

Самооценка готовности медучреждений к возможным проверкам со стороны регуляторов.

Организационно-технические аспекты защиты персональных данных в медицинских учреждениях

Левиев Дмитрий Олегович

эксперт

НОУ «Академия Информационных Систем»

Надзорные органы

1. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
2. ФСТЭК России
3. ФСБ России
4. Трудовая инспекция
5. Прокуратура

Порядок проведения плановых проверок

1. План проверок утверждается на год и доступен на сайте Генеральной Прокуратуры <http://www.genproc.gov.ru/>
2. Проверка несколькими надзорными органами в течении 1 года проводится совместно
3. Основанием включение в план проверок является выполнение любого из требований:
 1. Окончания срока предписания
 2. Прошло 3 года с момента последней проверки или регистрации юридического лица
 3. При наличии лицензий дополнительные условия:
 1. проверка через 1 год после получения лицензии
 2. проверка при переоформлении лицензии

Порядок проведения внеплановых проверок

1. Надзорный орган обращается с запросом в Прокуратуру за разрешением
2. На основании представленных сведений выносится решение Прокуратуры о проведении проверки
3. Проведение внеплановой проверки проводится в соответствии с 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»
4. Роскомнадзор имеет право в рамках своих полномочий запрашивать сведения, необходимые для выполнения своих государственных функций

Документы, запрашиваемые в ходе проверки

1. Учредительные документы Оператора
2. Копия уведомления об обработке персональных данных
3. Положение(я) о порядке обработки персональных данных;
4. Положение о подразделении, осуществляющем функции по организации защиты персональных данных;
5. Должностные регламенты лиц, имеющих доступ к персональным данным;
6. План мероприятий по защите персональных данных;
7. План внутренних проверок состояния защиты персональных данных;
8. Приказ(ы) о назначении ответственных лиц по работе с персональными данными;
9. Типовые формы документов, предполагающие или допускающие содержание персональных данных;

Документы, запрашиваемые в ходе проверки

10. Журналы, реестры, книги, содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях;
11. Договоры с субъектами персональных данных, лицензии на виды деятельности, в рамках которых осуществляется обработка персональных данных; выписки из ЕГРЮЛ, содержащие актуальные данные на момент проведения мероприятия по контролю (надзору);
12. Приказы об утверждении мест хранения материальных носителей персональных данных;
13. Письменное согласие субъектов персональных данных на обработку их персональных данных (типовые формы);
14. Распечатки электронных шаблонов полей, содержащие персональные данные; справки о постановке на балансный учет ПЭВМ, на которых осуществляется обработка персональных данных;

Документы, запрашиваемые в ходе проверки

15. Заключение экспертизы ФСБ России, ФСТЭК России об оценке соответствия средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке;
16. Приказ о создании комиссии и акты проведения классификации информационных систем персональных данных;
17. Журналы (книги) учета обращений граждан (субъектов персональных данных);
18. Акт об уничтожении персональных данных субъекта(ов) персональных данных (в случае достижения цели обработки);
19. Иные документы, отражающие исполнение Оператором требований законодательства Российской Федерации в области персональных данных

ПДн работников

1. Все ПДн получают у самого работника
2. При невозможности получения у работника – письменное согласие на получение у третьей стороны и последствия отказа от дачи согласия
3. Не основываться при принятии решения исключительно на автоматизированной обработке или электронного получения
4. Работник должен быть ознакомлен под роспись с локальными нормативными актами порядка обработки персональных данных
5. Работники не должны отказываться от своих прав на сохранение и защиту тайны
6. Работодатель обязан не сообщать персональные данные работника в коммерческих целях без его письменного согласия

ПДн медработников

1. Потребитель (пациент) имеет право получать информацию о квалификации медперсонала и уровне его подготовки в части оказания медицинских услуг, а также обеспечение права безопасности оказываемой услуги
2. Распространение ПДн работников в коммерческих целях возможно только с письменного согласия работника
3. Порядок обработки персональных данных медработников определяется внутренним нормативным актом работодателя

Особенность обработки ПДн медперсонала

1. При распространении ПДн медперсонала рекомендуется указывать:
 1. Полное ФИО
 2. Квалификация, включая переподготовку
 3. Часы приема или порядок оказания медицинской услуги
2. Не рекомендуется указывать при распространении ПДн медперсонала:
 1. Нахождение в отпуске
 2. Нахождение на больничном (при любом основании)

Трудовой договор с медперсоналом

1. В обязательном порядке содержит сведения о порядке обработки ПДн медработника, включая порядок распространения его ПДн (ссылка на внутренний нормативный документ работодателя)
2. Письменное согласие работника на распространение его персональных данных в целях выполнения трудовых обязанностей и защиты интересов потребителя (пациента) оформленного в соответствии с требованиями Федерального закона «О персональных данных»
3. Обработка персональных данных работника после его увольнения в целях защиты интересов потребителя медицинской услуги (пациента)

Обработка ПДн соискателя

1. Необходимо получать согласие на обработку персональных данных соискателя
2. Необходимо разработать и утвердить локальный нормативный акт о порядке обработке персональных данных соискателей и должностные инструкции для ответственных за прием работников
3. Возможна разработка договора-оферты для соискателя, регламентирующего порядок обработки ПДн
4. На основании Федерального закона «О персональных данных» внести сведения об обработке ПДн соискателя в уведомление

Неавтоматизированная обработка ПДн

1. Проверка комплекта внутренних нормативных документов организации о порядке неавтоматизированной обработки персональных данных:
 1. Политики (рекомендуется)
 2. Положения
 3. Регламенты
 4. Порядки
 5. Должностные инструкции
 6. Типовые формы документов

Неавтоматизированная обработка ПДн

2. Определение мест хранения и мер по защите от несанкционированного доступа
3. Ревизия договорных отношений с охранными предприятиями
4. Определение порядка передачи материальных носителей ПДн
5. Определение порядка учета материальных носителей ПДн
6. Назначение ответственных лиц

Передача ПДн для обработки

1. Передача ПДн для обработки осуществляется только на основании договора, существенным условием которого является обеспечение конфиденциальности ПДн субъекта
2. В договоре должен быть определены: цель обработки ПДн, порядок передачи персональных данных, способы обработки, условия возвращения материальных носителей ПДн или уничтожения ПДн
3. Передача ПДн осуществляется только с согласия субъекта, если иное не установлено федеральным законом

Передача биометрических ПДн

1. В организации должен быть разработан внутренний нормативный документ о передаче биометрических ПДн
2. При получении биометрических ПДн необходимо получать согласие от субъекта на передачу и обработку ПДн у Уполномоченного лица
3. Передача биометрических ПДн осуществляется только на основании договора
4. Порядок передачи биометрических ПДн должен быть закреплён в договоре
5. Необходимо рассматривать возможность обезличенной передачи биометрических ПДн

Медицинская документация

1. Владелец информации в медицинской документации является субъект – пациент!
2. Порядок обращения медицинской документации определяется действующим федеральным законодательством РФ и решением субъекта
3. Доступ к медицинской документации внутри организации должен быть регламентирован внутренним нормативным актом

Контроль за движением карты пациента

1. Пациент имеет право бесплатного неограниченного доступа к своим ПДн, в том числе в карте пациента во время обращения в ЛПУ в доступной форме
2. Доступ к карте пациента имеет:
 1. сам пациент
 2. законный представитель пациента(с нотариальной доверенностью)
 3. медицинские работники для постановки диагноза и оказания медицинских и медико-социальных услуг при соблюдении требований к врачебной тайне
 4. официальные опекуны недееспособных субъектов
 5. наследники субъекта
 6. уполномоченные органы в рамках своих полномочий
 7. на основании решения суда, вступившего в законную силу

Контроль за движением карты пациента

3. ЛПУ обязано обеспечить конфиденциальность сведений, указанных в карте пациента
4. ЛПУ обязано обеспечить доступность карты пациенту, в том числе сохранность сведений указанных в карте
5. Необходимо фиксировать перемещение карты, включая выдачу карты пациенту, контролирующим органам и т.п.

Построение технической защиты ИСПДн, обрабатывающей ПДн работников

1. На базе общего подхода с использованием документов ФСТЭК России:
 1. Методика определения актуальности угроз
 2. Базовая модель угроз
2. На базе отраслевых документов по защите ПДн в типовых медицинских информационных системах
 1. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости
 2. Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости

Построение технической защиты ИСПДн, обрабатывающей ПДн работников

2. На базе отраслевых документов по защите ПДн в типовых медицинских информационных системах
 1. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости
 2. Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости
 3. Модель угроз типовой МИС типового ЛПУ

Защита персональных данных в МИС

1. Разработать и утвердить внутри ЛПУ приказ о защите персональных данных
2. Разработать и утвердить внутри ЛПУ приказ о подразделении по защите персональных данных
3. Разработать и утвердить внутри ЛПУ приказ о назначении ответственных лиц за обработку персональных данных
4. Разработать и утвердить внутри ЛПУ Политику информационной безопасности
5. Разработать и утвердить внутри ЛПУ приказ о проведении внутренней проверки
6. Определить состав и категории обрабатываемых персональных данных и оформить в виде Перечня ПДн
7. Осуществить классификацию действующих информационных систем, обрабатывающих персональные данные (акт классификации ИСПДн)

Защита персональных данных в МИС

8. Разработать и утвердить внутри ЛПУ положение о разграничении прав доступа к обрабатываемым персональным данным
9. Частная модуль угроз к конкретной ИСПДн ЛПУ
10. Разработать и утвердить план мероприятий по защите ПДн
11. Назначить ответственных за защиту ПДн в ЛПУ
12. Разработать организационно-распорядительные документы по резервированию и восстановлению работоспособности МИС
13. Разработать и утвердить журнал обращений субъектов в ЛПУ

Защита персональных данных в МИС

14. Выполнить установку технических средств защиты информации
15. Выполнить аттестацию или декларацию соответствия всех ИСПДн
16. Разработать и утвердить план внутренних проверок состояния защиты ПДн в ЛПУ
17. Направить уведомление в Роскомнадзор по территориальному признаку

Лицензирование деятельности для уполномоченного органа

1. Лицензия ФСТЭК России на Техническую защиту конфиденциальной информации (99-ФЗ)
2. Лицензия ЦЛСЗ ФСБ России на осуществление оказания услуг шифрования* (99-ФЗ)
3. Лицензия ЦЛСЗ ФСБ России на осуществление распространения шифровальных (криптографических) средств* (99-ФЗ)
4. Лицензия ЦЛСЗ ФСБ России на осуществление технического обслуживания шифровальных (криптографических) средств* (99-ФЗ)
5. Использование сертификатов ключей шифрования и подписи Аккредитованных Удостоверяющих центров для квалифицированной подписи (ФЗ-63 «Об Электронной подписи»)

Контакты

Левиев Дмитрий Олегович

Эксперт

Академия Информационных Систем

Тел./факс +7 495 231-3049

E-mail dleviev@infosystem.ru

<http://www.infosystems.ru>