White Paper

Инструкции по организации и обеспечению безопасности ПДн

Содержание

Инструкция по организации обработки и обеспечению безопасности ПДн для оператора

Согласно 152-ФЗ, Статья 18.1. п 1. “Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обазанностей, предусмотренных настоящим Федеральным законом и принятыми в соответсвии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами”.

Таким образом, несмотря на самостоятельность определения состава и перечня мер, оператор не может решить, что защищать персональные данные он не будет, только потому что определенный им самостоятельно перечень мер не включает и не должен ничего включать, исходя из его личного мнения. Оператор обязан предпринимать необходимые и достаточные меры, а какие именно является такими следует самостоятельно определить из ФЗ-152 и принятых в соответствии с ним нормативных правовых актов.

Далее опишем каждую из мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных 152-ФЗ и закрепленных в статье 18.1 этого Закона.

Первый этап

Первым шагом в приведении процесса обработки персональных данных в организации в соответствие с требованиями закона должно стать назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных.

Кого следует назначить ответственным за организацию обработки персональных данных? Того, кто сможет эффективно выполнять следующие обязанности:

- Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства РФ о ПДн, в том числе требований к защите ПДн;
- Доводить до сведения работников оператора положения законодательства РФ о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;
- Организовывать прием и обработки обращений и запросов субъектов ПДн или представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Из этого следует, что отвветственный сотрудник занимается управлением процессом обработки ПДн и осуществляет функции менеджмента, а не обазанности специалиста, который работает напрямую с субъектами ПДн (клиентами или сотрудниками). Для эффективного выполнения возложенных на него обязанностей он должен обладать достаточным административным ресурсом в рамках компанни, чтобы процесс организации обработки ПДн не начинал “пробуксовывать” по причине недостаточной мотивации других сотрудников.

Должен ли ответственный за организацию обработки ПДн обладать компетенциями в вопросах технических мер защиты информации? Для ответа на этот вопрос важно помнить, что специалист, ответственный за организацию обработки, не равно ответственный за обеспечение безопасности ПДн, а процессс обеспечения безопасности ПДн является составляющей частью процесса организации обработки.

При этом, согласно Приказу ФСБ №378. который определяет требования по обеспечению безопасности с использованием средств криптозащиты, для выполнения требования, указанного в пункте 16 Приказа, необходимо назначение должностного лица (работника) оператора, обладающего достаточными навыками, ответственным за обеспечение безопасности персональных данных в информационной системе.

Таким образом, для ответственного за организацию обработки необходимые компетенции законодательно не закреплены. Требования предъявляются только к ответственному за обеспечение безопасности ПДн.

Второй этап

Результатами второго этапа должно стать:

Издание оператором, являющимся юридическим лицом

- Документов, определяющих политику оператора в отношении обработки персональных данных;
- Локальных актов по вопросам обработки персональных данных;
- Локальных актов устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

Применение

- Правовых;
- Организационных;
- Технических мер по обеспечению безопасности персональных данных.

Таким образом, второй этап можно разбить на две составляющие:

- Организацию обработки;
- Обеспечение безопасности.

Организация обработки

Для того, чтобы эффективно достичь затртаных по времени и труду результатов организации обработки, следует составить план мероприятий. Для реализации этого плана потребуется собрать комиссию, состав которой нужно определить исходя из понимания того, какие сотрудники наиболее хорошо знакомы с работой информационных систем организации, содержащих какие-либо персональные данные. О назначении комиссии следует издать указ и ознакомить членов комиссии с нормативными и методическими документами, которыми нужно руководствоваться.

Комиссия должна провести “инвентаризацию” персональных данных, обрабатываемых организацией и описать процессы их обработки. Каждый прцоесс должен иметь цель обработки на правовых основаниях (с письменным согласием субхекта ПДн или без него в соответствии с законом). Для каждлго процесса необходимо определить перечень ответственных за обработку и допущенных к ней лиц, состав обрабатываемых ПДн и сроки обработки.

Имея карту процессов обработки ПДн, организации необходимо выделить все “изолированные друг от друга” информационные системы персональных данных (ИСПДНн). При этом следует помнить, что не допускается объединение баз данных содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Для каждой ИСПДн необходимо определить перечень, категории и объемы обрабатываемых ПДн, перечень действий, правовые основания, даты начала обработки, сроки и условия прекращения обработки, сведения о трансграничной передаче, если таковая имеется. Для обследования ИСПДн рекомендуется разработать анкеты, которые помогут комиссии получить необходимые сведения от работников организации. Итогом работы комиссии должго стать издание оператором необходимых документов и актов с приказом о вводе документов в действие. Какой перечень документов необходимо утвердить руководителю организации?

Законодательно подробный перечень документов для организации с частной формой собственноси не закрплен. Однако, такой перечень можно найти в Постановлении Правительства ПП-211 и, адаптировав, применить в своей организации.

Политика оператора в отношении обработки персональных данных или правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также, определяющие для каждой цели обработки персональных данных:

- Содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
- Правила рассмотрения запросов субъектов персональных данных или их представителей;
- Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;
- Правила работы с обезличенными данными в случае обезличивания персональных данных;
- Перечень информационных систем персональных данных;
- Перечни персональных данных, обрабатываемых в организации;
- Перечень должностей ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных;
- Перечень должностей замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным;
- Должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обрабтки персональных данных; персональных данных, ставших известными ему в связи ис исполнением должностных обязаннстей;
- Типовая форма согласия на обработку персональных данных сотрудника, иных субъектов персональных данных;
- Типовая форма разъяснения субъекту персональных персональных данных юридических последствий отказа предоставить свои персональные данные;
- Порядок доступа сотрудников в помещения, в которых ведется обработка ПД.

При разработке документов можно воспользоваться рекомендациями Регуляторов, шаблонами документов, разработанных компаниями интеграторами и образовательными учреждениями, пользоваться для ориентира чужими опубликованными документами. Однако, строго обязательно адаптировать эти документы под специфику своей организации, так как неправильно оформленные документы, например, с указанием неверных целей обработки ПДн, могут быть причиной наложения штрафа на организацию.

Часть документов должны находится в публичном доступе. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. При этом стоит помнить, что политика описывает лишь общий характер действий, направленных на обеспечение безопасности ПДн в организации, поэтому детально раскрывать особенности организации обработки ПДн, которые не требуются по закону, не нужно.

Все владельцы сайтов, независимо от того сама организация осуществляет его администрирование или это отдано на аутсорсинг другому лицу, обязаны опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

Закончив краткий обзор деятельности оператора по разработке документов и локальных актов, перейдем к мерам по обеспечению безопасности персональных данных. Оба этих процесса, как применение мер, так и разработка, и издание документов, связаны с друг другом и происходят одновременно.

Обеспечение безопасности - организационные и технические меры

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Обеспечение безопасности персональных данных достигается, в частности:

- Определением угроз безопасности ПДн при их обработке в ИСПДн;
- Применением организационных и технических мер, необходимых для выполнения требований, исполнение которых обеспечивает установленные в ПП-1119 уровни защищенности ПДн;
- Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- Учетом машинных носителей персональных данных;
- и рядом других мер.

Таким образом организации нужно создать систему обеспечения безопасности ПДн, которая должна:

- Нейтрализовать актуальные угрозы;
- Включать в себя организационные и/или технические меры;
- Применять средства защиты информации, выбранные оператором в соответствии с нормативными правовыми актами ФСТЭК и ФСБ.

При принятии мер, необходимых и достаточных для обеспечения выполнения обязанностей оператора,нужно оценивать вред, который может быть причинен субъектам пд в случае нарушения 152-ФЗ и соотносить уровень возможного вреда и принимаемые им меры, направленные на выполнения обязанностей. Вред должен определяться исходя из оценки всех неблагоприятных последствий, которые может повлечь несоблюдение требования Закона: от размера штрафных санкций до репутационных рисков и судебных издержек. Для этого берём Постановление Правительства №1119 и определяем для каждой ИСПДн уровень защищённости. Сначала определяем вид ИСПДн.

Виды информационных систем ПДн:

- Обрабатывает специальные категории ПДн;
- Обрабатывает биометрические ПДн;
- Обрабатывается общедоступные ПДн;
- Обрабатывает иные категории ПДн;
- Обрабатывает только ПДн сотрудников оператора.

Далее в соответствии с этим Постановлением нужно понять какие угрозы актуальны для ИСПДн.

Типы актуальных угроз:

- Угрозы 1-го типа связаны с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в ИС;
- Угрозы 2-го типа связаны с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в ИС;
- Угрозы 3-го типа НЕ связаны с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИС.

Как понять, что такое угрозы каждого из типов? Технические детали операторы ожидали получить от ФСТЭК. Однако, в «Информационном сообщении по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России № 17 и № 21», Регулятор одновременно сообщил, что ФСТЭК России не наделена полномочиями по разъяснению Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, в том числе в части определения типов угроз персональных данных и порядка определения уровней защищенности персональных данных.

Таким образом, ФСТЭК обозначили свою позицию. Из неё следует, что Правительство России, выпустившее ПП-1119 должны сами разъяснить, что Правительство имело ввиду, говоря об угрозах 1-ого, 2-ого и 3-го типов. Однако, таких разъяснений с их стороны не было опубликовано. По этой причине возможность решить вопрос об актуальности угроз 1 и 2-ого типов оператору предоставляется на основе собственных суждений. Это приводит к тому, что большинство операторов при определении угроз считают актуальными только угрозы 3-го типа.

Теперь, зная тип ИСПДн, в соответствии с ПП-1119 мы можем определить уровень защищенности ПДн при их обработке в этой ИСПДн. Ниже приведена таблица, описывающая необходимость обеспечения каждого из уровней защищенности, установленных ПП-1119 в удобной для работы табличной форме.

Сотрудники оператора				
Категории ПДн	Количество	Угрозы 1 типа	Угрозы 2 типа	Угрозы 3 типа
Специальные		1 уровень	2 уровень	3 уровень
Биометрические		1 уровень	2 уровень	3 уровень
Иные		1 уровень	3 уровень	4 уровень
Общедоступные		2 уровень	3 уровень	4 уровень
Не сотрудники оператора				
Категории ПДн	Количество	Угрозы 1 типа	Угрозы 2 типа	Угрозы 3 типа
Специальные	более 100 000	1 уровень	1 уровень	2 уровень
	менее 100 000	1 уровень	2 уровень	3 уровень
Биометрические	более 100 000	1 уровень	2 уровень	3 уровень
	менее 100 000	1 уровень	2 уровень	3 уровень
Иные	более 100 000	1 уровень	2 уровень	3 уровень
	менее 100 000	1 уровень	3 уровень	4 уровень
Общедоступные	более 100 000	2 уровень	2 уровень	4 уровень
	менее 100 000	2 уровень	3 уровень	4 уровень

Для обеспечения каждого из уровней защищенности персональных данных при их обработке в информационных сисстемах необходимо выполнение набора требований.

Перечень мер защиты	1 УЗ	2 УЗ	3 УЗ	4 УЗ
Организовать режим обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих прав доступа в эти помещения	+	+	+	+
Обеспечить сохранность носителей ПДн	+	+	+	+
Утвердить перечень лиц, имеющих доступ к ПДн в рамках выполнения своих служебных обязанностей	+	+	+	+
Использовать сертифицированные СЗИ	+	+	+	+
Назначить приказом должностное лицо, ответственное за обеспечение безопасности ПДн в ИСПДн.	+	+	+	
Доступ к электронному журналу сообщении определить только лицам, которым необходимы сведения, содержащиеся в данном журнале для выполнения своих служебных обязанностей	+	+		
Обеспечить автоматическую регистрацию в электронном журнале безопасности изменения полномочии сотрудника по доступу к ПДн в ИСПДн	+			
Создать структурное подразделение ответственное за обеспечение безопасности ПДн в ИСПДн или возложить эти функции по обеспечению безопасности ПДн в ИСПДн на одно из существующих структурных подразделении	+			

Теперь зная требования для обеспечения необходимого уровня защищенности, берем Приказ ФСТЭК №21 от 18.02.2013г. “Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

- Определяем базовый набор мер;
- Проводим адаптацию базового набора мер;
- Уточнеяем адаптированный базовый набор мер;
- Дополняем уточненный адаптированный базовый набор.

Состав и содержание мер для каждого из уровней защищенности приведены в приложении к приказу. Все меры не предоставляется возможным и нужным здесь описывать, документ вы можете найти в открытом доступе. Как реализовывать выбранный набор мер оператор может узнать из Методического документа «Меры защиты информации в государственных информационных системах».
По применимости этого документа при построении системы защиты ПДн в организациях с частной формой собственности мы говорили ранее.
Количество базовых мер в наборе значительно возрастает между 2 и 3 уровнями защищенности.

Поэтому реализация требований по обеспечению 3 и 4 уровня защищенности является более простым и менее затратным процессом. При этом опираясь на таблицу по определению уровня защищенности, мы можем сделать вывод о том, что УЗ-3 и УЗ-4 наиболее вероятные для большинства ИСПДн уровни защищенности, особенно при условии определения оператором актуальности только 3 типа угроз.

Ниже приведен состав и содержание мер для УЗ-4 из приложения Приказа ФСТЭК №21.

ИАФ.1. Идентификация и аутентификация пользователей, являющихся работниками оператора.
ИАФ.3. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.
ИАФ.4. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.
ИАФ.5. Защита обратной связи при вводе аутентификационной информации
ИАФ.6. Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).
УПД.1. Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей.
УПД.2. Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.
УПД.3. Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.
УПД.4. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5. Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

УПД.6. Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).
УПД.13. Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационнотелекоммуникационные сети.
УПД.14. Регламентация и контроль использования в информационной системе технологий беспроводного доступа.
УПД.15. Регламентация и контроль использования в информационной системе мобильных технических средств.
УПД.16. Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).
РСБ.1. Определение событий безопасности, подлежащих регистрации, и сроков их хранения.
РСБ.2. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.
РСБ.3. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.
РСБ.7. Защита информации о событиях безопасности.
АВ3.1. Реализация антивирусной защиты.
АВ3.2.Обновление базы данных признаков вредоносных компьютерных программ (вирусов).
АН3.2. Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.
ЗСВ.1. Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.
ЗСВ.2. Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин.
ЗТС.3. Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены.
ЗТС.4. Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.
ЗИС.3. Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

Также необходимо в соответствии с Приказом ФСБ №378 применять средства криптографической защиты информации (СКЗИ) в случаях, если вы определили актуальными угрозы, которые могут быть нейтрализованы только с помощью СКЗИ, а именно:

- Передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования между филиалами организации);
- Хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

Для каждого из уровней защищенности ПДн должны применять СКЗИ соответствующего класса. Класс СКЗИ определяется исходя из совокупности предположений о возможностях для создания способов, подготовке и проведения атак и типа актуальных угроз безопасности ПДн.

Вкратце, для выбора СЗИ и СКЗИ для защиты ПДн необходимо предпринять следующие шаги:

1. Обследовать ИСПДн и определить какие ПДн в ней обрабатываются, кто субъекты и в каком количестве.
2. Определить тип актуальных угроз.
3. Определить требуемый уровень защищенности ПДн и состав и содержание мер:
   - По требуемому УЗ определить классы/уровни сертификации технических СЗИ и выбрать СЗИ.
4. Сформировать и утвердить совокупность предположений о возможностях для подготовки и проведения атак:
   - По требуемому УЗ, типу актуальных угроз и совокупности возможностей для атак определить требуемый класс СКЗИ и выбрать СКЗИ.

Обязательно ли применять сертифицированные средства защиты ПДН?

В Законе сказано, что обеспечение безопасности ПДн достигается применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

Требование «оценки соответствия» есть и его необходимо выполнять. Однако, оценка соответствия проводится в формах:

- государственного контроля (надзора);
- аккредитации;
- испытания;
- регистрации;
- подтверждения соответствия;
- приемки и ввода в эксплуатацию объекта, строительство которого закончено, и в иной форме.

Таким образом, оценка соответствия может быть в различных формах. Требования закона об обязательной сертификации средств защиты, применяемых в организациях с частной формой собственности, нет. Государственный контроль и надзор - это тоже форма оценки соответствия, а значит Оператор может дожидаться проверки со стороны ФСТЭК и ФСБ, чтобы узнать верно ли спроектирована система защиты и применены СЗИ в организации.

При прохождении проверок эффективность предпринятых мер необходимо доказать, поэтому использование в своей деятельности сертифицированных средств защиты информации - это наиболее надёжное решение, минимизирующее риски.

Заключительные этапы

Заключительными этапами в реализации необходимых и достаточных мер для обеспечения выполнения обязанностей добросовестного оператора ПДн являются:

- Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки;

Согласно Приказу ФСТЭК №21 оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации не реже одного раза в 3 года.

- Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите ПДн, документами, определяющими политику оператора в отношении обработки ПДн, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

Заключительные этапы

Также согласно ст. 22 Закона о персональных данных, Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, когда оператор вправе осуществлять без уведомления уполномоченного органа обработку ПДн:

- обрабатываются только данные сотрудников;
- ПДн получены оператором в связи с заключением договора, стороной которого является субъект ПДн, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта ПДн и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- субъект персональных данных сделал их общедоступными;
- обрабатываются только и исключительно фамилии, имена и отчества;
- для однократного пропуска субъекта персональных данных на территорию оператора;
- при обработке ПДн без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;
- в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности.

Причину, по которой вы решили не уведомлять Регулятора, рекомендуется отразить в ваших документах, определяющих политику в отношении обработки персональных данных.

Если обработка ПДн в вашей организации не попадает под перечисленные выше исключения об обязательном уведомлении, необходимо отправить уведомление в Роскомнадзор. В ином случае это может быть причиной наложения штрафа на огранизацию.

Типовые нарушения в области персональных данных

I. Представление в уполномоченный орган уведомления об обработке ПД, содержащих неполные и (или) недостоверные сведения

Признаки нарушения

Неполный перечень:

- Целей обработки ПД
- ПД, обрабатываемых оператором
- Категорий субъектов ПД
- Правовых оснований обработки ПД
- Адресов баз ПД

Отсуствие адреса базы ПД

Как избежать

- Получать информацию с портала https://pd.rkn.gov.ru
- Использовать приказ Роскомнадзора от 30.05.2017 No 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»

II. Непредставление в уполномоченный орган сведений о прекращении обработки персональных данных или об изменении информации, содержащейся в уведомлении об обработке персональных данных

Признаки нарушения

Неуведомление РКН о:

- Изменении перечня обрабатываемых ПД
- Изменении перечня категорий субъектов ПД
- Использовании шифровальных (криптографических средств)
- Осуществлении трансграничной передачи ПД
- Новых адресах баз ПД
- Изменеии ответсвенного за организацию обработки ПД, его контактных данных

Как избежать

В течение 10 дней направить в адрес Роскомнадзора информационное письмо о прекращении обработки ПД или об изменении сведений, ранее представленных в уведомлении об обработке ПД

III. Несоблюдение требований по информированию лиц, осуществляющих обработку персональных данных без использования автоматизации (п. 6 постановления правительства РФ от 15.09.2008 No 687)

Признаки нарушения

Отсутсвие информирования лиц, осуещствляющих обработку ПД без использования средств автоматизации:

- Факте обработки ПД
- Категориях обрабатываемых ПД
- Особенностях и правилах осуществления такой обработки установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии)

Как избежать

Добавить соответствующие положения в трудовой договор, должностной регламент, типовую форму, используемую оператором при обработке пд работника, локальных актов оператора.

IV. Несоответствие содержания письменного согласия субъекта персональных данных на обработку персональных данных требования законодательства Российской Федерации

Признаки нарушения

- Отсутствие адреса или данных основного документа, удостоверяющего личность субъекта
- Указание нескольких целей обработки ПД
- Отсутствие наименования или ФИО и адреса лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу
- Отсутствие перечня ПД, на обработку которых дается согласие Отсутствие способа отзыва согласия на обработку ПД.

Как избежать

Привести содержание письменного согласия субъекта персональных данных на обработку ПД в соответствие с требованиями законодательства Российской Федерации

V. Непринятие оператором мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных федеральным законом от 27 июля 2006 г. No 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами

Как избежать

- Назначить ответственного за организацию обработки пд, обладающего полномочиями, предусмотренными ст. 22.1 федерального закона «О персональных данных»
- Издать и/или опубликовать документ, определяющий политику в отношении ПД; издание локальных актов по всем вопросам обработки ПД в рамках пропускного режима, подбора персонала и т.д.
- Провести внутренний аудит

VI. Отсутствие места (мест) хранения персональных данных (материальных носителей), перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ (п. 13 постановления правительства РФ от 15.09.2008 No 687)

Как избежать

Издать приказ об утверждении перечня лиц, осуществляющих обработку ПД либо имеющих к ним доступ

Меры административного воздействия

Предмет жалоб граждан

Соцсети

Телеком

Банки

E-commerce

ЖКХ

Образование

Меры реагирования

1. Требование о прекращении неправомерной обработки ПД
2. Ограничение доступа к интернет-ресурсу
3. Принятие мер административного воздействия по ст. 13.11 КоАП РФ
4. Принятие мер пресекательного характера

Статья 13 КоАП РФ

Состав административных правонарушений

1

Часть 1
Несоответствие целям и условиям обработки ПД

2

Часть 2
Отсутствие письменного согласия либо не соблюдены требования к его содержанию

3

Часть 3
Отсутствие доступа к политике в отношении обработки ПД

4

Часть 4
Не реализовано право субъекта на получение информации

5

Часть 5
Нарушение сроков по уточнению, блокированию, уничтожению ПД

6

Часть 6
Невыполнение обязанностей по соблюдению условий, обеспечивающих сохранность материальных носителей

Чем мы можем Вам помочь?

ООО «НТЦ ЕВРААС», являясь многопрофильной коммерческой структурой, имеет все необходимые лицензии регуляторов рынка информационной безопасности, в том числе лицензии на осуществление работ с использованием сведений, составляющих государственную тайну.

Обладая фундаментальными знаниями и опытом в области защиты информации, эксперты НТЦ «ЕВРААС» предлагают новейшие комплексные разработки в сфере обеспечения безопасности персональных данных и соответствия требованиям регуляторов.

Мы проектируем системы под конкретные нужды и специфику организаций, тем самым гарантируя, что система информационной безопасности комплексно решает все задачи и обеспечивает надежную круглосуточную защиту ваших корпоративных ресурсов и данных.

Контакты:

г. Москва, ул. Автозаводская 13/1

8 (495) 748-09-44

evraas@evraas.ru