ГЛАВНОЕ УПРАВЛЕНИЕ ВЕТЕРИНАРИИ ОМСКОЙ ОБЛАСТИ

П Р И К А З

«07» августа 2017 года № 28

г. Омск

О внесении изменений в приказ Главного управления ветеринарии Омской области от 12 апреля 2017 года № 13 «Об обработке персональных данных в Главном управлении ветеринарии Омской области»

1. Внести в приказ Главного управления ветеринарии Омской области от 12 апреля 2017 года № 13 «Об обработке персональных данных в Главном управлении ветеринарии Омской области» следующие изменения:

1) в пункте 1:

- подпункт 6 исключить;

- в подпункте 7 слова «ведется обработка персональных данных» заменить словами «происходит обработка персональных данных с использованием средств автоматизации»;

- в подпункте 8 слова «перечень должностей работников Главного управления, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных» заменить словами «типовую форму согласия на включение персональных данных в общедоступные источники персональных данных Главного управления»;

- в подпункте 14 слова «положение об обработке персональных данных» заменить словами «должностную инструкцию лица, ответственного за организацию обработки персональных данных в Главном управлении»;

2) пункт 3 изложить в следующей редакции:

«3. Ответственный за организацию обработки персональных данных в Главном управлении назначается распоряжением Главного управления ветеринарии Омской области.»;

3) пункт 9 приложения № 2 исключить;

4) приложение № 6 исключить;

5) приложения № 7, 8, 10, 11, 13, 14 изложить в новой редакции согласно приложениям № 1- 6 к настоящему приказу.

2. Настоящий приказ вступает в силу после его подписания и официального опубликования на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru).

Начальник Главного управления В.П. Плащенко

Приложение № 1
к приказу Главного управления
ветеринарии Омской области
от 07 августа 2017 г. № 28

«Приложение № 7
к приказу Главного управления
ветеринарии Омской области
от 12 апреля 2017 г. № 13

ПОРЯДОК
доступа работников Главного управления в помещения, в которых происходит обработка персональных данных с использованием средств автоматизации

Термины и определения

АРМ	– Автоматизированное рабочее место
Ответственный за организацию обработки персональных данных в Главном управлении	Ответственный за организацию обработки ПДн
Помещение контролируемой зоны	– Помещение Главного управления, расположенное в пределах контролируемой зоны, в котором происходит обработка персональных данных
ПДн	– Персональные данные
СКЗИ	– Средства криптографической защиты информации
Спецпомещение	– Помещение контролируемой зоны, в котором размещено, хранится СКЗИ, используемое для обеспечения безопасности ПДн, и (или) носитель ключевой, аутентифицирующей и парольной информации СКЗИ

1. Общие положения

1.1. Настоящий Порядок доступа работников в помещения, в которых происходит обработка ПДн с использованием средств автоматизации (далее – Порядок), устанавливает единые требования к доступу работников Главного управления в помещения контролируемой зоны и спецпомещения с целью обеспечения безопасности СКЗИ, ПДн, при их обработке в Главном управлении, а так же направлен на предотвращение компрометации криптоключей.

1.2. Настоящий Порядок разработан в соответствии с:

- постановлением Правительства Российской Федерации от 21 марта 2012 года № 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»;
- приказом ФСТЭК России от 11февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;
- приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава 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 ФАПСИ от 13 июня 2001 года № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

1.3. Настоящий Порядок обязателен для применения и исполнения всеми работниками Главного управления, осуществляющими обработку ПДн, в том числе с использованием СКЗИ.

1.4. Ответственность за соблюдением положений настоящего Порядка несут работники структурных подразделений Главного управления, обрабатывающие ПДн, в том числе с использованием СКЗИ.

1.5. Контроль соблюдения требований настоящего Порядка обеспечивает ответственный за организацию обработки ПДн.

2. Требования к помещениям контролируемой зоны

2.1. Бесконтрольный доступ посторонних лиц в помещения контролируемой зоны должен быть исключён.

2.2. Помещения контролируемой зоны должны быть оборудованы прочными входными дверьми и запирающими устройствами.

2.3. Для предотвращения просмотра извне помещений контролируемой зоны, их окна должны быть защищены жалюзи или непрозрачными шторами.

2.4. К спецпомещениям, дополнительно к требованиям, установленным пунктами 2.1-2.3 настоящего Порядка, предъявляются требования по безопасности, указанные в разделе 4 настоящего Порядка.

3. Доступ в помещения контролируемой зоны

3.1. Перечень работников Главного управления, имеющих право доступа в помещения контролируемой зоны для выполнения ими служебных (трудовых) обязанностей, приведен в Приложении к настоящему Порядку.

3.2. Доступ работника Главного управления в помещения контролируемой зоны оформляется после ознакомления ответственным за организацию обработки ПДн работника Главного управления, непосредственно осуществляющего обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами Главного управления по вопросам обработки персональных данных.

3.3. Доступ посторонних лиц в помещения контролируемой зоны должен осуществляется только в присутствии работника Главного управления, имеющего право доступа в помещения контролируемой зоны для выполнения им служебных (трудовых) обязанностей.

3.4. В обычных условиях помещения контролируемой зоны должны быть вскрыты только работниками Главного управления, имеющими право доступа в помещения контролируемой зоны в соответствии с Приложением к настоящему Порядку.

3.5. На момент присутствия посторонних лиц в помещении контролируемой зоны, работником Главного управления, имеющим право доступа в помещение контролируемой зоны, должны быть приняты меры по недопущению ознакомления посторонних лиц с ПДн (мониторы повёрнуты в сторону от посетителей, документы убраны с обозреваемого посетителем пространства, либо находятся в непрозрачной папке или накрыты чистыми листами бумаги).

3.6. К доступу в спецпомещения, дополнительно к требованиям, установленным пунктами 3.1-3.5 настоящего Порядка, предъявляются требования по безопасности, указанные в разделе 5 настоящего Порядка.

4. Требования к спецпомещениям

4.1. Спецпомещения должны иметь прочные входные двери с надежными механическими замками (минимум - с двумя комплектами ключей), обеспечивающими постоянное закрытие дверей спецпомещений на замок и их

открытие только для санкционированного прохода с целью исключения возможности неконтролируемого проникновения или пребывания в них посторонних лиц.

4.2. Один комплект ключей используется отделом в постоянной работе, второй комплект сдается начальником отдела, эксплуатирующего спецпомещение, Ответственному за организацию обработки ПДн под роспись в опечатанном тубусе.

4.3. Спецпомещения должны быть оснащены охранной сигнализацией и (или) устройствами для опечатывания входной двери.

5. Доступ в спецпомещения

5.1. Перечень работников Главного управления, имеющих право доступа в спецпомещения для выполнения ими служебных (трудовых) обязанностей, приведен в Приложении к настоящему Порядку.

5.2. Обслуживание технического оборудования, на котором установлены СКЗИ, а так же смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

5.3. Двери спецпомещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода посторонних лиц.

5.4. Для доступа в закрытое спецпомещение в начале рабочего дня работники, внесенные в утвержденный Перечень получают комплект ключей, который находится в опечатанном тубусе, у сторожа. Проверяют целостность пластилиновой печати и сравнивают ее данные с данными печати. В случае отсутствия данных печати или нарушении целостности печати ставится в известность Ответственный за организацию обработки ПДн.

При этом делается запись в журнале, с указанием ФИО лица получившего и выдавшего комплект ключей, даты, времени и подписи указанных лиц.

5.5. Работники, внесенные в утвержденный Перечень, перед вскрытием спецпомещения проверяют целостность пластилиновой печати на двери спецпомещения и сравнивают ее данные с данными печати. В случае отсутствия данных печати или нарушении целостности печати ставится в известность Ответственный за организацию обработки ПДн, спецпомещение не вскрывается до принятия им соответствующего решения.

5.6. В течение рабочего дня работники, внесенные в утвержденный Перечень:

- при оставлении последним спецпомещения - закрывают дверь спецпомещения на замок и опечатывают их личной печатью;
- не покидают последними спецпомещение, если в нем находятся лица, не внесенные в Перечень;
- при обнаружении фактов нарушения режима доступа ставят в известность Ответственного за организацию обработки ПДн;
- при посещении спецпомещения посторонними лицами с целями проведения контрольных, проверочных мероприятий, а также работ по обслуживанию помещений и их инженерно-технических средств ставят в

известность об этом Ответственного за организацию обработки ПДн и начальника отдела.

5.7. В конце рабочего дня работники, внесенные в утвержденный Перечень сдают комплект ключей, который находится в опечатанном тубусе, сторожу.

При этом делается запись в журнале, с указанием ФИО лица сдавшего и принявшего комплект ключей, даты, времени и подписи указанных лиц.

5.8. Обслуживание спецпомещения (уборка или различный ремонт спецпомещения, инженерно-технического оборудования) проводится обслуживающим персоналом только в присутствии и под присмотром хотя бы одного из работника, имеющего право самостоятельно находиться в Помещении.

6. Порядок доступа работников в помещения Главного управления в нерабочее время

6.1. В нерабочее время помещения контролируемой зоны должны быть закрыты на замок. При этом материальные носители ПДн должны быть убраны в запираемые шкафы (сейфы), АРМ выключены или заблокированы.

6.2. В нерабочее время спецпомещения должны быть закрыты на замок, опечатаны и(или) должна быть произведена активация охранной сигнализации. При этом материальные носители ПДн и ключевые носители должны быть убраны в запираемые шкафы (сейфы), АРМ выключены или заблокированы.

6.3. Доступ работников в помещения Главного управления во внерабочее время регламентируется Порядком доступа работников в помещения Главного управления ветеринарии Омской области во внерабочее время, утвержденного распоряжением Главного управления ветеринарии Омской области от 17 июля 2017 года № 140.

7. Правила доступа в помещения Главного управления в нештатных ситуациях

7.1. К нештатным ситуациям относятся:

- прорывы водопровода или канализации;
- пожары;
- природные катаклизмы.

7.2. При нештатной ситуации, грозящей уничтожением или повреждением ПДн, СКЗИ, а так же компрометацией криптоключей, работнику Главного управления, обнаружившему факт возникновения нештатной ситуации, следует:

- немедленно оповестить работника Главного управления, ответственного за обслуживание административного здания;
- немедленно сообщить своему непосредственному руководителю;
- немедленно оповестить других работников и принять все меры для самостоятельной оперативной защиты помещения;

немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);

- по возможности, осуществить эвакуацию материальных носителей ПДн, СКЗИ, а так же криптоключи в безопасное место.

7.3. Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» беспрепятственно допускаются в помещения Главного управления для ликвидации нештатной ситуации или оказания медицинской помощи.

Приложение
к Порядку доступа работников Главного управления в помещения, в которых происходит обработка персональных данных с использование средств автоматизации

Перечень лиц, имеющих право доступа в помещения Главного управления

Место нахождения помещения	Наименование структурного подразделения	Ф.И.О. работника	Тип помещения
2 этаж каб. № 5	Отдел организации противоэпизоотических мероприятий	Юхимук Евгения Владимировна	Спецпомещение
		Чардынцев Дмитрий Михайлович	
2 этаж каб. № 7	Отдел экономики, финансирования и учета	Зюлина Анастасия Николаевна	Спецпомещение
		Таубе Рената Викторовна	
		Галеева Ирина Владимировна	
2 этаж каб. № 8	Специалист по организационно-правовой и кадровой работе	Савилов Дмитрий Александрович	Помещение контролируемой зоны
1 этаж каб. б/н	Отдел государственного ветеринарного надзора	Околелов Константин Владимирович	Спецпомещение
		Секин Евгений Юрьевич	
		Степанов Денис Николаевич	
1 этаж каб. б/н	Отдел организации противоэпизоотических мероприятий	Раков Иван Андреевич	Спецпомещение

»

Приложение № 2
к приказу Главного управления
ветеринарии Омской области
от 07 августа 2017 г. № 28

«Приложение № 8
к приказу Главного управления
ветеринарии Омской области
от 12 апреля 2017 г. № 13

ТИПОВАЯ ФОРМА
согласия на включение персональных данных в общедоступные источники персональных данных Главного управления

Я, _____
(Ф.И.О.)
_____
(вид основного документа, удостоверяющего личность)
серия _____ номер _____
_____
(кем и когда выдан)
проживающий(ая) по адресу: _____
_____

даю согласие на обработку моих персональных данных свободно, своей волей и в своем интересе и принимаю решение о включении моих персональных данных в общедоступные источники персональных данных (доски почета, новостные публикации, телефонные и иные справочники, включая электронные, размещенные в сети Интернет; официальный сайт Главного управления).

Наименование и адрес оператора, получающего согласие субъекта персональных данных:

Главное управление ветеринарии Омской области; 644024 г. Омск, ул. 30 лет ВЛКСМ, д.40.

Цели обработки персональных данных:

включение персональных данных в общедоступные источники, информирование граждан об общественно значимых событиях и достижениях.

Перечень персональных данных, на которое дается согласие субъекта персональных данных:

- фамилия, имя, отчество (при наличии);

_____.
(иные персональные данные)

Перечень действий с персональными данными, на совершение которых дается согласие:

сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, передача (распространение, предоставление, доступ), блокирование, уничтожение.

Обработка персональных данных осуществляется с применением средств автоматизации, а так же без применения таких средств.

Срок, в течение которого действует согласие субъекта персональных данных:

- по достижению цели обработки персональных данных;

- до момента отзыва настоящего согласия субъектом персональных данных;

- при ликвидации Главного управления.

Отзыв настоящего согласия субъектом персональных данных с требованием о прекращении обработки его персональных данных осуществляется на основании его письменного обращения в Главное управление.

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)

_____»

Приложение № 3
к приказу Главного управления
ветеринарии Омской области
от 07 августа 2017 г. № 28

«Приложение № 10
к приказу Главного управления
ветеринарии Омской области
от 12 апреля 2017 г. № 13

ТИПОВАЯ ФОРМА
согласия на обработку персональных данных в Главном управлении

Я, _____
(Ф.И.О.)

_____
(вид основного документа, удостоверяющего личность)

серия _____ номер _____

_____
(кем и когда выдан)

проживающий(ая) по адресу: _____

_____

свободно, своей волей и в своем интересе даю согласие на обработку следующих моих персональных данных:

_____

_____

_____
(перечень персональных данных)

Наименование и адрес оператора, получающего согласие субъекта персональных данных:

Главное управление ветеринарии Омской области; 644024 г. Омск, ул. 30 лет ВЛКСМ, д.40.

Цели обработки персональных данных:

_____

_____

_____

Перечень персональных данных, на которое дается согласие субъекта персональных данных:

- фамилия, имя, отчество;

_____.
(иные персональные данные)

Перечень действий с персональными данными, на совершение которых дается согласие:

сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, передача (распространение, предоставление, доступ), блокирование, уничтожение.

Обработка персональных данных осуществляется с применением средств автоматизации, а так же без применения таких средств.

Срок, в течение которого действует согласие субъекта персональных данных:

- по достижению цели обработки персональных данных;
- до момента отзыва настоящего согласия субъектом персональных данных;
- при ликвидации Главного управления.

Отзыв настоящего согласия субъектом персональных данных с требованием о прекращении обработки его персональных данных осуществляется на основании его письменного обращения в Главное управления информационных технологий и связи Омской области.

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)

_____»

_____

Приложение № 4
к приказу Главного управления
ветеринарии Омской области
от 07 августа 2017 г. № 28

«Приложение № 11
к приказу Главного управления
ветеринарии Омской области
от 12 апреля 2017 г. № 13

ТИПОВАЯ ФОРМА
разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в Главное управление

Мне,_____,
(фамилия, имя, отчество (при наличии))
разъяснены юридические последствия отказа предоставить свои персональные данные уполномоченным лицам Главного управления.

В соответствии _____,
(реквизиты Федерального закона, на основании которого предоставляются персональные данные)
Главным управлением определен перечень персональных данных, которые субъект персональных данных обязан представить уполномоченным лицам Главного управления в связи
с_____.
(цель обработки персональных данных)

В случае отказа предоставить свои персональные данные, Главное управление не сможет на законных основаниях осуществлять такую обработку, что приведет
к_____
_____
(указание юридических последствий)

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

_____»

_____

Приложение № 5
к приказу Главного управления
ветеринарии Омской области
от 07 августа 2017 г. № 28

«Приложение № 13
к приказу Главного управления
ветеринарии Омской области
от 12 апреля 2017 г. № 13

Перечень
информационных систем персональных данных в Главном управлении информационных технологий и связи Омской области

1) Государственная информационная система Омской области «СМЭВ»;
2) Информационная система персональных данных «1С»;
3) Информационная система персональных данных «Резерв»;
4) Информационная система персональных данных «Астрал-Отчетность»;
5) Информационная система персональных данных «Ветис»;
6) Информационная система персональных данных «Награды».

_____»

_____

Приложение № 6
к приказу Главного управления
ветеринарии Омской области
от 07 августа 2017 г. № 28

«Приложение № 14
к приказу Главного управления
ветеринарии Омской области
от 12 апреля 2017 г. № 13

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
лица, ответственного за организацию обработки персональных данных в Главном управлении

1. Общие положения

1.1. Лицо, ответственное за организацию обработки персональных данных в Главном управлении (далее – ответственный) с использованием средств автоматизации и без использования таких средств, а также доступ к персональным данным в Главном управлении.

1.2. Ответственный подчиняется начальнику Главного управления.

2. Должностные обязанности

Ответственный обязан:

2.1. Организовывать обработку и использование персональных данных в Главном управлении исключительно в целях, предусмотренных нормативными правовыми актами Российской Федерации.

2.2. Организовывать обеспечение безопасности персональных данных требуемому уровню защищенности.

2.3. Осуществлять контроль содержания и объема обрабатываемых персональных данных и соответствия их перечню, утвержденному в Главном управлении.

2.4. Осуществлять внутренний контроль соблюдения требований законодательства Российской Федерации при обработке персональных данных, в том числе требований к защите персональных данных.

2.5. Осуществлять контроль приема и обработки запросов субъектов персональных данных или их представителей.

2.6. Осуществлять контроль выполнения требований организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в информационных системах Главного управления.

2.8. Организовывать работы по контролю работоспособности технических средств защиты персональных данных, доступ в помещения Главного управления,

в которых производится обработка персональных данных, средств защиты информации от несанкционированного доступа.

2.9. Доводить до сведения работников Главного управления положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

3. Права

Ответственный имеет право:

3.1. Запрашивать у работников Главного управления информацию, необходимую для реализации полномочий.

3.2. Требовать от всех пользователей информационных систем персональных данных Главного управления выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

3.3. Требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.

3.4. Участвовать в разработке мероприятий по совершенствованию безопасности персональных данных.

3.5. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемых персональных данных и технических средств из состава информационных систем.

3.6. Принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации.

3.7. Вносить начальнику Главного управления предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных или нарушения режима конфиденциальности.

3.8. Вносить начальнику Главного управления предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке.

4. Ответственность

4.1. За ненадлежащее исполнение или неисполнение настоящей инструкции, а также за нарушение требований законодательства о персональных данных ответственный, несет предусмотренную законодательством Российской Федерации ответственность.

_____»

_____