ПДн, сопровождающийся возможностью ПО записывать логи;
- план периодического контроля и мониторинга;
- создание Политики безопасности, в которой содержатся предписания, определяющие:
    - правила и процедуры управления учётными записями пользователей;
    - правила и процедуры управления информационными потоками.

  Требования к:
    - используемым для зи организационным мерам;
    - условиям допуска пользователей и разграничения их полномочий;
    - техническим средствам;
    - средствам зи.

  К Политике безопасности создаются следующие приложения:
    - заявка на допуск пользователя к ИС или изменения объёма его полномочий;
    - положение о порядке разграничения прав доступа;
    - список лиц с указанием объёма их полномочий;
    - перечень правил пользования внешними сетями, электронной почтой и т.д. (требования ФСТЭК об управлении информационными потоками);

    - список разрешённых программных продуктов;
    - перечень пользователей, допущенных работать с системой на удалённом доступе;
    - порядок создания резервных копий конфиденциальной информации (152-ФЗ, ч.2 ст. 19);
    - план обеспечения непрерывности функционирования ИС (требования ФСТЭК о принятии мер по организации контроля безотказного функционирования технических средств).
- Приказ о назначении ответственных лиц, отвечающих за конфиденциальность ПДн (в этом же приказе прописываются должностные инструкции):
    - 152-ФЗ ст. 18.1 - необходимо назначить лицо, в чьи обязанности входит обеспечения сохранности ПДн и системного администратора, отвечающего за общие вопросы ИБ.
    - Приказ ФСТЭК №17 п.9 - необходимость наличия сисадмина.
- Инструкция пользователя.
- Приказ и положение о контролируемой зоне.
- План мероприятий по обеспечению безопасности информации (152-ФЗ ст. 18 аудит безопасности):
    - периодические мероприятия (по календарному плану);
    - разовые (инициированные внешними воздействиями).
- Журналы учёта:
    - жёстких дисков стационарных компьютеров;
    - винчестеров и иных носителей информации в портативных устройствах;
    - съёмных носителей.

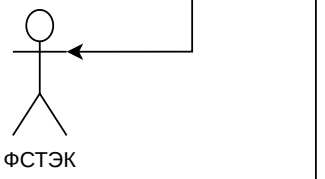
  Возможно создание одного журнала с учётом особенностей работы каждого типа носителя.
  + инструкция по заполнению журнала.

- Приказ о необходимости защиты информации (требование ФСТЭК о принятии решения о защите данных);
- Приказ о классификации ГИС;
- Приказ о вводе системы в действия (после успешных аттестации, испытаний, пробных запусков);
- Положение о защите ПНд, в нём указывается:
    - данные каких лиц и какой категории обрабатываются;
    - цели и методы обработки;
    - права субъектов ПДн;
    - обязанности оператора;
    - формат заполнения согласия на обработку ПДн и право на его отзыв;
    - порядок уведомления об изменении цели обработки и других существенных событиях.

  Положение должно находится в доступном месте.
- Правила рассмотрения запросов.
- Приказ об определении степени защищённости системы.

Если в данной организации применяются СКЗИ, то необходимо разработать (проверить следующие документы):

- Приказ о порядке хранения и эксплуатации средств криптографической защиты информации;
- Форма-перечень сотрудников, допущенных к работ с СКЗИ;
- Инструкция по обеспечению безопасности эксплуатации СКЗИ;
- Форма акта об уничтожении криптографических ключей и ключевых документов;
- Схема организации криптографической защиты информации.



ОБЩИЕ
Приказ о назначении ответственного за организацию обработки персональных данных и администратора безопасности информации
Инструкция администратора безопасности
Инструкция ответственного за организацию обработки ПНд
Приказ о назначении группы реагирования на инциденты ИБ и о правилах регистрации инцидентов ИБ и реагирования на них
Инструкция по реагированию на инциденты ИБ
Инструкция пользователя ГИС
Приказ об утверждении внутренних нормативных актов по ЗИ
Политика ИБ
Приказ об организации контролируемой зоны
Положение о контролируемой зоне
План мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищённости и выполнения мер по защите информации в ИС
Форма журнала учёта машинных носителей информации, стационарно устанавливаемых в корпус средств вычислительной техники.
Форма журнала учёта портативных вычислительных устройств, имеющих встроенные носители информации
Форма журнала учёта приёма/выдачи съёмных машинных носителей информации
Форма журнала учёта средств защиты информации
Форма журнала проведения инструктажей по ИБ
Форма журнала учёта мероприятий по контролю обеспечения ЗИ.

Схема 1. Общие нормативные акты, регулирующие обеспечение информационной безопасности на предприятии.

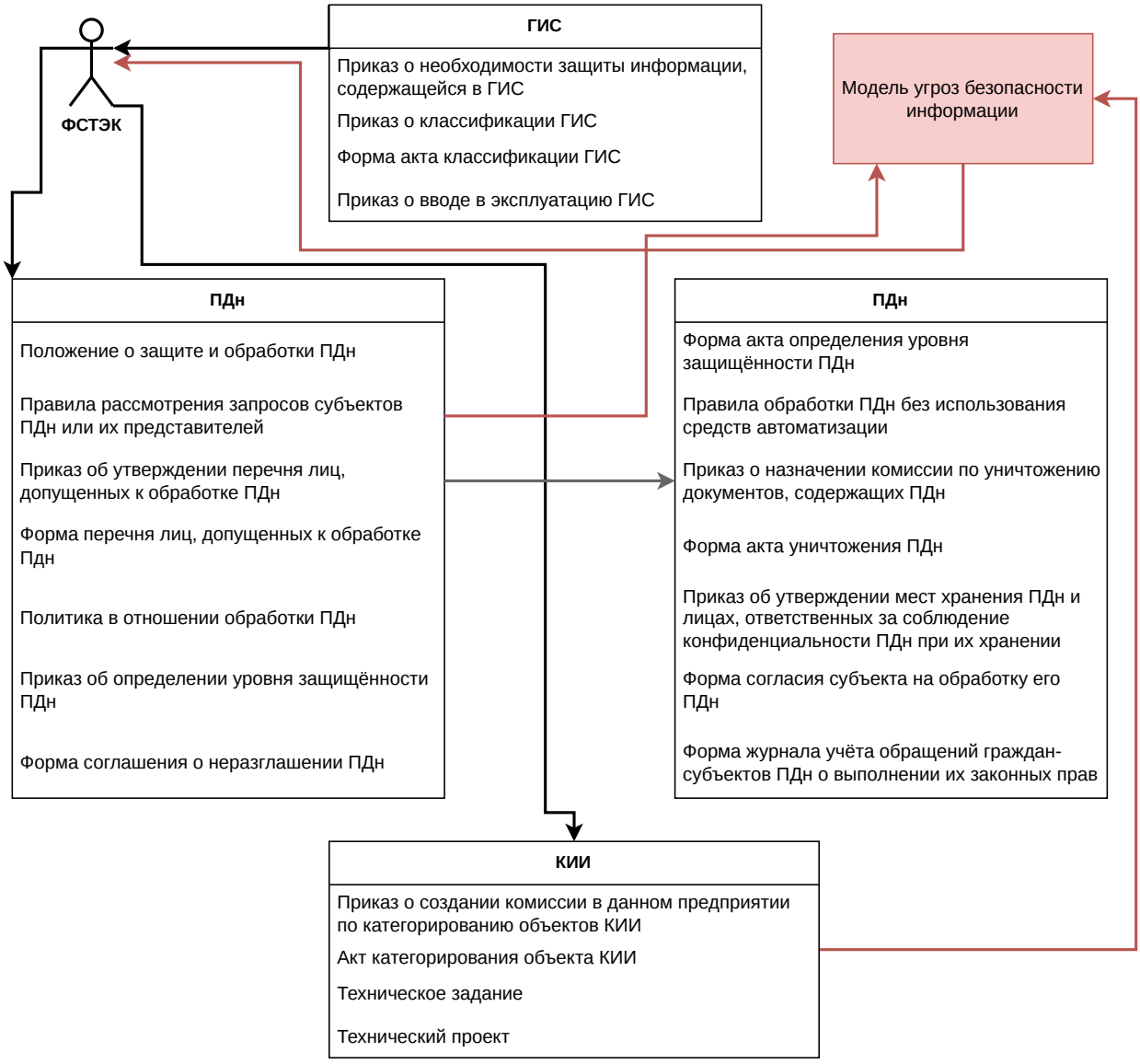


Схема 2. Специальные нормативные акты, регулирующие обеспечение информационной безопасности на предприятии.

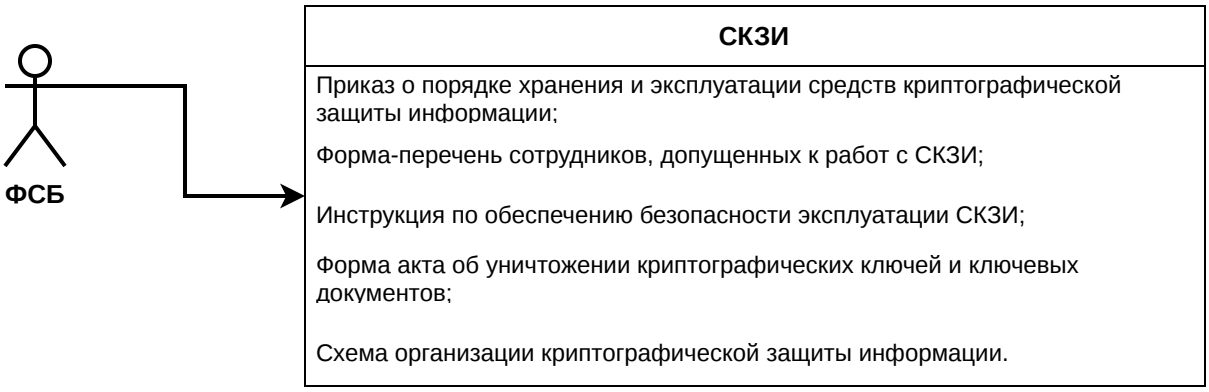


Схема 3. Специальные нормативные акты, регулирующие работу со СКЗИ.