

Модуль 2

Организация обеспечения безопасности персональных данных в информационных системах персональных данных

Тема 2.2. Разработка документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных

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

Постановление Правительства от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ...

Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в ...

Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в ...

Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных ...

Методический документ «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России от 11.02.2014 г.

Бюджетное учреждение
Ханты-Мансийского автономного округа - Югры
«Югра»
(БУ «Югра»)

ПРИКАЗ

№ 00

«__» _____ 20__ года

О защите персональных данных

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 №

Разработка документов, определяющих политику оператора в отношении обработки ПДн, локальных актов по вопросам обработки ПДн

2. Утвердить перечень должностей сотрудников БУ «Югра», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, согласно приложению 1 к настоящему приказу.

3. Создать комиссию по защите информации:

3.1. Утвердить состав комиссии по защите информации согласно приложению 2 к настоящему приказу.

3.2. Утвердить положение о комиссии по защите информации согласно приложению 3 к настоящему приказу.

4. Утвердить типовые формы документов по защите информации:

4.1. Согласие на обработку персональных данных согласно приложению 4 к настоящему приказу.

Правила доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн

Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям законодательства в области защиты ПДн

Инструкция ответственного за организацию обработки ПДн в учреждении

Журнал учета машинных носителей ПДн

Политика оператора в отношении обработки ПДн

Порядок доступа сотрудников учреждения в помещения, в которых ведется обработка ПДн

Правила рассмотрения запросов субъектов ПДн или их представителей

Типовое обязательство сотрудника учреждения, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним трудового договора прекратить обработку ПДн, ставших известными ему в связи с исполнением должностных обязанностей

Типовая форма согласия на обработку ПДн сотрудников учреждения, иных субъектов ПДн, а также типовая форма разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн

Журнал ознакомления работников оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ о ПДн

Инструкция по работе с инцидентами информационной безопасности

Перечень информационных систем персональных данных

Лицо, ответственное за обеспечение безопасности ПДн в информационных системах персональных данных

Инструкция по организации резервного копирования и восстановления программного обеспечения и баз ПДн в информационных системах персональных данных

Перечень должностей сотрудников учреждения, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн

Перечень ПДн, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций

Документы, определяющие политику оператора в отношении обработки ПДн, локальных актов по вопросам обработки ПДн

Требования постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом...» по разработке следующих документов

Правила обработки ПДн, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере ПДн, а также определяющие для каждой цели обработки ПДн содержание обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований

Типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку ПДн, ставших известными ему в связи с исполнением должностных обязанностей

Перечни ПДн, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций

Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора

Перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн

Должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки ПДн в государственном или муниципальном органе

Типовая форма согласия на обработку ПДн служащих государственного или муниципального органа, иных субъектов ПДн, а также типовая форма разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн

Порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка ПДн

Правила рассмотрения запросов субъектов ПДн или их представителей

Перечень информационных систем персональных данных

**РЕКОМЕНДАЦИИ
ПО СОСТАВЛЕНИЮ ДОКУМЕНТА, ОПРЕДЕЛЯЮЩЕГО ПОЛИТИКУ
ОПЕРАТОРА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, В ПОРЯДКЕ,
УСТАНОВЛЕННОМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ ОТ 27 ИЮЛЯ
2006 ГОДА N 152-ФЗ "О ПЕРСОНАЛЬНЫХ ДАННЫХ"**

1. Настоящие Рекомендации разработаны в целях выработки унифицированных подходов к структуре и форме документа, определяющего политику оператора в отношении обработки персональных данных (далее - Политика).

2. Основные понятия, используемые в Рекомендациях:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- оператор персональных данных (оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;

Рекомендации разработаны Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 27.07.2017 г. (<https://rkn.gov.ru/personal-data/p908/>)

Структура Политики в отношении обработки персональных данных (далее - Политика)

Общие положения
(назначение Политики, основные понятия, права и обязанности оператора и субъекта (ов) ПДн)

Цели сбора персональных данных
(проанализировать правовые акты, регламентирующие деятельность оператора, учредительные документы и т.д.)

Правовые основания обработки персональных данных
(федеральные законы, уставные документы, договоры, согласие на обработку ПДн)

Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

Порядок и условия обработки персональных данных
(перечень действий, способы и сроки обработки ПДн и т.д.)

Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

ИНСТРУКЦИЯ

ответственного за организацию обработки персональных данных

1. Общие положения

1.1. Ответственный за организацию обработки персональных данных в БУ «Югра» назначается приказом БУ «Югра» и отвечает за организацию обеспечения своевременного и квалифицированного выполнения сотрудниками БУ «Югра» требований по организации обработки и обеспечения безопасности персональных данных (далее - ПДн).

1.2. Ответственный за организацию обработки персональных данных (далее - Ответственный) в своей деятельности руководствуется:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

- Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;

- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

В соответствии с подпунктом 6 пункта 1 постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении Перечня мер ...» должен быть утвержден должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных в государственном или муниципальном органе

В соответствии с пунктом 4 федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» ответственный за организацию обработки ПДн обязан:

Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн

Доводить до сведения работников оператора положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн

Организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов

Порядок доступа сотрудников БУ «Югра» в помещения, в которых ведется обработка персональных данных

1. Общие положения

1.1. Порядок доступа сотрудников БУ «Югра» в помещения, в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с Постановлением правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», приказом ФСТЭК России от 11.02.2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2. Защита от проникновения посторонних лиц в помещения БУ «Югра» обеспечивается организацией порядка доступа, а также соответствующей инженерно-технической защитой помещений, а именно охранной сигнализацией и системой контроля и управления доступом.

2. Порядок доступа в помещения

2.1. Перечень должностей в БУ «Югра», доступ которых в Помещения необходим для выполнения ими должностных (трудовых) обязанностей приведен в приложении 1 к настоящему приказу.

2.2. Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 2.1 настоящего Порядка разрешено в период рабочего времени в соответствии с утвержденным графиком работы БУ «Югра» либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных дан-

Данный документ должен содержать следующие сведения:

Перечень лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены

Порядок санкционированного физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены

Порядок учета физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены

Требования, предъявляемые к помещениям, в которых ведется обработка персональных данных

СОГЛАСИЕ
на обработку персональных данных
г. Ханты-Мансийск «__» _____ г.

Я, _____
(фамилия, имя, отчество)
серия _____ № _____ выдан _____
(или документа, удостоверяющего личность)
(когда и кем)
проживающий(ая) по адресу: _____

настоящим даю свое согласие на обработку моих персональных данных БУ «Югра», расположенному по адресу: 628000, Ханты-Мансийский автономный округ - Югра, г. Ханты-Мансийск, ул. Мира, д. 1, и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

Согласие дается мною для целей обеспечения соблюдения в отношении меня законодательства Российской Федерации для реализации трудовых отношений и распространяется на следующую информацию:

- фамилия, имя, отчество; пол; гражданство;
- паспортные данные (серия, номер, кем и когда выдан);
- год, месяц и дата рождения; место рождения;
- ...

полученных лично от меня для обработки и передачи в документальной и электронной форме в различные государственные органы власти, если этого требует законодательство Российской Федерации или Ханты-Мансийского автономного округа – Югры, а также третьим лицам:

- Пенсионный фонд Российской Федерации (Адрес: 628000, 0 Ханты-Мансийский автономный округ - Югра, г. Ханты-Мансийск, ул. Мира, д. 100);
- ...

с целью исполнения обязательств представителя нанимателя в рамках трудового договора, и в установленных Федеральными законами случаях их обязательного предоставления.

В соответствии со статьей 8 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие на размещение моих персональных данных:

- фамилия, имени, отчества;
- ...

на официальном сайте БУ «Югра», который является общедоступным источником персональных данных.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных с учетом федерального законодательства.

Настоящее согласие дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается мной письменным заявлением.

(Ф.И.О., подпись лица, дающего согласие)

Примечание:

1. Вместо паспорта могут указываться данные иного основного документа, удостоверяющего личность субъекта персональных данных.
2. Письменное согласие заполняется и подписывается субъектом персональных данных собственноручно в присутствии должностного лица оператора.
3. Перечень персональных данных уточняется исходя из целей получения согласия.

Требования пункта 4 статьи 9
Федерального закона от 27.07.2006 № 152-ФЗ
«О персональных данных»

ФИО, адрес субъекта ПДн, номер
основного документа,
удостоверяющего его личность,
сведения о дате выдачи указанного
документа и выдавшем его органе

Наименование или ФИО и адрес
оператора, получающего согласие
субъекта ПДн

Цель обработки ПДн

Перечень ПДн, на обработку которых
дается согласие субъекта ПДн

Наименование или ФИО и адрес лица,
осуществляющего обработку ПДн по
поручению оператора, если обработка
будет поручена такому лицу

Перечень действий с ПДн, на
совершение которых дается согласие,
общее описание используемых
оператором способов обработки ПДн

Срок, в течение которого действует
согласие субъекта ПДн, а также способ
его отзыва, если иное не установлено
федеральным законом

Подпись субъекта ПДн

Разъяснение
субъекту персональных данных

Я _____
(фамилия, имя, отчество)

паспорт (иной документ, удостоверяющий личность) серия _____ № _____
выдан _____

_____ дата выдачи « _____ » _____ 20 ____ г.

получил(а) разъяснения о юридических последствиях отказа предоставить свои персональные данные БУ «Югра» в соответствии с законодательством Российской Федерации.

В соответствии со статьей 65 Трудового кодекса Российской Федерации субъект персональных данных при приеме на работу и заключении трудового договора, обязан предоставить определенный перечень информации о себе.

Без предоставления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

_____ дата _____ подпись _____ раскфрмла _____

Юридические последствия отказа предоставить персональные данные разъяснил(а):

_____ должность _____ подпись _____ раскфрмла _____

Обязательство
о неразглашении информации, содержащей персональные данные

Я, _____
(фамилия, имя, отчество полностью)

являясь _____ сотрудником БУ «Югра», в _____ должности _____

_____ (Содержит должность и наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____ дата _____ подпись _____ раскфрмла _____

Сводная таблица
действий БУ «Югра» в ответ на запросы субъекта персональных данных или его представителя

№ п/п	Запрос	Действия	Срок	Ответ
1. Запрос субъекта персональных данных или его представителя				
1.1.	Наличие персональных данных	Подтверждение обработки персональных данных	30 дней (согласно п. 1 ст. 20 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – 152-ФЗ))	Подтверждение обработки персональных данных
		Отказ подтверждения обработки персональных данных	30 дней (согласно п. 2 ст. 20 152-ФЗ)	Уведомление об отказе подтверждения обработки персональных данных
1.2.	Ознакомление с персональными данными	Предоставление информации по персональным данным	30 дней (согласно п. 1 ст. 20 152-ФЗ)	Подтверждение обработки персональных данных, а также правовые основания и цели такой обработки
				Способы обработки персональных данных
				Сведения о лицах, которые имеют доступ к персональным данным
				Перечень обрабатываемых персональных данных и источник их получения
				Сроки обработки персональных данных, в том числе сроки их хранения
				Информация об осуществленной или о предполагаемой трансграничной передаче
		Отказ предоставления информации по персональным данным	30 дней (согласно п. 2 ст. 20 152-ФЗ)	Уведомление об отказе предоставления информации по персональным данным
1.3.	Уточнение персональных данных	Изменение персональных данных	7 рабочих дней со дня предоставления уточняющих сведений (согласно п. 3 ст. 20 152-ФЗ)	Уведомление о внесенных изменениях
		Отказ изменения персональных данных	30 дней	Уведомление об отказе изменений персональных данных

Продолжение сводной таблицы

№ п/п	Запрос	Действия	Срок	Ответ
1.4.	Уничтожение персональных данных	Уничтожение персональных данных	7 рабочих дней со дня предоставления сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно п. 3 ст. 20 152-ФЗ)	Уведомление об уничтожении персональных данных
		Отказ уничтожения персональных данных	30 дней	Уведомление об отказе уничтожения персональных данных
1.5.	Отзыв согласия на обработку персональных данных	Прекращение обработки и уничтожение персональных данных	30 дней (согласно п. 5 ст. 21 152-ФЗ)	Уведомление о прекращении обработки и уничтожении персональных данных
		Отказ прекращения обработки и уничтожения персональных данных	30 дней	Уведомление об отказе прекращения обработки и уничтожения персональных данных
1.6.	Недостоверность персональных данных Субъекта	Блокирование персональных данных	с момента получения запроса на период проверки (согласно п. 1 ст. 21 152-ФЗ)	Уведомление о внесенных изменениях
		Изменение персональных данных	7 рабочих дней со дня предоставления уточненных сведений (согласно п. 2 ст. 21 152-ФЗ)	
		Снятие блокировки персональных данных		Уведомление об отказе изменения персональных данных
		Отказ изменения персональных данных	30 дней	

Продолжение сводной таблицы

№ п/п	Запрос	Действия	Срок	Ответ
1.7.	Неправомерность действий с персональными данными Субъекта	Прекращение неправомерной обработки персональных данных	3 рабочих дня (согласно п. 3 ст. 21 152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение персональных данных в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно п. 3 ст. 21 152-ФЗ)	Уведомление об уничтожении персональных данных
1.8.	Достижение целей обработки персональных данных Субъекта	Прекращение обработки персональных данных	30 дней (согласно п. 4 ст. 21 152-ФЗ)	Уведомление об уничтожении персональных данных
		Уничтожение персональных данных		
2. Запрос Уполномоченного органа по защите прав субъектов персональных данных				
2.1.	Информация для осуществления деятельности уполномоченного органа	Предоставление затребованной информации по персональным данным	30 дней (согласно п. 4 ст. 20 152-ФЗ)	Предоставление затребованной информации по персональным данным
2.2.	Неточность персональных данных Субъекта	Блокирование персональных данных	с момента получения запроса на период проверки (согласно п. 1 ст. 21 152-ФЗ)	Уведомление о внесенных изменениях
		Изменение персональных данных	7 рабочих дней со дня предоставления уточненных сведений (согласно п. 2 ст. 21 152-ФЗ)	Уведомление об отказе изменения персональных данных
		Снятие блокировки персональных данных		
		Отказ изменения персональных данных	30 дней	

Продолжение сводной таблицы

№ п/п	Запрос	Действия	Срок	Ответ
2.3.	Неправомерность действий с персональными данными Субъекта	Прекращение неправомерной обработки персональных данных Уничтожение персональных данных в случае невозможности обеспечения правомерности обработки	3 рабочих дня (согласно п. 3 ст. 21 152-ФЗ) 10 рабочих дней (согласно п. 3 ст. 21 152-ФЗ)	Уведомление об устранении нарушений Уведомление об уничтожении персональных данных
2.4.	Достижение целей обработки персональных данных Субъекта	Прекращение обработки персональных данных Уничтожение персональных данных	30 дней с даты достижения цели обработки персональных данных (согласно п.4 ст. 21 152-ФЗ)	Уведомление об уничтожении персональных данных

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в БУ «Югра» требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Правила), разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных, а также определяют основания, порядок и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации.

2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных к требованиям защиты персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в БУ «Югра» организовывается проведение ежегодных проверок.

2.2. Проверки проводятся ответственным за организацию обработки персональных данных совместно с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных и ответственным за эксплуатацию информационной системы персональных данных.

Проверки осуществляются ответственным за организацию обработки ПДн либо комиссией, образуемой руководителем учреждения, в соответствии с ежегодным планом внутренних проверок режима защиты ПДн (плановые проверки) или на основании поступившей информации о нарушениях правил обработки ПДн (внеплановые проверки)

При проведении проверки должны быть полностью, объективно и всесторонне, установлены:

Соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям БУ «Югра»

Соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн

Достаточность (избыточность) ПДн для целей обработки ПДн, заявленных при сборе ПДн

Отсутствие (наличие) объединения, созданных для несовместимых между собой целей, баз данных ИСПДн

Порядок и условия применения организационных и технических мер по обеспечению безопасности ПДн при их обработке, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн

Порядок и условия соблюдения парольной и антивирусной защиты; порядок и условия обеспечения резервного копирования; порядок и условия обновления программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн; порядок и условия применения средств защиты информации

Соблюдение учета носителей ПДн, правил доступа к ПДн, порядка доступа в помещения, в которых ведется обработка ПДн

Наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер; мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; осуществление мероприятий по обеспечению целостности ПДн

По структуре ИСПДн может
быть распределенная,
локальная или автономная

Всего 3 класса защищенности ИС (К₁, К₂,
К₃)

К₁ – самый высокий

К₃ – самый низкий

Класс защищенности ИС определяется
если она является государственной
информационной системой

Перечень информационных систем персональных данных

Наименование ИСПДн	Адрес расположения	Структура ИСПДн	Наличие подключений к ССОП и сетям МНО (Интернет)	Разграничение доступа пользователей	Уровень защищенности ИСПДн	Класс защищенности ИСПДн
«Кадры»	628000, Ханты- Мансийский ав- тономный округ – Югра, г. Ханты- Мансийск, ул. Мира, д. 1	Локальная	Имеется	С разграничением прав доступа	Четвертый (УЗ ₄)	-

Всего 4 уровня защищенности
ПДн (УЗ₁, УЗ₂, УЗ₃, УЗ₄):
УЗ₁ – самый высокий
УЗ₄ – самый низкий

Локальные акты по вопросам обработки ПДн

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утвержден ФСТЭК России
11 февраля 2014 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ
В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ**

2014

18

Содержание базовой меры ИАФ.1:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ИАФ.1	+	+	+	+
Усиление ИАФ.1			1а, 2а, 3	1а, 2а, 3, 4

ИАФ.2 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ УСТРОЙСТВ, В ТОМ ЧИСЛЕ СТАЦИОНАРНЫХ, МОБИЛЬНЫХ И ПОРТАТИВНЫХ

Требования к реализации ИАФ.2: В информационной системе до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

Оператором должен быть определен перечень типов устройств, используемых в информационной системе и подлежащих идентификации и аутентификации до начала информационного взаимодействия.

Идентификация устройств в информационной системе обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

Аутентификация устройств в информационной системе обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

Правила и процедуры идентификации и аутентификации устройств регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ИАФ.2:

1) в информационной системе должна обеспечиваться аутентификация устройств до начала информационного взаимодействия с ними:

а) взаимная аутентификация устройства и средства вычислительной техники (или другого взаимодействующего устройства);

б) аутентификация по уникальным встроенным средствам аутентификации.

ИНСТРУКЦИЯ
по идентификации и аутентификации
пользователей информационных систем персональных данных

1. Общие положения

1.1. Настоящая инструкция определяет в БУ «Югра» порядок действий ответственного за обеспечение безопасности персональных данных (далее - администратора информационной безопасности) и пользователей информационных систем персональных данных (далее - ИСПДн) при прохождении идентификации и аутентификации пользователями в ИСПДн.

1.2. Настоящая Инструкция разработана на основе следующих нормативных документов:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
- Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Данная Инструкция должна содержать следующие сведения:

Порядок идентификации и аутентификации внутренних пользователей, а также устройств, в том числе стационарных, мобильных и портативных

Порядок управления идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

Порядок управления средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

Порядок управления (заведения, активации, блокирования и уничтожения) учетными записями пользователей, в том числе внешних пользователей

Порядок блокирования сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

Перечень действий пользователей, разрешенных до идентификации и аутентификации

ЖУРНАЛ учета машинных носителей персональных данных (стационарные носители)				
№ п/п	Регистрационный номер	Тип и ёмкость	Дата и место установки (использования)	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ учета машинных носителей персональных данных (съёмные носители)						
№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

Идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей; номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации

Ответственным за учет машинных носителей, в большинстве случаев, назначается администратор информационной безопасности

Перечень лиц, физический доступ которых к машинным носителям персональных данных необходим для выполнения ими должностных обязанностей

№ п/п	ФИО	Должность
1.	П.П. Петров	Программист
2.		

Физический доступ к машинным носителям должен предоставляться в соответствии с утвержденным Перечнем лиц, физический доступ которых к машинным носителям персональных данных необходим для выполнения ими должностных обязанностей

ПОРЯДОК уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

1. Общие положения

1.1. Настоящий документ устанавливает порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2. Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

2.1. Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

2.2. Вопрос об уничтожении документов, содержащих персональные данные, рассматривается на заседании Комиссии по защите информации.

2.3. Уничтожение документов производится в присутствии всех членов комиссии, которые несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (проводится комиссией по классификации информационных систем и определению уровней защищенности персональных данных). Результаты уничтожения документов оформляются актом (акт составляется в свободной

ИНСТРУКЦИЯ по регистрации событий безопасности

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с п. 8.5 приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», п. 20.5 приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2. Событие безопасности (информационной) – это идентифицированное возникновение состояния информационной системы персональных данных (далее – ИСПДн) (сегмента, компонента информационной системы персональных данных), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

1.3. Отслеживание событий (проверку), происходивших на автоматизированных рабочих местах (далее – АРМ), осуществляет ответственный за обеспечение безопасности персональных данных (далее – ПДн) в информационных системах персональных данных (далее – администратор информационной безопасности ИСПДн).

1.4. Основными задачами проверки являются:

- контролирование состояния защищенности системы;
- выявление причин произошедших изменений;
- определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к ИСД;
- установление времени изменений.

2. Определение событий безопасности, подлежащих регистрации, их состава, содержания и сроков хранения

2.1. События, происходящие на АРМ, входящих в состав ИСПДн, регистрируются в журналах, приведенных в п. 3.1. настоящей инструкции.

Данная Инструкция должна содержать следующие сведения:

Перечень событий безопасности, подлежащих регистрации, и сроки их хранения

Состав и содержание информации о событиях безопасности, подлежащих регистрации

Порядок сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения

Порядок реагирования на сбой при регистрации событий безопасности

Порядок мониторинга результатов регистрации событий безопасности и реагирования на них

Порядок защиты информации о событиях безопасности, а также должно быть определено должностное лицо, которому предоставляется доступ к записям аудита и функциям управления механизмами регистрации (аудита)

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационных системах
персональных данных

1. Общие требования

1.1. Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководства и сотрудников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все существующие и вновь разрабатываемые ИСПДн.

1.2. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.3. Установка и настройка средств антивирусного контроля осуществляется ответственным за обеспечение безопасности персональных данных (далее - ПДн) в ИСПДн (далее - администратор информационной безопасности ИСПДн).

2. Применение средств антивирусного контроля

2.1. При загрузке автоматизированного рабочего места (далее – АРМ) в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

2.2. Быстрой и полной антивирусной проверке АРМ и сервера подвергаются один раз в неделю.

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по информационно-телекоммуникационным сетям, а также информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень

Данная Инструкция должна содержать следующие сведения:

Порядок применения средств антивирусной защиты
(на рабочих местах, серверах, межсетевых экранах и т.д.)

Порядок установки, конфигурирования и управления средствами антивирусной защиты

Частота периодических проверок компонентов информационных систем персональных данных на наличие вредоносных компьютерных программ (вирусов)

Порядок реагирования при обнаружении в информационных системах персональных данных объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами)

Порядок обновления базы данных признаков вредоносных компьютерных программ (вирусов)

ИНСТРУКЦИЯ

по организации резервного копирования и восстановления программного обеспечения и баз персональных данных в информационных системах персональных данных

1. Общие положения

1.1. Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2. Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных (далее – ИСПДн).

2. Резервируемое программное обеспечение и базы персональных данных

2.1. В ИСПДн резервированию подлежат:

- общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);
- прикладное программное обеспечение, используемое для обработки персональных данных (далее – ПДн) (средства обработки текстов и таблиц, специализированные программы и т.п.);
- базы ПДн (текстовые и табличные файлы, а также файлы баз данных специализированных программ);
- программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

3. Порядок резервирования и хранения резервных копий

3.1. Резервирование общего и прикладного программного обеспечения, программного обеспечения средств защиты информации осуществляется путем создания и хранения резервных копий (дистрибутивов) общего и прикладного программного обеспечения, программного обеспечения средств защиты.

Данная Инструкция должна содержать следующие сведения:

Перечень сведений, подлежащих резервному копированию

Порядок резервного копирования и хранения резервных копий

Периодичность резервного копирования

Порядок восстановления персональных данных из резервных копий и работоспособности информационных систем персональных данных

ИНСТРУКЦИЯ
ответственного за обеспечение
безопасности персональных данных в информационных системах
персональных данных

1. Общие положения

1.1. Ответственный за обеспечение безопасности персональных данных (далее – администратор информационной безопасности) назначается приказом БУ «Югра» и отвечает за обеспечение безопасности заданных характеристик информации (конфиденциальность, целостность и доступность), содержащей персональные данные, в процессе их обработки в информационных системах персональных данных (далее - ИСПДн) БУ «Югра».

1.2. В своей деятельности администратор информационной безопасности руководствуется:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Политикой в отношении обработки персональных данных;
- Настоящей Инструкцией.

1.3. Методическое руководство работой администратора информационной безопасности осуществляет ответственный за организацию обработки персональных данных.

1.4. Настоящая инструкция определяет функции, права и обязанности лица, ответственного за обеспечение безопасности ПДн в ИСПДн.



ИНСТРУКЦИЯ по работе с инцидентами информационной безопасности

1. Общие положения

1.1. Настоящая инструкция устанавливает порядок действий по управлению инцидентами информационной безопасности (далее - ИБ) в БУ «Югра».

1.2. Под инцидентом ИБ понимается событие или совокупность событий, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности.

1.3. Ответственным за выявление инцидентов ИБ и реагирование на них в БУ «Югра» возлагается на администратора информационной безопасности.

2. Порядок выявления инцидентов информационной безопасности и реагирование на них

2.1. В качестве источников информации об инцидентах могут использоваться:

- факты, выявленные руководителями структурных подразделений и сотрудниками БУ «Югра»;
- журналы и оповещения системы защиты информации (далее - СЗИ);
- информация, полученная на основе анализа защищенности ИСПДн и контроля эффективности системы защиты информации (далее – СЗИ);
- запросы и предписания органов надзора за соблюдением прав субъектов ПДн;
- обращения субъектов ПДн с указанием инцидента ИБ;
- другие источники информации.

2.2. Сотрудник БУ «Югра» может выявить признаки наличия инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям, утвержденным в БУ «Югра».

2.3. Выявленные несоответствия дают основания предполагать факт возникновения инцидента ИБ. Любые сведения об инциденте ИБ должны быть незамедлительно переданы выявившим их сотрудником

Данная Инструкция должна содержать следующие сведения:

Перечень лиц, ответственных за выявление инцидентов и реагирование на них

Порядок обнаружения, идентификации и регистрации инцидентов

Способы своевременного информирования лиц, ответственных за выявление инцидентов и реагирования на них, о возникновении инцидентов в информационной системе пользователями и администраторами

Порядок анализа инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий

Порядок принятия мер по устранению последствий инцидентов

Порядок планирования и принятия мер по предотвращению повторного возникновения инцидентов