Методическое пособие по выполнению требований

Федерального закона №152 «О персональных данных»

Комплексная защита
Персональных данных

Разработано: *Центром информационной безопасности.*

2009

Содержание

Требования законов в области защиты Персональных данных.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Ст. 3 Федерального закона №152-ФЗ
«О персональных данных» от 27.07.2006

В наиболее общем случае персональные данные в медицинском учреждении это:

- Данные кадрового учета;
- Информация о физических лиц;
- Информация о клиентах и посетителях;
- Данные статистического учёта;
- Экспертные системы анализа.

Во всех подобных случаях Закон однозначно обязывает Вас принимать меры по защите персональных данных независимо от формы собственности и размера Вашего предприятия.

Требования законодательства

«Операторы при обработке данных обязаны принимать необходимые организационные и технические меры, в том числе шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним».

Федеральный закон №152-ФЗ «О персональных данных» от 27.07.2006.

«Операторами» в соответствии с Законом, являются: государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Таким образом:

«Информационные системы персональных данных, созданные до дня вступления в силу настоящего Федерального закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона ***не позднее 1 января 2010 года****»*

Федеральный закон №152-ФЗ «О персональных данных» от 27.07.2006.

Это означает, что до 1 января 2010 года все мы с Вами обязаны модернизировать наши компьютеры, локальные, корпоративные сети и программное обеспечение средствами для обеспечения безопасности персональных данных

Далее, постановлением Правительства РФ от 17 ноября 2007г. «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» утверждено положение, согласно которому «*методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности РФ в пределах их полномочий*».

Таким образом, на ФСТЭК и ФСБ России возложена часть функций контроля исполнения Закона. Основная функция по контролю за юридической защитой персональных данных

возложена на Россвязькомнадзор, **который уже начал проводить проверки в Алтайском крае.**

Требования Закона распространяются **на все государственные и коммерческие организации,** независимо от их размера и рода деятельности.

Ответственность

Если же мы с Вами невыполняем эти требований, то Закон считает это нарушением или даже ПРЕСТУПЛЕНИЕМ. Невыполнение требований Закона может привести к крайне негативным последствиям.

Ответственность за нарушения в области защиты персональных данных закреплена как в Административном, так и в Уголовном кодексах РФ:

«Нарушение установленного законом порядка сбора, хранения, использования и распространения информации о гражданах персональных данных»

Ст.13.11. Кодекса об административных правонарушениях РФ.

«Нарушение неприкосновенности частной жизни»

Ст.137. Уголовного кодекса РФ.

Порядок действий по защите персональных данных.

Информации о том, что же делать предприятиям (организациям) и какие меры предпринимать много – Законы, Постановления, письма и т.п.

К сожалению, информация разрознена и находится в достаточно неудобном для неспециалиста виде.

Мы постарались собрать и упорядочить информацию так, чтобы Вам было понятно, что делать сегодня, что завтра, что затем.

В **общем случае** перечень действий, которые необходимо произвести для защиты персональных данных, выглядит следующим образом:

а) *До конца 2008 года всем операторам персональных данных необходимо зарегистрироваться (направить уведомление в соответствующий орган). Т.е. Вам необходимо пройти процедуру регистрации.*
Занимается такой регистрацией «Федеральная служба по надзору в сфере массовых коммуникаций», которая с 25 октября 2007 года и осуществляет прием уведомлений о намерении осуществлять обработку персональных данных.

В Приложении №1 и №2 приведены шаблон стандартного бланка-уведмления о намерении осуществлять обработку персональных данных и рекомендации по его заполнению.

Уведомления необходимо направлять по территориальному признаку по следующим адресам:

- ***Управление Россвязькомнадзора по Республике Алтай***
  Коммунистический проспект, д.61, г. Горно-Алтайск, 649006
  gssdc04@mail.gorny.ru;
- ***Управление Россвязькомнадзора по Алтайскому краю***
  Интернациональная ул., д.72, г. Барнаул, 656049
  22_office@ufsns22.ab.ru;

После регистрации Вы сможете увидеть свою организацию в списке

зарегистрированных операторов на сайте ***pd.rsoc.ru***

Нарушение этих требований ведет к наказанию: от штрафа до прекращения деятельности организации.;

б) В соответствии с тройственным приказом № 55/ 86/ 20ФСБ России, ФСТЭК России и Мининформзвязи России необходимо проклассифицировать АС и утвердить внутренним приказом акт классификации; (Приложение №3)

в) Проверка соответствия организационно технических мер защиты требованиям руководящих документов ФСТЭК и ФСБ;

г) Разработка недостающей организационно распорядительной документации, описание системы защиты и обработки персональных данных.

д) Установка и ввод в эксплуатацию средств защиты информации в соответствии с руководящей и технической документацией;

е) Проведение специальных исследований на объекте (является не обязательной для операторов 3 класса);

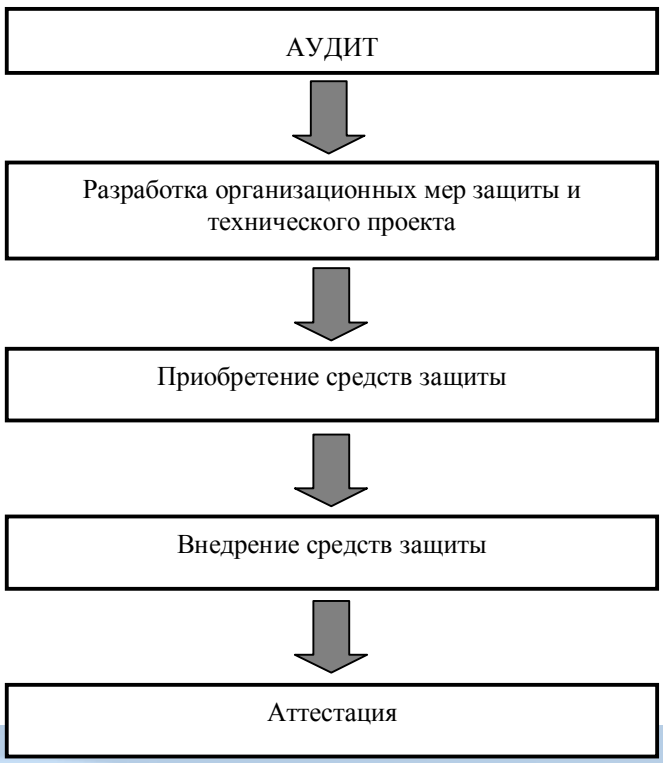
ж) Аттестация. Проведение комплексных испытаний. Оценка результатов испытаний и выдача рекомендаций по обеспечению защищенности информации на аттестованных объектах. Оформление документов по результатам аттестационных испытаний и выдача аттестата соответствия ОИ требованиям по безопасности информации; (является не обязательной для операторов 3 класса)

Законы РФ однозначно обязывают Вас принимать меры по защите персональных данных. Эта обязанность возлагается на ВСЕ предприятия и организации, независимо от формы собственности и размера.

Другими словами, защищать персональные данные должны и Пенсионный фонд России, и районная поликлиника, и частное кредитное агентство.

Услуги по выполнению требований законодательства, помогающие успешно пройти проверки регуляторов!

Центр информационной безопасности готов в 5 этапов помочь вам выполнить все требования регуляторов! Схематично это выглядит так:



1. Аудит информационной безопасности

Является способом получения объективных качественных и количественных оценок текущего состояния информационной безопасности организации и их соответствие требованиям ФСТЭК, ФСБ по защите конфиденциальной информации и персональных данных.

Основными **целями** проведения аудита информационной безопасности в организации являются:

– анализ текущего состояния всех автоматизированных систем (АС), подготовка материалов для разработки необходимых организационно-распорядительных документов («Перечня сведений, подлежащих защите», формуляров ресурсов (АРМ, задач, программных средств) и списков пользователей для включения в «Планы защиты» конкретных подсистем АС и т.д.);

– сбор и подготовка данных для оценки эффективности применяемых мер и средств защиты информации (организационных, физических, технических) в подразделениях и разработки предложений и рекомендаций по совершенствованию системы защиты информации от НСД в конкретных подсистемах АС.

Основными задачами аудита информационной безопасности являются:

*анализ, систематизация и уточнение данных об автоматизированных системах, имеющихся организационно-распорядительных документов по вопросам обеспечения информационной безопасности в подразделении, применяемых мерах и средствах обеспечения защиты информации и других сведений, касающихся организации безопасности информации в АС;

* классификация АС

*инвентаризация в подразделении всех имеющихся автоматизированных рабочих мест подсистемы, всех решаемых в подразделениях с использованием автоматизированной системы функциональных задач, всех видов информации, циркулирующей, хранимой, обрабатываемой, передаваемой, принимаемой и т.д. в подсистемах (подразделениях);

* анализ состава и характеристик технических и программных средств, технологии обработки и передачи информации в подсистеме;

* анализ топологии, состава и характеристик технических и программных средств телекоммуникации подсистемы АС;

* анализ информационных потоков (входящих, исходящих и циркулирующих внутри) в подсистеме АС;

* выявление возможных путей реализации значимых угроз информационной безопасности, возможных каналов несанкционированного доступа к ресурсам подсистемы АС с целью нарушения ее работоспособности или доступа к защищаемой информации;

* анализ существующего порядка допуска сотрудников подразделения к работе с подсистемой АС и определения их полномочий по доступу к ресурсам подсистемы;

* анализ существующего порядка разработки, приобретения, установки и обновления программных средств на АРМ подсистемы АС;

* анализ существующего в подразделении порядка приобретения, установки, ремонта и замены технических средств АС;

* анализ состояния и оценка эффективности применяемых мер и средств защиты информации в подсистеме АС (организационных, физических, технических и программных).

В результате проведения аудита информационной безопасности должны быть получены:

- сводная таблица характеристик автоматизированных систем организации, как объектов защиты;
- классификация автоматизированных систем, осуществляющих обработку персональных данных.
- анализ выполнения требований по защите информации в автоматизированных системах организации;
- перечень персональных данных и конфиденциальной информации, обрабатываемой в автоматизированных системах;
- список организационно-распорядительных документов по защите конфиденциальной информации и персональных данных;
- рекомендуемые меры по формированию режима информационной безопасности в автоматизированных системах.

2. Разработка организационных мер защиты, документации по защите информации и технического проекта

Для выполнения требованиям ФСТЭК, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, ФСБ необходимо разработать следующие документы:

– Политика безопасности;
– Перечень конфиденциальных сведений;
– Обязательство о неразглашении конфиденциальных сведений;
– Инструкция по обращению с носителями конфиденциальной информации;
– Модель нарушителя;
– Модель угроз;
– Техническое задание на АС;
– Частное техническое задание на СЗИ АС;
– Технический паспорт АС;
– Описание технологического процесса обработки информации в АС;
– Инструкция ответственного за эксплуатацию объекта информатизации;
– Инструкция администратора безопасности АС;
– Инструкция по работе пользователей в АС;
– Инструкция по проведению антивирусного контроля в АС;
– Инструкция о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав объекта информатизации;
– Инструкция по использованию средств защиты информации, установленных на объекте информатизации;
– Список лиц, имеющих доступ в помещения, в которых расположены объекты информатизации;

– Список постоянных пользователей АС и установленные им права доступа к информационным и техническим ресурсам. Матрица доступа;
– Перечень разрешенного к использованию в АС программного обеспечения.
– Журналы учёта и приказы.

3. Приобретение средств защиты

Закупка СЗИ от НСД, средства межсетевого экранирования, антивирусной защиты и др. программное обеспечение, позволяющее выполнить обязательные требования*:*

Требования (мероприятия)
1. Подсистема управления доступом
1.1. Идентификация и проверка подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.
1.2. Идентификация терминалов, компьютеров, узлов сети ИСПДн, каналов связи, внешних устройств компьютеров по их логическим именам и (или) адресам.
1.3. Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.
1.4. Контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.
1.5. Управление потоками информации с помощью меток конфиденциальности, при этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации.
1.6. ***Межсетевое экранирование*** *при подключении к сетям общего пользования должно обеспечивать.*
1.6.1. Фильтрация для каждого сетевого пакета независимо.
1.6.2. Идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ.
1.6.3. Идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.
1.6.4. Регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова.
1.6.5. Контроль целостности своей программной и информационной части.
1.6.6. Фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.
1.6.7. Фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов.
1.6.8. Фильтрацию с учетом любых значимых полей сетевых пакетов.
1.6.9. Восстановление после сбоев и отказов оборудования.
1.6.10. Регламентное тестирование реализации правил фильтрации, процесса идентификации, аутентификации и регистрации действий администратора МЭ.
1.6.11. Контроль целостности программной и информационной части МЭ.
1.6.12. Восстановления после сбоев и отказов.
1.6.13. Возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети.
1.6.14. Возможность трансляции сетевых адресов.
1.6.15. Дистанционную сигнализацию попыток нарушения правил фильтрации.
1.6.16. Регистрацию и учет запрашиваемых сервисов прикладного уровня.
1.6.17. Программируемую реакцию на события в МЭ.
1.6.18. Идентификацию и аутентификацию администратора МЭ при его запросах на доступ по идентификатору (коду) и паролю временного действия.

1.6.19. Блокирование доступа неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась, методами, устойчивыми к пассивному и активному перехвату информации.
2. Подсистема регистрации и учета
2.1. Регистрация входа (выхода) субъекта доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова.
2.2. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. *(В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная – несанкционированная), идентификатор (код и фамилия) субъекта, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке).*
2.3. Регистрация выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности, спецификация устройства выдачи - логическое имя (номер) внешнего устройства, идентификатор субъекта доступа, запросившего документ.
2.4. Регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задачи), идентификатор субъекта доступа, запросившего программу (процесс, задание), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный – несанкционированный), должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого файла.
2.5. Регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров в составе ИСПДн, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого объекта – логическое имя (номер).
2.6. Регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются дата и время изменения полномочий, идентификатор субъекта доступа (администратора), осуществившего изменения.
2.7. Учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).
2.8. Автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта.
2.9. Учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал (учетную карточку), учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).
2.10. Проведение нескольких видов учета (дублирующих) защищаемых носителей информации.
2.11. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, ранее использованную для хранения защищаемой информации.
2.12. Сигнализация попыток нарушения защиты.
3. Подсистема обеспечения целостности:
3.1. Обеспечена целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации..

3.2. Осуществляется физическая охрана ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации, особенно в нерабочее время.
3.3. Периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД.
3.4. Наличие средства восстановления средств защиты информации в составе СЗПДн, предусматривающих ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности.
3.5. Проведение резервного копирования ПДн на отчуждаемые носители информации.
3.6. Проведение проверки целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм.
3.7. Восстановление средства защиты от ПМВ, предусматривающие ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности.
3.8. Реализация механизмов проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм.
3.9. Наличие администратора (службы) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы средств защиты информации в составе СЗПДн.
3.10. Использование сертифицированных средств защиты.
4. Подсистема антивирусной защиты
4.1. Автоматическая проверка на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа.
4.2. Наличие механизмов автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения.
4.3. Регулярная проверка (при первом запуске средств защиты ПДн от ПМВ и с устанавливаемой периодичностью) на предмет наличия в них ВП.
4.4. Автоматическая инициация проверки ИСПДн на предмет наличия ВП при выявлении факта ПМВ.
4.5. Наличие механизма отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.

4. Внедрение средств защиты

Данный этап выполняется специалистами, прошедшими обучение и получившими сертификаты на выполнение данного спектра работ, которые не только выполнят пусконаладочные работы но ещё и проведут обучение вашего персонала работе с данным комплексом.

5. Аттестация.

1	Проведение специальных исследований на объекте:
	ПЭВМ (в составе системный блок, клавиатура, мышь)
	принтер
	сканер
2	Анализ представленных документов, определяющих состав и порядок эксплуатации ОИ, принятие решения по выполнению технических мер и организационно-технических требований по защите информации.
3	Подготовка и согласование программы-методики аттестационных испытаний.
4	Проведение комплексных испытаний. Оценка результатов испытаний и выдача рекомендаций по обеспечению защищенности информации на аттестованных объектах. Оформление документов по результатам аттестационных испытаний и выдача аттестата соответствия ОИ требованиям по безопасности информации.

Антикризисное предложение! Провайдер безопасности!

Только до конца 2009 года! Действует специальное предложение!

Наша компания готова заключить с вами комплексный договор по выполнению требований Федеральных законов с рассрочкой платежей!

Звоните, пишите, приезжайте…
Мы рады Вам!

А также вы можете звонить на телефон Горячей линии!
По вопросам защиты Персональных данных!
Тел. **8 923 655 03 00**

Приложение № 1

Примерная форма уведомления

(Угловой штамп) На бланке учреждения

Руководителю Управления Федеральной службы по надзору в сфере связи и массовых коммуникаций (Россвязькомнадзора) по Алтайскому Краю

Н.В. Ложкину

Исх. № ___ от «___» _____ 200_г

Уведомление
об обработке персональных данных

Полное наименование: Открытое акционерное общество «_____», (согласно Устава)

Краткое наименование: ОАО «_____».
Генеральный директор (): Фамилия Имя Отчество.
Юридический (почтовый) адрес: XXXXXX
(Тел./Факс/E-mail):

(наименование (фамилия, имя, отчество), адрес оператора)

ИНН: XXXXXXXXXX КПП: XXXXXXXXX ОГРН: XXXXXXXXXXXXX

руководствуясь ст. 6 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных»; ст.ст. 85-90 Трудового кодекса Российской Федерации (Федерального закона от 30.12.2001г. №197-ФЗ). Федеральным законом от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», (учредительными документами оператора, определяющими деятельность); Лицензией (№ XXX от XX.XX.XXXXг.), Уставом XXXXX (утвержден XX.XX.XXXXг.)

(правовое основание обработки персональных данных)

обработка ПД осуществляется в целях оказания услуг в области связи, либо с целью оказания медицинских услуг, или в целях оказания услуг по кредитованию граждан и т.д. (указывается как в учредительных документах).

(цель обработки персональных данных)

Основные(непосредственные):
фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, ИНН, паспортные данные, медицинский полис, страховое свидетельство)
если есть специальные(биометрические):
состояние здоровья, политические взгляды и т.д.

(категории персональных данных)

принадлежащих: Гражданам РФ (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.), сотрудникам ОАО «_____» (ООО, ЗАО и т.д.).

(категории субъектов, персональные данные которых обрабатываются)

Смешанная обработка вышеуказанных персональных данных будет осуществляться с использованием ПЭВМ (информация доступна лишь для строго определенных сотрудников юридического лица) с передачей полученной информации, с использованием сети общего пользования Интернет. Хранение сведений (базы данных) организовано на электронных носителях с паролем, на бумажных носителях - в сейфах

(Описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке)

на территории Алтайского края

(указывается территория субъекта (ов), на которой (ых) осуществляется обработка персональных данных)

Дата начала обработки персональных данных: XX.XX.XXXXг.

Срок или условия прекращения обработки персональных данных: прекращение деятельности как юридического лица.

Приложение № 2
к Приказу Россвязькомнадзора
от "17" июля 2008 № 08

РЕКОМЕНДАЦИИ ПО ЗАПОЛНЕНИЮ ОБРАЗЦА ФОРМЫ УВЕДОМЛЕНИЯ ОБ ОБРАБОТКЕ (О НАМЕРЕНИИ ОСУЩЕСТВЛЯТЬ ОБРАБОТКУ) ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящие Рекомендации разработаны в целях установления единых принципов и порядка заполнения уведомления об обработке (о намерении осуществлять обработку) персональных данных (далее - Уведомление).

2. Уведомление оформляется на бланке оператора, осуществляющего обработку персональных данных, и направляется в территориальный орган Федеральной службы по надзору в сфере массовых коммуникаций (далее - территориальный орган Россвязькомнадзора).

3. Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации.

4. В поле **«наименование (фамилия, имя, отчество), адрес оператора»** указывается:

4.1. Для юридических лиц (операторов):
- полное наименование с указанием организационно-правовой формы и сокращенное наименование юридического лица (оператора), осуществляющего обработку персональных данных;
- наименование филиала(ов) (представительства(в) юридического лица (оператора), осуществляющего обработку персональных данных <1>;
- место нахождения<2>;

<1> Для юридических лиц с филиальной структурой указывается список субъектов Российской Федерации (с указанием кода субъекта – согласно справочнику «Коды регионов», утвержденному приказом ФНС России от 13.10.2006 года № САЭ-3-04/706@ «Об утверждении формы сведений о доходах физических лиц»), на территории которых находятся филиалы (представительства) юридического лица и (или) где оператором производится обработка персональных данных. Уведомление направляется юридическим лицом в соответствующее территориальное управление Россвязькомнадзора по месту своего нахождения с указанием всех имеющихся филиалов (представительств) (Примечание № 1).

Примечание 1. *Если для каких-либо операторов (с учетом филиалов (представительств) значения пунктов 5-12 отличаются, то для них формируется отдельное уведомление.*

<2> Указывается место нахождения юридического лица в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, а также место нахождения филиала(ов) (представительств) юридического лица, контактная информация (Примечание № 2).

Примечание 2. *Для организаций, учреждений, имеющих филиалы (представительства), указываются юридический и фактический адрес (как юридического лица, так и его филиалов и представительств), где осуществляется непосредственная обработка персональных данных (все действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных). При этом необходимо уточнить - обработка персональных данных осуществляется только юридическим лицом (формирование центральной информационной системы) и (или) филиалами (представительствами).*

- индивидуальный номер налогоплательщика (ИНН).

4.2. Для физических лиц:
-фамилия, имя, отчество физического лица (оператора);
- место жительства <1>;

<1> Указывается место жительства физического лица в соответствии с данными документа, удостоверяющего личность, а в случае расхождения, также фактическое место жительство, контактная информация.

- данные документа, удостоверяющего личность, дата его выдачи, наименование органа, выдавшего документ,

удостоверяющий личность.

Для индивидуальных предпринимателей:
-фамилия, имя, отчество индивидуального предпринимателя (оператора);
-место жительства <1>;

<1> Указывается место жительства индивидуального предпринимателя (оператора) в соответствии с данными документа, удостоверяющего личность, и свидетельством о постановке индивидуального предпринимателя на учет в налоговом органе, контактная информация.

- индивидуальный номер налогоплательщика (ИНН).

4.3. Для государственных, муниципальных органов (операторов):
полное и сокращенное наименование государственного, муниципального органа;
наименование территориального(ых) органа(ов), осуществляющего(их) обработку персональных данных;
место нахождения<1>;

<1> Указывается место нахождения государственного, муниципального органа в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, контактная информация.

- индивидуальный номер налогоплательщика (ИНН).

При указании наименования (фамилии, имени, отчества), адреса оператора, а также направления деятельности рекомендуется использовать также ссылки на код(ы) классификаторов (ОКВЭД, ОКПО, ОКОГУ, ОКОП, ОКФС).

5. В поле **«цель обработки персональных данных»** указываются цели обработки персональных данных (а также их соответствие полномочиям оператора) (Примечание № 1).

***Примечание № 1**: Под «целью обработки персональных данных» понимаются, как цели, указанные в учредительных документах оператора, так и цели, фактически осуществляемой оператором деятельности по обработке персональных данных.*

6. В поле **«категории персональных данных»** указываются все категории персональных данных, подлежащих обработке:

6.1. Персональные данные (любая информация, относящаяся к определенному или определяемому на основе такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата рождения, место рождение, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая необходимая информация).

6.2. Специальные категории персональных данных (расовая принадлежность, национальная принадлежность, политические взгляды, религиозные убеждения, философские убеждения, состояние здоровья, состояние интимной жизни).

6.3. Биометрические персональные данные (сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность).

7. В поле **«категории субъектов, персональные данные которых обрабатываются»** указываются категории субъектов (физических лиц) и виды отношений с субъектами (физическими лицами), персональные данные которых обрабатываются. Например: работники (субъекты), состоящие в трудовых отношениях с юридическим лицом (оператором), физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.) (субъекты), состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором) и др.

8. В поле **«правовое основание обработки персональных данных»** указываются:
Федеральный закон, постановление Правительства Российской Федерации, иной нормативно-правовой акт, закрепляющий основание и порядок обработки персональных данных (Примечание № 1);
Номер, дату выдачи и наименование лицензии на осуществляемый вид деятельности, с указанием лицензионных условий, закрепляющих запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных. (Примечание № 2).

***Примечание № 1:** Указываются не только соответствующие статьи Федерального закона «О персональных данных», но и статьи иного нормативно-правового акта, регулирующие осуществляемый вид деятельности и касающиеся обработки персональных данных. (Например: ст. ст. 85-90 Трудового кодекса РФ, ст. 85.1 Воздушного кодекса РФ, ст. 12 Федерального закона «Об актах гражданского состояния» и др.).*

***Примечание № 2:** Номер лицензии и пункт лицензионных условий, закрепляющий запрет на передачу персональных данных (или информации, касающейся физических лиц), отражается только при наличии лицензии и (или) соответствующего пункта лицензионных условий.*

9. В поле **«перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных»**, указываются действия, совершаемые оператором с персональными данными, а также описание используемых оператором способов обработки персональных данных:
- неавтоматизированная обработка персональных данных;
- исключительно автоматизированная обработка персональных данных с передачей полученной информации по сети или без таковой;
- смешанная обработка персональных данных. (Примечание № 1).

***Примечание № 1**: При автоматизированной обработке персональных данных либо смешанной обработке, необходимо указать, передается ли полученная в ходе обработки персональных данных информация по внутренней сети юридического лица (информация доступна лишь для строго определенных сотрудников юридического лица) либо информация передается с использованием сети общего пользования Интернет либо без передачи полученной информации.*

10. В поле **«описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке»**, указываются организационные и технические меры, в том числе использование шифровальных (криптографических) средств, используемых для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий при их обработке.

11. В поле **«дата начала обработки персональных данных»** указывается конкретная дата начала совершения действий с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных (*фактическая дата начала обработки персональных данных*).

12. В поле **«срок или условие прекращения обработки персональных данных»** указывается конкретная дата или основание (условие), наступление которого повлечет прекращение обработки персональных данных.

Приложение № 3

Шаблон «**АКТ классификации информационной системы персональных данных»**

УТВЕРЖДАЮ
Главный врач МУЗ «Городская больница №1»

_____
(дата, подпись)

АКТ
классификации информационной системы персональных данных
Муниципального учреждения здравоохранения «Городская больница №1»

Комиссия в составе:
Председатель:
- ***Ф.И.О. должностного лица***

Члены комиссии:
- ***Ф.И.О. должностного лица***
- ***Ф.И.О. должностного лица***

Рассмотрев исходные данные на информационную систему информационную систему <***указание информационной системы***>

установила:

1. ИС содержит персональные данные - <***категория данных***>.
2. Объем обрабатываемых персональных данных – <***объем хранимых записей***>.
3. Заданные характеристики безопасности персональных данных - <***типовые/специальные***>.
4. Структура ИС - <***струтктура***>.
5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) - <***с подключением/без подключения***>.
6. Режим обработки персональных данных – <***многопользовательский/однопользовательский***>.
7. Права доступа к персональным данным (полномочия) пользователей – <***разные/равные***>.

РЕШИЛА:

На основании приказа ФСТЭК от 13 февраля 2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных <***номер класса***>;

Председатель комиссии ***Ф.И.О. должностного лица***

Члены комиссии: ***Ф.И.О. должностного лица***

Ф.И.О. должностного лица

Список сокращений

АС – автоматизированная система;
АРМ — автоматизированное рабочее место;
ИСПДн — информационная система персональных данных;
ПДн — персональные данные;
НСД — несанкционированный доступ;
ЛВС – локальная вычислительная сеть;
СЗПДн – средства защиты персональных данных;
ЗИ – защита информации;
ПО – программное обеспечение;
ППО – программно прикладное обеспечение;
ТУ – техническое условие;
СВТ – средства вычислительной техники;
СЗИ – средства защиты информации.
ПМВ – программно-математическое воздействие.
ВП – вредоносные программы.
УБПДн - угрозы безопасности персональных данных.
ПЭМИН - побочные электромагнитные излучения и наводки.