ГОСУДАРСТВЕННАЯ ИНСПЕКЦИЯ ПО ОХРАНЕ ОБЪЕКТОВ КУЛЬТУРНОГО НАСЛЕДИЯ НОВОСИБИРСКОЙ ОБЛАСТИ

ПРИКАЗ

20.07.2023 № 115

Об организации обработки персональных данных в государственной инспекции по охране объектов культурного наследия Новосибирской области

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» **п р и к а з ы в а ю:**

1. Утвердить:

1) Инструкцию по организации антивирусной защиты в информационных системах персональных данных согласно приложению № 1 к настоящему приказу;

2) Инструкцию по выявлению инцидентов безопасности и реагированию на них в информационных системах персональных данных согласно приложению № 2 к настоящему приказу;

3) Инструкцию об организации учета, хранения и выдачи машинных носителей информации в информационных системах персональных данных согласно приложению № 3 к настоящему приказу;

4) Инструкцию по организации парольной защиты в информационных системах персональных данных согласно приложению № 4 к настоящему приказу;

5) Инструкцию о порядке работы при подключении к информационно-телекоммуникационным сетям международного информационного обмена согласно приложению № 5 к настоящему приказу;

6) Инструкцию о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации, в информационных системах персональных данных согласно приложению № 6 к настоящему приказу;

7) Инструкцию по учёту лиц, допущенных к работе в информационных системах персональных данных согласно приложению № 7 к настоящему приказу;

8) Инструкцию по эксплуатации средств защиты информации в информационной системе персональных данных государственной инспекции по охране объектов культурного наследия Новосибирской области согласно приложению № 8 к настоящему приказу;

9) Инструкцию по работе пользователей в информационных системах персональных данных согласно приложению № 9 к настоящему приказу;

10) Инструкцию о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных систем персональных данных согласно приложению № 10 к настоящему приказу;

11) Инструкцию системного администратора информационных систем персональных данных согласно приложению № 11 к настоящему приказу;

12) Типовое обязательство должностного лица государственной инспекцией по охране объектов культурного наследия Новосибирской области, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (трудового договора) прекратить обработку персональных данных, ставших ему известными в связи с исполнением должностных обязанностей согласно приложению № 12 к настоящему приказу;

13) Перечень информационных систем государственной инспекции по охране объектов культурного наследия Новосибирской области согласно приложению № 13 к настоящему приказу;

14) Перечень обязанностей лиц, осуществляющих обработку персональных данных, либо имеющих доступ к персональным данным согласно приложению № 14 к настоящему приказу;

15) Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных согласно приложению № 15 к настоящему приказу;

16) Порядок доступа в помещения государственной инспекции по охране объектов культурного наследия Новосибирской области согласно приложению № 16 к настоящему приказу;

17) Правила рассмотрения запросов субъектов персональных данных или их представителей; согласно приложению № 17 к настоящему приказу;

18) Правила работы с обезличенными персональными данными согласно приложению № 18 к настоящему приказу;

19) Перечень должностей в государственной инспекции по охране объектов культурного наследия Новосибирской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным согласно приложению № 19 к настоящему приказу;

20) Перечень должностей в государственной инспекции по охране объектов культурного наследия Новосибирской области, исполнение обязанностей по которым связано с ответственностью за проведение мероприятий по обезличиванию обрабатываемых персональных данных согласно приложению № 20 к настоящему приказу;

21) Инструкцию ответственного за организацию обработки персональных данных согласно приложению № 21 к настоящему приказу;

22) Политику в отношении обработки персональных данных согласно приложению № 22 к настоящему приказу;

23) Правила обработки персональных данных, осуществляемой без использования средств автоматизации согласно приложению № 23 к настоящему приказу;

24) Типовую форму согласия субъекта персональных данных на обработку персональных данных в государственной инспекции по охране объектов культурного наследия Новосибирской области (для государственных гражданских служащих государственной инспекции по охране объектов культурного наследия Новосибирской области) согласно приложению № 24 к настоящему приказу;

25) Типовую форму согласия субъекта персональных данных на обработку персональных данных (для лиц, замещающих должности, не относящиеся к должностям государственной гражданской службы в государственной инспекции по охране объектов культурного наследия Новосибирской области) согласно приложению № 25 к настоящему приказу;

26) Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные и (или) дать согласие на их обработку согласно приложению № 26 к настоящему приказу;

27) Журнал учета лиц, допущенных к работе в информационных системах персональных данных государственной инспекции по охране объектов культурного наследия Новосибирской области согласно приложению № 27 к настоящему приказу;

28) Журнал учета средств защиты информации, эксплуатационной и технической документации к ним согласно приложению № 28 к настоящему приказу;

29) Журнал учета машинных носителей информации в информационных системах персональных данных согласно приложению № 29 к настоящему приказу.

30) Журнал учета обращений субъектов персональных данных обратившихся в государственную инспекцию по охране объектов культурного наследия Новосибирской области согласно приложению № 30 к настоящему приказу;

2. Признать утратившим силу приказ государственной инспекции по охране объектов культурного наследия Новосибирской области от 01.04.2020 № 33 «О защите персональных данных».

3. Контроль исполнения настоящего приказа оставляю за собой.

Начальник инспекции Е.В. Макавчик

Приложение № 1

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Инструкция
по организации антивирусной защиты в информационных системах персональных данных

1. Общие требования

1.1. Настоящая Инструкция по организации антивирусной защиты в информационных системах персональных данных (далее – Инструкция) определяет требования к организации защиты информационных систем персональных данных (далее – ИСПДн) государственной инспекции по охране объектов культурного наследия Новосибирской области) (далее – ГИО ОКН НСО) от разрушающего воздействия вредоносных компьютерных программ (компьютерных вирусов) и устанавливает ответственность сотрудников ГИО ОКН НСО, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. К использованию в ИСПДн допускаются только средства антивирусной защиты прошедшие в установленном порядке процедуру оценки соответствия.

1.3. Установка и настройка средств антивирусной защиты осуществляется специально назначенным лицом (администратором безопасности информации), в соответствии с руководствами по применению конкретных средств антивирусной защиты.

2. Применение средств антивирусной защиты

2.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных машинных носителях (USB «флэш»-накопителях, накопителях на гибких магнитных дисках, оптических компакт-дисках и прочие) перед копированием в ИСПДн.

2.2. Накопители на жестких дисках, и оперативная память АРМ должны находятся под постоянным контролем средства антивирусной защиты.

2.3. Полная проверка всех файлов ИСПДн должна выполняться по расписанию не реже одного раза в неделю, а также по запросу пользователя ИСПДн.

2.4. Быстрая проверка файлов ИСПДн должна выполняться автоматически после запуска средства антивирусной защиты.

2.5. Должна проводиться автоматическая проверка подключаемых съемных машинных носителей.

2.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения автоматизированного рабочего места (далее - АРМ), администратором безопасности информации должна быть выполнена антивирусная проверка соответствующего АРМ.

2.7. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИСПДн самостоятельно или вместе с администратором безопасности информации должен провести внеочередную антивирусную проверку своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИСПДн обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности информации;

провести анализ необходимости дальнейшего использования зараженных файлов;

провести лечение или уничтожение зараженных файлов.

2.8. Обновление базы данных признаков вредоносных компьютерных программ средства антивирусной защиты должно осуществляться не реже чем один раз в два часа в автоматическом режиме со специального сервера обновлений средства антивирусной защиты.

3. Ответственность

3.1. Ответственность за организацию и проведение мероприятий по антивирусной защите в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности информации.

3.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников ГИО ОКН НСО, являющихся пользователями ИСПДн.

3.3. Периодический контроль за состоянием антивирусной защиты в ИС АП ЕГИСМ, а также за соблюдением установленного порядка антивирусной защиты и выполнением требований настоящей Инструкции осуществляется администратором безопасности информации.

Приложение № 2

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Инструкция
по выявлению инцидентов безопасности и реагированию на них в информационных системах персональных данных

1. Общие положения

1.1. Настоящая Инструкция по выявлению инцидентов безопасности и реагированию на них в информационных системах персональных данных (далее - Инструкция) устанавливает порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления, разбирательства и предотвращения иных инцидентов информационной безопасности в информационных системах персональных данных (далее – ИСПДн) государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО).

1.2. Инструкция разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3. Настоящий Инструкция обязателен к соблюдению всеми сотрудниками ГИО ОКН НСО, участвующими в выявлении, разбирательстве и предотвращении инцидентов безопасности информации в ИСПДн.

1.4. Разбирательство по всем инцидентам безопасности информации проводится ответственным за обеспечение безопасности персональных данных и администратором безопасности информации с привлечением, в необходимых случаях руководителей и сотрудников других подразделений.

1.5. Разбирательство инцидентов безопасности информации, затрагивающих два или более подразделения ГИО ОКН НСО, проводится с ответственным за обеспечение безопасности персональных данных и администратором безопасности информации с привлечением руководителей соответствующих подразделений.

2. Выявление инцидента безопасности информации

2.1. Основными источниками информации об инцидентах безопасности информации являются:

факты, выявленные ответственным за обеспечение безопасности персональных данных, администратором безопасности информации, а также другими сотрудниками организации.

результаты работы средств мониторинга безопасности информации результаты проверок и аудита (внутреннего или внешнего);

обращения субъектов персональных данных с указанием инцидента безопасности информации;

запросы и предписания органов надзора за соблюдением прав субъектов персональных данных;

другие источники информации.

2.2. Сотрудник ГИО ОКН НСО может выявить признаки наличия инцидента безопасности информации путем анализа текущей ситуации на предмет ее соответствия требованиям утвержденных в ГИО ОКН НСО для ИСПДн. Выявленные несоответствий дают основания предполагать факт возникновения инцидента безопасности информации. Любые сведения о происшествие или инциденте безопасности информации должны быть незамедлительно переданы выявившим их сотрудником ответственному за обеспечение безопасности персональных данных и администратору безопасности информации любым доступным способом.

2.3. Сотрудники ГИО ОКН НСО при подозрении на инцидент безопасности информации обязаны также дополнительно уведомить ответственного за обеспечение безопасности персональных данных.

3. Анализ исходной информации и принятие решения о проведении разбирательства.

3.1. Ответственный за обеспечение безопасности персональных данных после получения информации о предполагаемом инциденте безопасности информации незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа Ответственный за обеспечение безопасности персональных данных проводит проверку наличия в выявленном факте нарушений.

3.2. По усмотрению ответственного за обеспечение персональных данных единичный инцидент безопасности информации, не приведший к негативным последствиям и совершенный сотрудником ГИО ОКН НСО впервые, фиксируется ответственным за обеспечение безопасности персональных данных в карточке данных «Инциденты безопасности информации» (приложение №1) с присвоением статуса «Разбирательство не требуется».

3.3. В случае наличия признаков инцидента безопасности в полученной информации, ответственный за обеспечение безопасности персональных данных определяет предварительную степень важности инцидента безопасности информации и принимает решение о необходимости проведения разбирательства, инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

3.4. В срок не более 3 (трех) рабочих дней с момента поступления информации об инциденте безопасности информации, ответственный за обеспечение безопасности персональных данных определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.

4. Разбирательство инцидента безопасности информации.

4.1. Цели и этапы разбирательства инцидента безопасности информации:

4.1.1. Целями разбирательства инцидентов безопасности информации являются:

выработка организационных и технических решений, направленных на снижение рисков нарушения безопасности информации, предотвращение и минимизацию подобных нарушений в будущем;

защита прав установленных законодательством Российской Федерации;

защита репутации ГИО ОКН НСО и его ресурсов;

обеспечение безопасности персональных данных;

обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых в ИСПДн;

предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.1.2. Разбирательство инцидента безопасности информации, состоит из следующих этапов:

подтверждение/опровержение факта возникновения инцидента безопасности информации;

подтверждение/корректировка уровня значимости инцидента безопасности информации;

уточнение дополнительных обстоятельств (деталей) инцидента безопасности информации;

получение (сбор) доказательств возникновения инцидента безопасности информации, обеспечение их сохранности и целостности;

минимизация последствий инцидента безопасности информации;

информирование и консультирование персонала ГИО ОКН НСО по действиям обнаружения, устранения последствий и предотвращения инцидентов безопасности информации;

разработка мероприятий по обнаружению и/или предупреждению инцидентов безопасности информации.

4.2. Создание Рабочей группы для проведения расследования инцидента безопасности информации:

При необходимости ответственный за обеспечение безопасности персональных данных незамедлительно уведомляет руководство ГИО ОКН НСО о факте инцидента безопасности информации и инициирует подготовку Распоряжения о создании Рабочей группы для разбирательства указанного инцидента безопасности информации. Подготовка, согласование и организация издания распоряжения о создании Рабочей группы по разбирательству инцидента безопасности информации осуществляется в установленном порядке

распоряжением за подписью руководства ГИО ОКН НСО. В Распоряжении по представлению ответственного за обеспечение безопасности персональных данных определяются: Руководитель Рабочей группы, состав Рабочей группы, сроки разбирательства инцидента безопасности информации, при необходимости определяются дополнительные полномочия членов Рабочей группы. Рабочая группа может состоять из ответственного за обеспечение безопасности персональных данных, администратора безопасности информации и сотрудников других подразделений ГИО ОКН НСО в зависимости от характера бизнес-процессов и ресурсов, затронутых инцидентом безопасности информации.

Взаимодействие между членами Рабочей группы осуществляется в рабочем порядке с соблюдением при этом требований конфиденциальности. При необходимости проводятся заседания Рабочей группы, время, место и темы которых определяются ее Руководителем.

4.3. Порядок проведения разбирательства инцидента безопасности:

4.3.1. В процессе проведения разбирательства инцидента безопасности информации обязательными для установления являются:

дата и время совершения инцидента безопасности информации;

ФИО, должность и подразделение нарушителя безопасности информации;

уровень критичности инцидента безопасности;

обстоятельства и мотивы совершения инцидента безопасности информации;

информационные ресурсы, затронутые инцидентом безопасности информации;

характер и размер реального и потенциального ущерба;

обстоятельства, способствовавшие совершению инцидента безопасности информации.

4.3.2. В случае проведения временного отключения прав доступа у предполагаемого нарушителя безопасности информации информация об отключении прав доступа администратором безопасности информации направляется ответственному за обеспечение безопасности персональных данных.

4.3.3. После получения необходимой информации по инциденту безопасности информации осуществляющий разбирательство сотрудник проводит анализ полученных данных.

4.3.4. Ответственный за обеспечение безопасности персональных данных запрашивает у нарушителя безопасности информации объяснительную записку. Объяснительная записка должна быть составлена, подписана нарушителем безопасности информации и представлена ответственному за обеспечение безопасности персональных данных. В случае отказа нарушителя безопасности информации предоставить объяснительную записку ответственному за обеспечение безопасности персональных данных составляется акт.

4.3.5. Ответственный за обеспечение безопасности персональных данных проводит оценку негативных последствий от реализации инцидента безопасности информации. В ходе данной оценки учитываются:

прямой финансовый ущерб;

репутационный ущерб;

потенциальный ущерб;

косвенные потери, связанные с недоступностью сервисов, потерей информации;

другие виды ущерба или аспекты негативных последствий для ГИО ОКН НСО или субъектов персональных данных.

4.3.6. С целью минимизации последствий инцидента безопасности информации возможно временное отключение прав доступа сотрудника к ИСПДн на время проведения расследования предварительно сделав заявку. Подобное отключение инициируется ответственным за обеспечение безопасности персональных данных с обязательным предварительным устным согласованием с ответственным за организацию обработки персональных данных.

4.3.7. В случае, если у нарушителя безопасности были отключены права доступа к ИПСДн на время проведения разбирательства, то по его результатам ответственный за обеспечение безопасности персональных данных по согласованию с ответственным за организации обработки персональных данных принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имеющихся у нарушителя безопасности информации прав доступа к ИСПДн либо инициирует официальную процедуру отмены (изменения) прав доступа к ИСПДн. Если нарушение безопасности информации было вызвано незнанием нарушителем безопасности правил (технологии) работы в ИСПДн, то основанием для возврата прав доступа является успешное прохождение повторного инструктажа ответственным за обеспечение безопасности персональных данных и администратором безопасности информации, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами ГИО ОКН НСО по безопасности информации.

4.3.8. Восстановление временно отключенных у нарушителя безопасности прав доступа к ИСПДн (разблокировка пользователя) может производиться только администратором безопасности информации после согласования с ответственным за обеспечение безопасности персональных данных.

5. Оформление результатов проведенного разбирательства

5.1. Собранная в процессе разбирательства инцидента безопасности информации информация фиксируется ответственным за обеспечение безопасности персональных данных в картотеке данных «Инциденты безопасности информации» и учитывается при подготовке итогового заключения по инциденту безопасности (Приложение №1).

5.2. Ответственный за обеспечение безопасности персональных данных формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента безопасности информации.

5.3. Итоговое заключение по инциденту безопасности информации ответственный за обеспечение безопасности персональных данных направляет ответственному за организацию обработки персональных данных.

5.4. Осуществляющий разбирательство сотрудник фиксирует завершение разбирательства в карточке «Инциденты безопасности информации» и присваивает инциденту статус «Разбирательство завершено».

5.5. Ответственный за обеспечение безопасности персональных данных, при необходимости определения правовой оценки инцидента безопасности, может обратиться за консультациями в юридическое подразделение ГИО ОКН НСО.

5.6. В случае выявления в инциденте безопасности информации признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий ответственный за обеспечение безопасности персональных данных передает все материалы по инциденту безопасности информации руководству ГИО ОКН НСО для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

5.7. Ответственный за обеспечение безопасности персональных данных фиксирует полученную дополнительную информацию в карточке данных «Инциденты безопасности информации» и информирует ответственного за организацию обработки персональных данных.

6. Завершение разбирательства, превентивные мероприятия.

6.1. По завершению разбирательства инцидента безопасности информации, ответственный за обеспечение безопасности персональных данных передает имеющиеся материалы (в объеме, достаточном для принятия решения) ответственному за организацию обработки персональных данных для решения вопроса о целесообразности привлечения нарушителя безопасности информации к дисциплинарной ответственности.

6.2. На основании полученных результатов разбирательства ответственный за организацию обработки персональных данных организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков безопасности информации в будущем:

повторное ознакомление нарушителя безопасности с локальными нормативными актами ГИО ОКН НСО по безопасности информации;

анализ и пересмотр имеющихся прав доступа к информационным ресурсам ИСПДн у нарушителя безопасности информации;

обсуждение инцидента безопасности на совещании руководителей или собрании коллектива;

отмена неактуальных прав доступа к информационным ресурсам ИСПДн;

проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

другие обоснованные мероприятия.

6.3. О результатах проведенного разбирательства инцидента безопасности информации ответственный за обеспечение безопасности персональных данных по необходимости инициирует подготовку сообщения об инциденте безопасности информации в адрес руководства ГИО ОКН НСО.

7. Права, обязанности и ответственность участников разбирательства

7.1. Ответственный за обеспечение безопасности персональных данных имеет право:

7.1.1. По согласованию с ответственным за организацию обработки персональных данных требовать предоставлений письменных объяснений по

обстоятельствам инцидента безопасности информации у нарушителя безопасности информации.

Запрашивать и получать от руководителей и сотрудников ГИО ОКН НСО, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства инцидента безопасности информации.

Инициировать на основании заявок отключение от информационных ресурсов ИСПДн сотрудников ГИО ОКН НСО, нарушивших правила или требования безопасности информации, на период проведений расследования инцидента безопасности информации в случае если имеется существенный риск того, что продолжение работы сотрудника с ИСПДн может повлечь значительное увеличение ущерба или новые инциденты безопасности информации.

По результатам расследования инцидента безопасности информации инициировать изменения в бизнес-процессах и информационных ресурсах ГИО ОКН НСО с целью повышения их защищенности и снижения рисков инцидентов безопасности информации.

Инициировать процедуры привлечения нарушителя безопасности информации к дисциплинарной/материальной ответственность согласно внутренним нормативным документам ГИО ОКН НСО.

7.2. Ответственный за обеспечение безопасности персональных данных обязан:

Объективно и основательно проводить разбирательство каждого инцидента безопасности информации.

Определять первоочередные меры, направленные на локализацию инцидента безопасности информации и минимизацию негативных последствий.

Фиксировать в карточке данных «Инциденты безопасности информации» всю исходную информацию об инциденте безопасности информации и результаты его расследования.

Предоставлять отчеты и рекомендации по проведенным разбирательствам ответственному за организацию обработки персональных данных.

Проводить анализ обстоятельств, способствовавших совершению каждого инцидента безопасности информации, и на его основе, совместно с администратором безопасности информации, разрабатывать рекомендации и предложения по оптимизации бизнес-процессов и снижения ущерба от подобных инцидентов безопасности информации и минимизации возможности их повторения в будущем.

Составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

7.3. Руководители структурных подразделений и сотрудники ГИО ОКН НСО обязаны:

предоставлять по запросам ответственного за обеспечение безопасности персональных данных устные и письменные разъяснения и иную информацию в

рамках своей компетенции, необходимую для проведения разбирательства инцидента безопасности информации;

информировать ответственного за обеспечение безопасности персональных данных о выявленных инцидентах безопасности информации;

информировать ответственного за обеспечение безопасности персональных данных об имеющихся запросах и обращениях субъектов персональных данных.

Приложение
к Инструкции по выявлению инцидентов безопасности и реагированию на них в информационных системах персональных данных

Карточка данных о инциденте безопасности информации.

Дата события _____

Номер события[1]:

Информация о сообщающем лице

Фамилия Имя Отчество _____

Отдел _____

Телефон _____

Электронная почта _____

Описание события ИБ

Описание события:

- Что произошло _____
- Как произошло _____
- Почему произошло _____
- Пораженные компоненты _____
- Негативное воздействие _____
- Любые идентифицированные уязвимости _____

Детали события безопасности информации

Дата и время возникновения события _____

Дата и время обнаружения события _____

Дата и время сообщения о событии _____

Закончилось ли событие? *(отметить квадрат)* Да ☐ Нет ☐

Если «да», то уточнить, как долго длилось событие в днях/часах/минутах

Дополнительная информация

_____

_____

_____

_____

[1] (Номера событий назначаются руководителем)

Приложение № 3

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.04. 2023 г. № 115

Инструкция
об организации учета, хранения и выдачи машинных носителей информации
в информационных системах персональных данных

1. Настоящая Инструкция устанавливает организацию учета, хранения и выдачи машинных носителей машинных носителей информации в информационных системах персональных данных (далее – ИСПДн) государственной инспекции по охране объектов культурного наследия (далее – ГИО ОКН НСО).

2. Учет, хранение и выдачу машинных носителей информации (далее – МНИ) осуществляет ответственный за обеспечение безопасности персональных данных. При увольнении сотрудника, ответственного за учет, хранение и выдачу МНИ, составляется акт приема-сдачи этих документов, который утверждается начальником инспекции.

3. Организация учета МНИ

Все находящиеся на хранении и в обращении МНИ подлежат учёту. Учет всех видов и типов МНИ производится в журнале учета машинных носителей информации в информационных системах персональных данных.

Каждый носитель должен иметь этикетку, на которой указывается его уникальный учетный номер.

4. Организация выдачи МНИ

Пользователи ИСПДн получают учтенный МНИ у ответственного за обеспечение безопасности персональных данных для выполнения работ. При получении делаются соответствующие записи в журнале учета машинных носителей информации в информационных системах персональных данных. По окончании работ пользователь сдает МНИ для хранения ответственному за обеспечение безопасности персональных данных, о чем делается соответствующая запись в журнале учета машинных носителей информации в информационных системах персональных данных.

5. Организация хранения МНИ

Хранение МНИ осуществляется в условиях, исключающих несанкционированное копирование, изменение или уничтожение содержащихся на нем персональных данных, а также хищение МНИ.

Носители должны храниться в служебных помещениях, в металлическом хранилище (сейфе) в установленном порядке. Запрещается оставлять МНИ без присмотра или передавать на хранение другим лицам.

6. В случае утраты МНИ, содержащих персональные данные, либо разглашения содержащихся в них сведений, немедленно ставится в известность ответственный за обеспечение безопасности персональных данных. Соответствующие отметки вносятся в журнале учета машинных носителей информации в информационных системах персональных данных.

7. МНИ, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. По результатам уничтожения МНИ составляется Акт уничтожения МНИ.

8. При передаче средств вычислительной техники ИСПДн сторонним организациям для проведения ремонтно-восстановительных или иных работ, несъемные МНИ изымаются из состава средств вычислительной техники.

9. Ответственность за выполнение правил эксплуатации МНИ при выполнении непосредственных работ с носителями несет пользователь ИСПДн.

10. Контроль выполнения пользователями установленных правил эксплуатации МНИ, осуществляют ответственный за обеспечение безопасности персональных данных и администратор безопасности информации в рамках своих должностных обязанностей.

Приложение № 4

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07 2023 г. № 115

Инструкция
по организации парольной защиты в информационных системах
персональных данных

1. Общие положения

1.1. Настоящая Инструкция по организации парольной защиты в информационных системах персональных данных (далее – Инструкция) определяет порядок использования, генерации, смены и прекращения действия паролей пользователей в информационных системах персональных данных (далее – ИСПДн), а также контроль действий пользователей при работе с паролями. Инструкция распространяется на все ИСПДн, существующие и вновь создаваемые в ИСПДн. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности их работы.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль за реализацией требований по обеспечению безопасности при использовании паролей возлагается на администратора безопасности информации.

2. Требования к организации парольной защиты

2.1. Установку первичного пароля производит администратор безопасности информации при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на администраторе безопасности информации.

2.2. При создании первичного пароля, администратор безопасности информации обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

2.3. Первичный пароль так же используется при сбросе забытого пароля на учетную запись.

2.4. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

2.5. Устанавливаемые пароли должен отвечать следующим требованиям:

длина пароля должна быть не менее 8 символов;

пароль должен содержать строчные и прописные буквы, а также небуквенные символы (цифры, знаки пунктуации, специальные символы);

пароль, должен отличаться от предыдущего не менее чем на 4 символа;

использование трех и более, подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;

использование в качестве пароля одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов недопустимо;

новое значение пароля не должно совпадать с одним из пяти предыдущих значений;

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования автоматизированного рабочего места, имя учетной записи или какую-либо его часть, общепринятые сокращения (password, USER, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе.

2.6. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом администратору безопасности информации и изменить основной пароль.

2.7. Восстановление забытого основного пароля пользователя осуществляется администратором безопасности информации путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной либо электронной заявки пользователя.

2.8. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

2.9. Для предотвращения несанкционированного доступа в ИСПДн должен быть реализован механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

2.10. Разблокирование учетной записи пользователя осуществляется администратором безопасности информации на основании заявки владельца учетной записи.

2.11. Должен быть установлен пароль на доступ к настройкам используемых средств защиты информации. Указанный пароль должен отвечать установленным требованиям (п. 2.5.).

2.12. Пользователи и администратор безопасности информации обязаны:

сохранять в тайне свой личный пароль;

четко знать и строго выполнять требования настоящей Инструкции;

своевременно сообщать лицам, ответственным за обеспечение безопасности ПДн обо всех нештатных ситуациях, нарушениях работы подсистем защиты от несанкционированного доступа, возникающих при работе с паролями.

2.13. При организации парольной защиты запрещается:

записывать свои пароли на любой носитель;

хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги;

сообщать посторонним лицам, в том числе сотрудникам ГИО ОКН НСО безопасности информации, свои пароли, а также пересылать открытым текстом в электронных сообщениях.

3. Порядок применения парольной защиты

3.1. Полная плановая смена паролей производится регулярно, не реже одного раза в 90 дней. При плановой смене пароля, пользователь самостоятельно меняет свой пароль.

3.2. Внеплановая смена (удаление) личного пароля любого пользователя производится в следующих случаях:

по окончании срока действия пароля;

в случае прекращения полномочий пользователя;

при обнаружении факта успешной попытки несанкционированного доступа к элементам ИСПДн;

при обнаружении факта компрометации пароля.

3.3. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности информации.

3.4. Скомпрометированные пароли выводятся из действия немедленно.

3.5. Порядок внеплановой смены пароля аналогичен порядку плановой смены пароля.

3.6. По каждому случаю, связанному с компрометацией действующих паролей, ответственным за обеспечение безопасности персональных данных, организуется и проводится служебное расследование.

3.7. Результаты служебного расследования в виде служебной записки предоставляются руководителю структурного подразделения или ответственному за организацию обработки персональных данных. По результатам расследования лица, допустившие разглашение паролей, привлекаются к дисциплинарной ответственности.

Приложение № 5

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Инструкция
о порядке работы при подключении к информационно-телекоммуникационным сетям международного информационного обмена

1. Общие положения

1.1. Настоящая Инструкция о порядке работы при подключении к информационно-телекоммуникационным сетям международного информационного обмена (далее – Инструкция) устанавливает условия и единый порядок работы сотрудников государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО) при подключении к информационно-телекоммуникационным сетям международного информационного обмена, в том числе сети «Интернет» (далее – Сеть «Интернет»), а также основные требования по обеспечению безопасности информации.

1.2. Подключение к Сети «Интернет» в подразделениях ГИО ОКН НСО используется в целях получения различной технической, аналитической и другой служебной информации в режиме реального времени.

1.3. Основными угрозами безопасности информации при использовании сети «Интернет» в ГИО ОКН НСО являются:

заражение информационно-вычислительных ресурсов ГИО ОКН НСО вирусами;

несанкционированный доступ внешних пользователей к информационно-вычислительным ресурсам ГИО ОКН НСО (в т.ч. сетевые атаки);

внедрение в информационные системы ГИО ОКН НСО программных закладок;

загрузка трафика нежелательной корреспонденцией (спамом);

несанкционированная передача персональных данных сотрудниками ГИО ОКН НСО в Сеть «Интернет»;

1.4. Основными методами обеспечения безопасности информации при использовании Сети «Интернет» для предотвращения указанных угроз являются:

межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов, прошедших в установленном порядке процедуру оценки соответствия;

использование средств антивирусной защиты, средств (систем) обнаружения вторжений, прошедших в установленном порядке процедуру оценки соответствия;

контроль информации, загружаемой или передаваемой в сеть «Интернет»;

запрет обращения к нежелательным ресурсам сети «Интернет»;

шифрование конфиденциальной информации с использованием средств криптографической защиты информации, прошедших в установленном порядке процедуру оценки соответствия, при необходимости её передачи по сети «Интернет», а также использование электронно-цифровой подписи для контроля целостности и подтверждения подлинности отправителя и/или получателя информации;

2. Доступ к Интернет-ресурсам

2.1. Подключение к сети Интернет, дальнейшая техническая поддержка и сопровождение программных и аппаратных средств, предназначенных для взаимодействия с Сетью «Интернет», осуществляется системным администратором после согласования с администратором безопасности информации.

2.2. Основанием для предоставления доступа к Сети «Интернет» является решение руководства ГИО ОКН НСО при наличии необходимости предоставления доступа.

2.3. Подключение автоматизированных рабочих мест и серверов информационных систем к Сети «Интернет» допускается только с использованием средств межсетевого экранирования, прошедших в установленном порядке процедуру оценки соответствия.

2.4. Каждое автоматизированное рабочее место, на котором установлен доступ к Сети «Интернет» должно быть оснащено средством антивирусной защиты, прошедшего в установленном порядке процедуру оценки соответствия, которое должно функционировать в режиме «постоянная защита».

2.5. Доступ к ресурсам Сети «Интернет» предоставляется сотрудникам ГИО ОКН НСО только для выполнения ими прямых должностных обязанностей. Использование Сети «Интернет» в других целях запрещается.

2.6. Самостоятельная организация дополнительных точек доступа к Сети «Интернет» (удаленный доступ, канал по локальной сети, использование беспроводных модемов и пр.) запрещена.

3. Основные ограничения при работе в сети Интернет

3.1. Пользователям Сети «Интернет» запрещается:

вносить какие-либо изменения в программное обеспечение, установленное на автоматизированном рабочем месте;

совершать любые попытки деструктивных действий по отношению к нормальной работе локальной вычислительной сети ГИО ОКН НСО и Сети «Интернет» (рассылка вирусов, сетевые-атаки и т.п.);

осуществлять передачу информации конфиденциального характера по Сети «Интернет» в открытом виде;

передавать информацию конфиденциального характера третьей стороне;

применять имена пользователей и пароли используемые в информационных системах за пределами ГИО ОКН НСО;

использовать служебную электронную почту ГИО ОКН НСО в личных целях;

использовать для служебной переписки электронную почту отличную от электронной почты ГИО ОКН НСО;

посещать игровые, развлекательные и прочие сайты, не имеющие отношения к деятельности сотрудника ГИО ОКН НСО;

совершать действия, противоречащие законодательству, а также настоящей Инструкции.

4. Ответственность

4.1. Ответственность за доступ пользователей к ресурсам Сети «Интернет» в ГИО ОКН НСО несет руководитель.

4.2. Каждый пользователь Сети «Интернет» несет персональную ответственность за свои действия и за вводимую и выводимую информацию. В случае нарушения пользователем положений настоящей Инструкции системный администратор или администратор безопасности информации по распоряжению руководства ГИО ОКН НСО вправе отключить соответствующее автоматизированное рабочее место (пользователя) от Сети «Интернет» и уведомить об этом руководство подразделения.

4.3. Если нарушения повлекли тяжкие последствия, должно проводиться служебное расследование.

5. Контроль использования ресурсов сети «Интернет»

5.1. В целях обеспечения информационной безопасности в информационных системах системный администратор и администратор безопасности информации обеспечивают:

контроль посещения ресурсов Сети «Интернет» сотрудниками ГИО ОКН НСО, а также получаемых и передаваемых сотрудниками данных, в том числе и по электронной почте;

контроль за соблюдением настоящей Инструкции;

безопасное использование ресурсов сети «Интернет».

Приложение № 6

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Инструкция
о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации, в информационных системах персональных данных

1. Общие положения

1.1. Настоящая Инструкция о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации, в информационных системах персональных данных (далее – Инструкция) определяет правила работ по техническому обслуживанию, ремонту, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации, в информационных системах персональных данных (далее – ИСПДн) государственной инспекции по охране объектов культурного наследия (далее – ГИО ОКН НСО), защищенных от несанкционированного доступа и предназначенных для обработки и хранения персональных данных.

1.2. Данные работы проводятся только с разрешения руководства ГИО ОКН НСО или лица, исполняющего его обязанности, после согласования с ответственным за обеспечение безопасности персональных данных.

2. Порядок проведения работ по техническому обслуживанию, ремонту, модернизации технических средств

2.1. В случае, когда необходимо провести работы по техническому обслуживанию (ремонту, модернизации) технических средств, входящих в состав ИСПДн, ответственный за обеспечение безопасности персональных данных представляет служебную записку, в которой:

указывает название и номер автоматизированного рабочего места (далее – АРМ) (технического средства, системы), техническое обслуживание (ремонт, модернизацию) которой необходимо провести и с какой целью;

обосновывает необходимость технического обслуживания (модернизации);

указывает планируемые место и сроки работ, режим их проведения;

перечисляет меры безопасности, которые будут реализованы при техническом обслуживании (ремонте, модернизации) с целью недопущения доступа к персональным данным посторонних лиц.

2.2. В случае если для проведения работ необходимо привлекать лиц, не имеющих постоянного допуска к работе на АРМ или в помещение, составляется список лиц, который согласовывается с руководством ГИО ОКН НСО.

2.3. Запрещается выносить технические средства, входящие в состав ИСПДн, из помещений, занимаемых ГИО ОКН НСО, без согласования с ответственным за обеспечение безопасности персональных данных и разрешения руководства ГИО ОКН НСО.

2.4. Вскрытие печатей на корпусах АРМ или других технических средств и последующее опечатывание производится комиссионно в присутствии ответственного за обеспечение безопасности персональных данных, о чём составляется акт.

В акте указывается:

номер (название) помещения, в котором проводились работы;

дата и время начала и окончания работ;

лица, присутствовавшие при вскрытии и обслуживании (ремонте, модернизации);

наличие, целостность и места размещения печатей (пломб, специальных защитных знаков) до вскрытия АРМ (технического средства, системы);

установленные неисправности;

виды и результаты проведенных работ;

замененные или отремонтированные узлы (детали), наличие на этих узлах специальных защитных знаков;

какими печатями (пломбами и т.д.) и в каких местах АРМ (устройство) опечатано по окончании работ;

иная необходимая для дальнейшей работы и обеспечения безопасности информация.

2.5. Если для ремонта (модернизации) ИСПДн (другого технического средства, системы, элемента АРМ в составе ИСПДн) необходимо направить в специализированную организацию, то комиссией составляется заключение.

2.6. Перед отправкой АРМ (другого технического средства, системы, элемента АРМ) ответственный за обеспечение безопасности персональных данных обязан гарантированно удалить персональные данные с жесткого диска и иных устройств памяти АРМ (другого технического средства, системы) сертифицированными средствами, о чем составляется акт. По запросу из специализированной организации копия акта передаётся и ей.

2.7. В случае если не имеется возможности гарантированно удалить персональные данные с жесткого диска и иных устройств памяти АРМ (другого технического средства, системы) сертифицированными средствами

или произвести обезличивание персональных данных, эти устройства опечатываются и хранятся у ответственного за обеспечение безопасности персональных данных с соблюдением требований, предъявляемым к хранению персональных данных.

2.8. Ремонт и замена жесткого диска производится с соблюдением требований п.п. 2.5-2.7 настоящей Инструкции в присутствии ответственного за обеспечение безопасности персональных данных. При диагностике и ремонте жесткого диска должны быть реализованы меры безопасности, исключающие несанкционированный доступ к хранящимся на нём данным.

3. Порядок обновления общесистемного и прикладного программного обеспечения.

3.1. Установку, обновление и модификацию общесистемного и прикладного программного обеспечения АРМ ИСПДн проводит администратор безопасности информации.

3.2. Изменение конфигурации программных средств ИСПДн кем-либо, кроме администратора безопасности информации запрещено.

3.3. Установка или обновление программного обеспечения ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций данного программного обеспечения.

3.4. Установка и обновление программного обеспечения (системного, прикладного, тестового и т.п.) на АРМ ИСПДн производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), если иной порядок установки и обновления не предусмотрен разработчиком программного обеспечения.

3.5. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.

3.6. Программное обеспечение, устанавливаемое на АРМ ИСПДн, а также его обновления, перед установкой должны пройти антивирусный контроль.

4. Порядок обновления программного обеспечения средств защиты информации

4.1. Внесение изменений в конфигурацию аппаратно-программных и программных средств защиты информации проводит администратор безопасности информации.

4.2. Обновление баз данных, необходимых для реализации функций безопасности средства защиты информации (обновление баз сигнатур вирусов средств антивирусной защиты, баз сигнатур уязвимостей средств контроля (анализа) защищенности, баз решающих правил систем обнаружения вторжений и других) выполняется в автоматическом режиме по расписанию со специальных серверов обновления производителей средств защиты информации.

4.3. Обновление программного обеспечения средств защиты информации, направленное на устранение уязвимостей средства защиты информации осуществляется после получения информации от производителя средства защиты информации о необходимости обновления в порядке, установленном производителем средства защиты информации.

4.4. Обновление, направленное на добавление функции (функций) безопасности средства защиты информации, на совершенствование реализации функции (функций) безопасности средства защиты информации, на расширение числа поддерживаемых программных и аппаратных платформ, а также обновление, не влияющее на безопасность средства защиты информации (изменение интерфейса средства защиты информации, иных функций, не влияющее на функции безопасности средства защиты информации) осуществляются по решению руководства ГИО ОКН НСО в порядке, определенном производителем средства защиты информации.

Приложение № 7

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Инструкция
по учёту лиц, допущенных к работе в информационных системах персональных данных

1. Настоящая Инструкция по учёту лиц, допущенных к работе в информационных системах персональных данных (далее – Инструкция) определяет порядок учёта лиц, допущенных к работе в информационных системах персональных данных (далее – ИСПДн) государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО).

2. С целью организации учёта лиц, допущенных к работе в ИСПДн, ведется «Журнал учёта лиц, допущенных к работе в…».

3. Основанием для допуска сотрудника ГИО ОКН НСО к работе в ИСПДн является список лиц, допущенных в ИСПДн, утвержденный руководством ГИО ОКН НСО.

4. Основанием для прекращения допуска сотрудника к работе в ИСПДн, может служить его исключение из «Списка лиц, допущенных к работе…» или его увольнение (переводе на другую должность, не требующую работы в ИСПДн).

5. Журнал учета лиц, допущенных к работе в информационных системах персональных данных ведется ответственным за обеспечение безопасности персональных данных.

6. На каждого сотрудника ГИО ОКН НСО, допущенного в ИСПДн, в журнале должна быть отведена отдельная страница.

7. Журнал учета лиц, допущенных к работе в информационных системах персональных данных ведется до его полного заполнения. Заполненные журналы хранятся не менее 3 лет.

Приложение № 8

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Инструкция
по эксплуатации средств защиты информации в информационной системе персональных данных государственной инспекции по охране объектов культурного наследия Новосибирской области

1. Общие положения

Настоящая Инструкция по эксплуатации средств защиты информации в информационной системе персональных данных государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО) (далее – Инструкция) разработана для пользователей и администратора безопасности информации и определяет правила эксплуатации средств защиты информации, установленных в информационной системе персональных данных «ГИО ОКН НСО» (далее – ИСПДн), а также устанавливает ответственность пользователей ИСПДн за их нарушение.

2. Правила эксплуатации средств защиты информации

2.1. Для обеспечения необходимого уровня защищенности при работе в ИСПДн применяются следующие средства защиты информации:

Средство защиты информации от несанкционированного доступа «Dallas Lock 8.0-K»;

Программный комплекс «ViPNet Client 3.2»;

Средство антивирусной защиты «Kaspersky Endpoint Security 10 для Windows».

2.2. Эксплуатация средств защиты информации осуществляется в соответствии с эксплуатационной документацией, предоставляемой производителями средств защиты информации.

2.3. Пользователи ИСПДн должны быть ознакомлены со следующими документами:

Система защиты информации от несанкционированного доступа Dallas Lock 8.0. Руководство оператора. RU.48957919.501410-01 34;

ViPNet Контроль приложений 3.2. Руководство пользователя. ФРКЕ. 00004-05 34 04;

ViPNet Деловая почта 3.2. Руководство пользователя. ФРКЕ. 00004-05 34 03;

Основные термины и определения. Приложение к документации ViPNet CUSTOM. ФРКЕ. 00068-02 90 02;

Kaspersky Endpoint Security 10 для Windows Руководство администратор.

2.4. Администратор безопасности информации при эксплуатации средств защиты информации должен руководствоваться следующими документами:

Система защиты информации от несанкционированного доступа Dallas Lock 8.0. Руководство по эксплуатации. RU.48957919.501410-02 92;

Система защиты информации от несанкционированного доступа Dallas Lock 8.0. Руководство оператора. RU.48957919.501410-01 34;

Система защиты информации от несанкционированного доступа Dallas Lock 8.0. Описание применения. RU.48957919.501410-01 31;

ViPNet Контроль приложений 3.2. Руководство пользователя. ФРКЕ. 00004-05 34 04;

ViPNet Деловая почта 3.2. Руководство пользователя. ФРКЕ. 00004-05 34 03;

Основные термины и определения. Приложение к документации ViPNet CUSTOM. ФРКЕ. 00068-02 90 02;

Kaspersky Endpoint Security 10 для Windows Руководство администратор.

2.5. Пользователи ИСПДн должны быть ознакомлены с организационно-распорядительными документами ГИО ОКН НСО по защите информации в ИСПДн.

2.6. Перед началом эксплуатации средств защиты информации администратором безопасности информации должен быть проведен контроль знаний и навыков пользователей ИСПДн в части обеспечения безопасности информации с использованием применяемых в ИСПДн средств защиты информации.

2.7. Внесение изменений в конфигурацию используемых средств защиты информации осуществляет администратор безопасности информации после согласия с ответственным за обеспечение безопасности персональных данных.

2.8. Эксплуатируемые средства защиты учитываются ответственным за обеспечение безопасности персональных данных в журнале учёта средств защиты информации, эксплуатационной и технической документации к ним.

2.9. Администратор безопасности информации должен периодически проводить плановые и внеплановые проверки выполнения пользователями ИСПДн требований по защите информации в ИСПДн.

2.10. Администратором безопасности информации осуществляется контроль работоспособности, параметров настройки и правильности функционирования средств защиты информации один раз в полгода, а также в случае изменения списка допущенных лиц, смены администратора безопасности информации, изменения конфигурации ИСПДн.

3. Ответственность

Пользователи и администратор безопасности информации ИСПДн несут персональную ответственность за нарушение правил эксплуатации средств защиты информации.

Приложение № 9

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07 2023 г. № 115

Инструкция
по работе пользователей в информационных системах персональных данных

1. Общие положения

1.1. Пользователями информационных систем персональных данных (далее – ИСПДн), являются сотрудники государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО), допущенные к работе в ИСПДн.

1.2. Настоящая инструкция определяет задачи, функции, обязанности, права и ответственность пользователей, допущенных к работе в ИСПДн.

2. Обязанности пользователя

2.1. При эксплуатации ИСПДн пользователь обязан:

2.1.1. Руководствоваться требованиями следующих документов:

инструкция по организации парольной защиты в информационных системах персональных данных ГИО ОКН НСО;

инструкция по организации антивирусной защиты в информационных системах персональных данных ГИО ОКН НСО, в части их касающейся;

настоящей инструкцией.

2.1.2. Помнить личные пароли.

2.1.3. Соблюдать установленную технологию обработки информации.

2.1.4. Размещать устройства вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн, в помещениях, в которых они установлены, таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

2.1.5. При возвращении на рабочее место контролировать целостность меток, исключающих негласное вскрытие системного блока средства вычислительной техники (далее – СВТ) и в случае нарушения целостности, сообщать об этом администратору безопасности информации.

2.1.6. Препятствовать использованию СВТ лицами, не указанными в «Разрешительной системе доступа пользователей к информационным ресурсам и техническим средствам информационной системы…».

2.2. При временном оставлении рабочего места пользователь обязан:

блокировать ввод-вывод информации на своем рабочем месте ИСПДн в случаях кратковременного отсутствия (перерыв) или выключать СВТ ИСПДн;

блокировать вывод информации на монитор СВТ;

2.3. Пользователю запрещается:

подключать к СВТ нештатные устройства;

производить загрузку нештатной операционной системы с внешнего носителя;

самостоятельно вносить изменения в состав, конфигурацию и размещение ИСПДн;

самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения (далее – ПО), установленного в ИСПДн;

устанавливать запрещенное к использованию ПО;

самостоятельно вносить изменения в размещение, состав и настройку средств защиты информации ИСПДн, а также завершать работу средств защиты информации ИСПДн;

сообщать устно, письменно или иным способом (показ и т.п.) другим лицам пароли, передавать личные идентификаторы (наименование учетной записи), ключевые носители и другие реквизиты доступа к ресурсам ИСПДн.

3. Права

Пользователь ИСПДн имеет право:

обращаться к администратору безопасности информации с просьбой об оказании технической и методической помощи по обеспечению безопасности, обрабатываемой в ИСПДн информации, по использованию установленных программных и технических средств ИСПДн, а также по вопросам эксплуатации установленных СЗИ;

обращаться к ответственному за обеспечение безопасности персональных данных по вопросам эксплуатации ИСПДн (выполнение установленной технологии обработки информации, инструкций и других документов по обеспечению информационной безопасности объекта и защиты информации);

обращаться к ответственному за обеспечение безопасности персональных данных в ИС по вопросам выполнения режимных мер при обработке информации.

4. Ответственность

Пользователь несет персональную ответственность:

за соблюдение установленной технологии обработки информации;

за соблюдение режима конфиденциальности при обработке и хранении в ИСПДн информации;

за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИСПДн;

за соблюдение требований нормативных правовых актов, приказов, распоряжений и указаний, определяющих порядок организации работ по обеспечению безопасности при работе с персональными данными.

Приложение № 10

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Инструкция
о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных систем персональных данных

1. Общие положения

1.1. Настоящая Инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных систем персональных данных (далее – Инструкция) определяет порядок действий по резервированию и восстановлению работоспособности технических средств (далее – ТС) и программного обеспечения (далее – ПО), баз данных и средств защиты информации (далее – СЗИ), связанных с функционированием информационных систем персональных данных (далее – ИСПДн) государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью Инструкции является превентивная защита элементов ИСПДн от потери защищаемой информации.

1.3. Задачами данной Инструкции является:

определение мер защиты от потери информации;

определение действий восстановления в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех сотрудников ГИО ОКН НСО, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

системы жизнеобеспечения;

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

1.5. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности информации.

1.6. Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к

потере защищаемой информации, назначается администратор безопасности информации или ответственный по обеспечению безопасности персональных данных.

2. Порядок реагирования на инцидент

2.1. В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

в результате непреднамеренных действий пользователей;

в результате преднамеренных действий пользователей и третьих лиц;

в результате нарушения правил эксплуатации технических средств ИСПДн;

в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником.

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, администратор безопасности информации, предпринимает меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Технические меры:

3.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

системы жизнеобеспечения;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

3.1.2. Системы жизнеобеспечения ИСПДн включают:

пожарные сигнализации и системы пожаротушения;

системы вентиляции и кондиционирования;

системы резервного питания.

3.1.3. Все критичные помещения ГИО ОКН НСО (помещения, в которых размещаются элементы ИСПДн и средства защиты информации) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.1.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие

станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

резервные линии электропитания в пределах комплекса зданий.

3.1.5. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на носителе информации (жесткий диск, оптический диск, флэш накопитель и т.п.).

3.2. Организационные меры:

3.2.1. Резервное копирование данных должно осуществлять на периодической основе:

для обрабатываемых персональных данных – не реже раза в неделю;

для технологической информации – не реже раза в месяц;

эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в 6 месяцев, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2.2. Данные о проведение процедуры резервного копирования и восстановления, должны отражаться в специально созданном журнале учета (приложение).

3.2.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.2.4. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

3.2.5. Носители должны храниться не менее года, для возможности восстановления данных.

4. Порядок восстановления работоспособности информационных систем

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы, в общем случае, осуществляются в следующей последовательности:

проверка исправности и работоспособности средств обеспечения функционирования ИСПДн;

восстановление работоспособности (ремонт или замена) средств обеспечения функционирования ИСПДн, при необходимости;

проверка правильности функционирования общего программного обеспечения ИСПДн;

восстановление нормального функционирования общего программного обеспечения ИСПДн с использованием дистрибутивов и обновлений к ним или резервных копий настроек, при необходимости;

проверка правильности функционирования средств защиты информации;

восстановление нормального функционирования средств защиты информации с использованием дистрибутивов и обновлений к ним, при необходимости;

проверка правильности функционирования специального программного обеспечения ИСПДн;

восстановление нормального функционирования специального программного обеспечения ИСПДн с использованием дистрибутивов и обновлений к ним, при необходимости;

восстановление баз персональных данных с использованием резервной копии в течении одного рабочего дня.

Данные работы осуществляются в соответствии с эксплуатационной документацией на технические и программные средства до полного восстановления работоспособности.

Восстановление персональных данных, созданных после их последнего резервирования, осуществляется пользователями, осуществившими их внесение в базы персональных данных.

Работы по техническому обслуживанию технических и программных средств ИСПДн осуществляется в соответствии с правилами, установленными в «Инструкции о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации, в информационных системах персональных данных ГИО ОКН НСО».

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными, а также несанкционированного копирования на машинные носители информации. Ответственность за выполнение данного требования возлагается на администратора безопасности информации.

Приложение к Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных систем персональных данных ГИО ОКН НСО

Форма
журнала резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных систем персональных данных ГИО ОКН НСО

№	Дата	Вид операции	Устройство	Каталог накопителя	Наименование резервной копии	Место хранения резервной копии	ФИО, проводившего резервирование / восстановление	Подпись, проводившего резервирование / восстановление

Приложение № 11

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Инструкция
системного администратора информационных систем персональных данных

1. Общие положения

1.1. Системный администратор информационных систем персональных данных (далее – ИСПДн) государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО) относится к категории специалистов.

1.2. На должность системного администратора ИСПДн назначается лицо, имеющее профильное профессиональное образование, опыт технического обслуживания и ремонта персональных компьютеров и оргтехники, знающее основы локальных сетей (стек протоколов TCP/IP, сетевое оборудование, принципы построения локальных вычислительных сетей).

1.3. Системный администратор ИСПДн должен знать:

1.3.1. Технические характеристики, назначение, режимы работы, конструктивные особенности, правила технической эксплуатации оборудования локальных вычислительных сетей, оргтехники, серверов, персональных компьютеров и принцип работы ИСПДн.

1.3.2. Аппаратное и программное обеспечение локальных вычислительных сетей.

1.3.3. Принципы ремонта персональных компьютеров и оргтехники.

1.3.4. Основы информационной безопасности, способы защиты информации от несанкционированного доступа, повреждения или умышленного искажения.

1.3.5. Порядок оформления технической документации.

1.3.6. Правила внутреннего трудового распорядка.

1.3.7. Основы трудового законодательства.

1.3.8. Правила и нормы охраны труда, техники безопасности и противопожарной защиты.

1.4. Назначение на должность системного администратора и освобождение от должности производится приказом директора.

2. Должностные обязанности системного администратора ИСПДн

2.1. Системный администратор ИСПДн:

2.1.1. Устанавливает на рабочие станции ИСПДн операционные системы и необходимое для работы программное обеспечение (после согласования с администратором безопасности информации).

2.1.2. Осуществляет конфигурацию программного обеспечения на рабочих станциях ИСПДн (после согласования с администратором безопасности информации).

2.1.3. Поддерживает в работоспособном состоянии программное обеспечение рабочих станций ИСПДн.

2.1.4. Осуществляет техническую и программную поддержку пользователей, консультирует пользователей по вопросам работы локальной сети и программ, составляет инструкции по работе с программным обеспечением и доводит их до сведения пользователей.

2.1.5. Совместно с администратором безопасности информации выявляет ошибки пользователей и программного обеспечения и принимает меры по их исправлению.

2.1.6. Проводит мониторинг сети, разрабатывает предложения по развитию инфраструктуры сети (после согласования с администратором безопасности информации).

2.1.7. Готовит предложения по модернизации и приобретению сетевого оборудования.

2.1.8. Осуществляет контроль за монтажом оборудования локальной сети специалистами сторонних организаций.

2.1.9. Сообщает своему непосредственному руководителю и администратору безопасности информации о случаях нарушения правил пользования локальной вычислительной сетью и принятых мерах.

3. Права системного администратора ИСПДн

3.1. Системный администратор ИСПДн имеет право:

3.1.1. Устанавливать и изменять правила пользования локальной вычислительной сетью (после согласования с администратором безопасности информации).

3.1.2. Знакомиться с документами, определяющими его права и обязанности, критерии оценки качества исполнения свих обязанностей.

3.1.3. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

3.1.4. Требовать от руководства обеспечения организационно - технических условий, необходимых для исполнения своих обязанностей.

4. Ответственность системного администратора ИСПДн

4.1. Системный администратор ИСПДн несет ответственность за:

4.1.1. Нарушение функционирования локальной вычислительной сети и рабочих станций ИСПДн вследствие ненадлежащего исполнения своих обязанностей.

4.1.2. Несвоевременное уведомление руководства и администратора безопасности информации о случаях нарушения правил пользования локальной вычислительной сетью.

4.2. Системный администратор ИСПДн привлекается к ответственности:

4.2.1. За ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей инструкцией - в пределах, установленных действующим трудовым законодательством Российской Федерации.

4.2.2. За правонарушения, совершенные в процессе своей деятельности - в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.2.3. За причинение материального ущерба компании - в пределах, установленных действующим законодательством Российской Федерации.

Приложение № 12

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Типовое обязательство должностного лица государственной инспекцией по охране объектов культурного наследия Новосибирской области, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (трудового договора) прекратить обработку персональных данных, ставших ему известными в связи с исполнением должностных обязанностей

Я,

_____.

(фамилия, имя, отчество (последнее при наличии)),

замещающий(ая) должность_____

_____

(наименование должности)

ознакомлен(а) с требованиями по соблюдению конфиденциальности обрабатываемых мною персональных данных субъектов персональных данных и обязуюсь в случае расторжения государственной инспекцией по охране объектов культурного наследия Новосибирской области со мной служебного контракта (трудового договора) прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей.

Я также ознакомлен(а) с предусмотренной законодательством Российской Федерации ответственностью за нарушения неприкосновенности частной жизни и установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

_____

(дата, подпись, (Ф.И.О (последнее - при наличии))

Приложение № 13

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Перечень
информационных систем государственной инспекции по охране объектов культурного наследия Новосибирской области

№ п/п	Наименование информационной системы	Цели обработки ПДн	Категория ПДн	Сотрудники оператора	Количество субъектов ПДн
1.	Информационная система персональных данных государственной инспекции по охране объектов культурного наследия Новосибирской области	осуществление возложенных на государственную инспекцию по охране объектов культурного наследия Новосибирской области полномочий, а также ведения кадровой работы (ведение и хранение личных дел, учетных карточек и трудовых книжек государственных гражданских служащих, содействия государственному гражданскому служащему в прохождении государственной гражданской службы Российской Федерации, в обучении и должностном росте, обеспечения личной безопасности государственного гражданского служащего и членов его семьи, учета результатов исполнения им должностных обязанностей, в целях обеспечения сохранности имущества государственной инспекции по охране объектов культурного наследия Новосибирской области, документов кандидатов на замещение вакантных должностей государственной гражданской службы государственной инспекции по охране объектов культурного наследия Новосибирской области	Иная	Нет	Менее 100 000

Приложение № 14

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07 2023 г. № 115

Перечень
обязанностей лиц, осуществляющих обработку персональных данных, либо имеющих доступ к персональным данным

1. Лица, осуществляющие обработку персональных данных, либо имеющие доступ к персональным данным, в своей работе руководствуются Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативно-правовыми актами в сфере персональных данных.

2. Лица, осуществляющие обработку персональных данных, либо имеющие доступ к персональным данным, обязаны:

вести прием и обработку обращений и запросов субъектов персональных данных или их представителей;

хранить в тайне известные ему персональные данные;

информировать ответственного за организацию обработки персональных данных о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;

соблюдать правила обработки персональных данных;

обрабатывать только те персональные данные, к которым получен доступ в рамках исполнения служебных обязанностей.

3. При обработке персональных данных запрещается:

использовать сведения, содержащие персональные данные, в неслужебных целях, а также в служебных целях – при ведении переговоров по телефонной сети, в открытой переписке и выступлениях;

передавать персональные данные по незащищенным каналам связи (телетайп, факсимильная связь, электронная почта и т.п.) без использования сертифицированных средств криптографической защиты информации;

выполнять на дому работы, связанные с использованием персональных данных, выносить документы и другие носители информации, содержащие персональные данные, из помещений государственной инспекции по охране объектов культурного наследия Новосибирской области.

4. Лица, осуществляющие обработку персональных данных, либо имеющие доступ к персональным данным несут персональную ответственность за нарушение требований законодательства о защите персональных данных, в том числе за разглашение персональных данных.

Приложение № 15

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

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

1. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО) проводятся периодические проверки условий обработки персональных данных.

3. Проверки осуществляются лицом, ответственным за организацию обработки персональных данных в ГИО ОКН НСО.

4. Проверки соответствия обработки персональных данных установленным требованиям проводятся на основании утвержденного руководством ГИО ОКН НСО ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в ГИО ОКН НСО письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

5. При проведении проверки соответствия порядка обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

1) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

2) порядок и условия применения средств защиты информации;

3) эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

4) состояние учета машинных носителей;

5) соблюдение правил обработки персональных данных в ГИО ОКН НСО;

6) наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

7) мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) осуществление мероприятий по обеспечению целостности персональных данных.

9) соответствие информационной системы, обрабатывающей персональные данные, эксплуатационной, проектной и аттестационной документации.

6. Лицо, ответственное за организацию обработки персональных данных в ГИО ОКН НСО при проведении проверки соответствия обработки персональных данных имеет право:

1) запрашивать у работников ГИО ОКН НСО информацию, необходимую для реализации полномочий;

2) требовать от уполномоченных на обработку персональных данных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

3) принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

4) вносить руководству ГИО ОКН НСО предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

5) вносить руководству ГИО ОКН НСО предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

7. В отношении персональных данных, ставших известными лицу, ответственному за организацию обработки персональных данных при проведении проверки соответствия обработки персональных данных в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

8. Своевременность и правильность проведения проверки контролируется ответственным за организацию обработки персональных данных.

9. Проверка должна быть завершена не позднее чем через 30 календарных дней со дня принятия решения о её проведении.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководству ГИО ОКН НСО докладывает ответственный за организацию обработки персональных данных в форме письменного заключения (докладной записки).

Приложение № 16

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Порядок
доступа в помещения государственной инспекции по охране объектов культурного наследия Новосибирской области

1. Настоящий Порядок устанавливает единые требования к доступу в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных и обеспечения соблюдения требований законодательства о персональных данных и обязателен для применения и исполнения всеми сотрудниками государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО).

2. В помещениях, в которых ведется обработка персональных данных, должна быть исключена возможность бесконтрольного пребывания посторонних лиц и обеспечена сохранность находящихся в этих помещениях документов и средств автоматизации.

3. Входные двери оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время.

4. По завершении рабочего дня, помещения, в которых ведется обработка персональных данных, закрываются.

5. Вскрытие помещений, где ведется обработка персональных данных, производят сотрудники, в соответствии со списком лиц, имеющих право вскрытия помещений ГИО ОКН НСО.

6. При отсутствии сотрудников, имеющих право вскрытия помещений ГИО ОКН НСО в соответствии с утвержденным списком, помещения могут быть вскрыты комиссией, созданной по указанию руководства ГИО ОКН НСО.

7. Уборка в помещениях, где ведется обработка персональных данных, производится только в присутствии ответственных сотрудников, работающих в этих помещениях.

8. При обнаружении повреждений замков или других признаков, указывающих на возможное проникновение посторонних лиц в помещения, в которых ведется обработка персональных данных, эти помещения не вскрываются, а составляется акт и о случившемся немедленно ставятся в известность ответственный за организацию обработки персональных данных и правоохранительные органы. Одновременно принимаются меры по охране места происшествия и до прибытия работников правоохранительных органов в эти помещения никто не допускается.

Приложение № 17

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 116

Правила
рассмотрения запросов субъектов персональных данных или их представителей

1. Субъект персональных данных имеет право на получение информации в государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО), касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных ГИО ОКН НСО;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые в ГИО ОКН НСО способы обработки персональных данных;

4) наименование и место нахождения ГИО ОКН НСО, сведения о лицах (за исключением работников ГИО ОКН НСО), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с ГИО ОКН НСО или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

8) наименование должности, фамилию, имя, отчество и местонахождение лица, осуществляющего обработку персональных данных по поручению ГИО ОКН НСО, если обработка поручена или будет поручена такому лицу;

9) информацию о способах исполнения оператором обязанностей, установленных в Приложении № 26;

10) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

11) информацию о способах исполнения министерством обязанностей, установленных Федеральным законом «О персональных данных» и

предусмотренных локальными нормативными актами инспекции, принятыми во исполнение Федерального закона «О персональных данных»;

12) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

3. Сведения, указанные в пункте 1 настоящих Правил, должны быть предоставлены субъекту персональных данных ГИО ОКН НСО в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4. Сведения, указанные в пункте 1 настоящих Правил, предоставляются субъекту персональных данных или его представителю ГИО ОКН НСО в течение десяти рабочих дней с момента обращения либо получения ГИО ОКН НСО запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления ГИО ОКН НСО в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с ГИО ОКН НСО (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных ГИО ОКН НСО, подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. ГИО ОКН НСО предоставляет сведения, указанные в части 7 настоящей статьи, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.»;

5. В случае, если сведения, указанные в пункте 1 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в ГИО ОКН НСО или направить повторный запрос в целях получения сведений, указанных в пункте 1 настоящих Правил, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо

выгодоприобретателем или поручителем по которому является субъект персональных данных.

6. Субъект персональных данных вправе обратиться повторно в ГИО ОКН НСО или направить повторный запрос в целях получения сведений, указанных в пункте 1 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих Правил, должен содержать обоснование направления повторного запроса.

7. ГИО ОКН НСО вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на ГИО ОКН НСО.

8. Обязанности ГИО ОКН НСО при обращении субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя:

1) ГИО ОКН НСО обязано сообщить в порядке, предусмотренном пунктами 1 – 7 настоящих Правил, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления ГИО ОКН НСО в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации;

2) в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя ГИО ОКН НСО обязано дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае

направления ГИО ОКН НСО в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации;».

3) ГИО ОКН НСО обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных;

4) в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, ГИО ОКН НСО обязано внести в них необходимые изменения;

5) в срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, ГИО ОКН НСО обязано уничтожить такие персональные данные;

6) ГИО ОКН НСО обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

Приложение № 18

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Правила
работы с обезличенными персональными данными

1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» обрабатываемые персональные данные подлежат обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

2. Руководство государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО) принимает решение о необходимости обезличивания персональных данных.

3. Руководители структурных подразделений, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, включающие обоснование такой необходимости и способы обезличивания.

4. Специалисты, обслуживающие базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

5. В ГИО ОКН НСО применяются следующие способы обезличивания:

1) метод введения идентификаторов – замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным;

2) метод изменения состава или семантики – изменение состава или семантики персональных данных путем замены результатами статистической обработки, преобразования, обобщения или удаления части сведений;

3) метод декомпозиции – разделение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;

4) метод перемешивания – перестановка отдельных значений или групп значений атрибутов персональных данных в массиве персональных данных.

6. Выбор и применение конкретного метода осуществляется в соответствии с Методическими рекомендациями по применению приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

7. Обезличивание персональных данных осуществляют сотрудники, ответственные за проведение мероприятий по обезличиванию обрабатываемых персональных данных.

8. Обезличенные персональные данные не подлежат разглашению.

9. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

10. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

1) парольной политики;

2) антивирусной политики;

3) правил работы со съемными носителями (если они используются);

4) правил резервного копирования;

5) правил доступа в помещения, где расположены элементы информационных систем.

11. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

1) правил хранения бумажных носителей;

2) правил доступа к обезличенным персональным данным и в помещения, где они хранятся.

Приложение № 19

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07 2023 г. № 115

Перечень
должностей в государственной инспекции по охране объектов культурного наследия Новосибирской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1. Начальник государственной инспекции по охране объектов культурного наследия Новосибирской области.

2. Заместитель начальника инспекции – начальник отдела государственной охраны, использования и популяризации объектов культурного наследия государственной инспекции по охране объектов культурного наследия Новосибирской области.

3. Начальник отдела обеспечения бюджетного процесса и деятельности – главный бухгалтер государственной инспекции по охране объектов культурного наследия Новосибирской области.

4. Консультант-юрист отдела государственного надзора и контроля государственной инспекции по охране объектов культурного наследия Новосибирской области.

5. Главный специалист отдела государственной охраны, использования и популяризации объектов культурного наследия государственной инспекции по охране объектов культурного наследия Новосибирской области.

6. Главный специалист отдела обеспечения бюджетного процесса и деятельности государственной инспекции по охране объектов культурного наследия Новосибирской области.

7. Ведущий эксперт отдела обеспечения бюджетного процесса и деятельности государственной инспекции по охране объектов культурного наследия Новосибирской области.

Приложение № 20

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07 2023 г. № 115

Перечень должностей в государственной инспекции по охране объектов культурного наследия Новосибирской области, исполнение обязанностей по которым связано с ответственностью за проведение мероприятий по обезличиванию обрабатываемых персональных данных

1. Начальник отдела обеспечения бюджетного процесса и деятельности – главный бухгалтер государственной инспекции по охране объектов культурного наследия Новосибирской области.

2. Консультант-юрист отдела государственного надзора и контроля государственной инспекции по охране объектов культурного наследия Новосибирской области.

3. Главный специалист отдела государственной охраны, использования и популяризации объектов культурного наследия государственной инспекции по охране объектов культурного наследия Новосибирской области.

4. Главный специалист отдела обеспечения бюджетного процесса и деятельности государственной инспекции по охране объектов культурного наследия Новосибирской области.

5. Ведущий эксперт отдела обеспечения бюджетного процесса и деятельности государственной инспекции по охране объектов культурного наследия Новосибирской области.

Приложение № 21

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07 2023 г. № 115

Инструкция
ответственного за организацию обработки персональных данных

I. Общие положения

1. Настоящая Инструкция определяет основные права и обязанности ответственного за организацию обработки персональных данных в государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО).

2. Ответственный за организацию обработки персональных данных в своей работе руководствуется настоящей Инструкцией, нормативными правовыми актами и методическими документами Федеральной службы по техническому и экспортному контролю Российской Федерации, Федеральной службы безопасности Российской Федерации и приказами ГИО ОКН НСО, регламентирующими вопросы обработки и защиты персональных данных, и отвечает за организацию, обеспечение своевременного и квалифицированного выполнения сотрудниками ГИО ОКН НСО законодательства Российской Федерации о персональных данных, в том числе требований к обработке и защите персональных данных.

3. Ответственный за организацию обработки персональных данных назначается приказом начальника ГИО ОКН НСО.

II. Обязанности ответственного за организацию обработки персональных данных

4. Ответственный за организацию обработки персональных данных обязан:

1) знать и соблюдать требования действующих нормативных правовых актов, а также внутренних инструкций, правил и положений, регламентирующих вопросы в сфере обработки и обеспечения безопасности персональных данных;

2) обеспечивать проведение работ по определению и пересмотру (при необходимости) уровня защищенности персональных данных при их обработке в информационных системах ГИО ОКН НСО в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными

постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

3) обеспечивать доведение до сведения сотрудников ГИО ОКН НСО с периодичностью не реже одного раза в год положений законодательства Российской Федерации о персональных данных, приказов ГИО ОКН НСО по вопросам обработки персональных данных, требований к защите персональных данных (в случае изменения нормативных правовых актов, в том числе приказов ГИО ОКН НСО в области защиты персональных данных, обучение сотрудников должно быть проведено не позднее одного месяца со дня изменений);

4) обеспечивать информирование пользователей информационных систем ГИО ОКН НСО об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации;

5) осуществлять внутренний контроль за соблюдением ГИО ОКН НСО и его сотрудниками законодательства Российской Федерации о защите персональных данных, в том числе требований к защите персональных данных в соответствии с Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

6) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль над приемом и обработкой таких обращений и запросов в соответствии с Правилами рассмотрения запросов субъектов персональных данных или их представителей по поводу обработки их персональных данных в информационных системах ГИО ОКН НСО;

7) контролировать ведение документации, предусмотренной приказами ГИО ОКН НСО в части обеспечения обработки и безопасности персональных данных;

8) обеспечивать доступ к персональным данным и учет сотрудников ГИО ОКН НСО, допущенных к обработке персональных данных;

9) вести учет машинных носителей информации в Журнале учета машинных носителей информации в информационных системах персональных данных и осуществлять контроль перемещения используемых в ГИО ОКН НСО машинных носителей информации за пределы контролируемой зоны;

10) обеспечивать регистрацию и контроль действий по удалению защищаемой информации и уничтожению машинных и иных материальных носителей информации путем составления соответствующих актов, с занесением соответствующих записей в Журнал учета машинных носителей информации в ГИО ОКН НСО;

11) сообщать начальнику ГИО ОКН НСО или лицу, ответственному за организацию обработки персональных данных, обо всех зафиксированных попытках посторонних лиц получить несанкционированный доступ к персональным данным, о возникновении иных инцидентов в информационных системах ГИО ОКН НСО;

12) обеспечивать контроль за актуализацией уведомлений уполномоченного органа, осуществляющего функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных;

13) участвовать в рассмотрении проектов технических заданий, нормативных актов и указаний, договоров на выполнение работ, отчетной и иной документации, с целью определения достаточности предусмотренных в них требований и мероприятий по защите персональных данных в соответствии с требованиями действующего законодательства Российской Федерации и приказов ГИО ОКН НСО;

14) в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных;

15) осуществлять в пределах своей компетенции иные функции в соответствии с целями и задачами ГИО ОКН НСО.

III. Права ответственного за организацию обработки персональных данных

5. Ответственный за организацию обработки персональных данных вправе:

1) знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на него задач;

2) проходить обучение по защите информации в специализированных учебных центрах;

3) требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей;

4) получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей;

5) требовать от сотрудников ГИО ОКН НСО соблюдения требований действующего законодательства о защите персональных данных, приказов ГИО ОКН НСО по вопросам обработки персональных данных;

6) проводить проверки соблюдения режима обеспечения безопасности персональных данных в ГИО ОКН НСО;

7) инициировать проведение и принимать участие в служебных расследованиях по фактам нарушения сотрудниками ГИО ОКН НСО установленных требований обработки и защиты персональных данных;

8) требовать прекращения обработки персональных данных в случае нарушения правил обработки и требований по защите персональных данных в случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных;

9) обращаться за необходимыми разъяснениями по вопросам функционирования программных и технических средств информационных систем и обеспечения безопасности персональных данных к администратору информационной безопасности;

10) вносить предложения начальнику ГИО ОКН НСО об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по обработке и защите персональных данных.

IV. Ответственность

6. Ответственный за организацию обработки персональных данных несет материальную, дисциплинарную, административную и уголовную ответственность:

1) за неисполнение либо ненадлежащее исполнение должностных обязанностей;

2) за нарушения в работе информационных систем ГИО ОКН НСО, вызванные его неправомерными действиями или неправильным использованием предоставленных прав, предусмотренных настоящей Инструкцией;

3) за нарушение действующего законодательства Российской Федерации, приказов ГИО ОКН НСО по защите персональных данных;

4) за превышение должностных полномочий и злоупотребление ими;

5) в случае применения к ГИО ОКН НСО штрафных санкций по вине ответственного за организацию обработки персональных данных;

6) за совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в отношении персональных данных, к которым он допущен в рамках выполнения своих должностных (функциональных) обязанностей.

Приложение № 22

Утверждено
приказом государственной
инспекции по охране
объектов культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Политика
в отношении обработки персональных данных

I. Общие положения

1. Политика в отношении обработки персональных данных в государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО) определяет права и обязанности сторон, цели и основные принципы обработки персональных данных, а также меры, направленные на защиту персональных данных при их обработке в ГИО ОКН НСО.

2. Настоящая Политика разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»).

Термины, используемые в настоящей Политики, применяются в том же значении, что и в ФЗ «О персональных данных».

3. Обязанности субъекта персональных данных и ГИО ОКН НСО:

1) субъект персональных данных обязан:

а) предоставлять в ГИО ОКН НСО полные и достоверные данные о себе;

б) в случае изменения своих персональных данных сообщать данную информацию ГИО ОКН НСО;

2) ГИО ОКН НСО обязано:

а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено ФЗ «О персональных данных»;

б) обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных субъектов персональных данных с использованием баз данных, находящихся на территории Российской Федерации;

в) 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;

г) сообщать в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления ГИО ОКН НСО в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации;

д) осуществлять иные действия и проводить иные мероприятия по обработке и защите персональных данных субъектов персональных данных в соответствии с законодательством Российской Федерации.

4. Права субъекта персональных данных:

1) субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

а) подтверждение факта обработки персональных данных министерством;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые ГИО ОКН НСО способы обработки персональных данных;

г) сведения о лицах (за исключением сотрудников ГИО ОКН НСО), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с ГИО ОКН НСО или на основании ФЗ «О персональных данных»;

д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен ФЗ «О персональных данных»;

е) сроки обработки персональных данных, в том числе сроки их хранения;

ж) порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ «О персональных данных»;

з) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

г) наименование или фамилию, имя, отчество (при наличии) и адрес лица, осуществляющего обработку персональных данных по поручению ГИО ОКН НСО, если обработка поручена или будет поручена такому лицу;

д) информацию о способах исполнения ГИО ОКН НСО обязанностей, установленных ФЗ «О персональных данных» и предусмотренных локальными нормативными актами ГИО ОКН НСО, принятыми во исполнение ФЗ «О персональных данных»;

е) иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами.

Сведения, указанные в подпункте 1 пункта 4 настоящей Политики, предоставляются субъекту персональных данных или его представителю в

течение десяти рабочих дней с момента обращения, либо получения ГИО ОКН НСО запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления ГИО ОКН НСО в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с ГИО ОКН НСО (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных ГИО ОКН НСО, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. ГИО ОКН НСО предоставляет сведения, указанные в подпункте 1 пункта 4 настоящей Политики, субъекту персональных данных или его представителю в той форме, в которой направлено соответствующее обращение либо запрос, если иное не указано в обращении или запросе;

2) субъект персональных данных имеет право на определение представителей для защиты своих персональных данных;

3) субъект персональных данных вправе требовать от ГИО ОКН НСО уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

4) субъект персональных данных имеет право требовать об извещении всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта персональных данных, обо всех произведенных в них исключениях, исправлениях или дополнениях;

5) если субъект персональных данных считает, что ГИО ОКН НСО осуществляет обработку его персональных данных с нарушением требований ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие ГИО ОКН НСО в уполномоченном органе по защите прав субъектов персональных данных;

6) субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

II. Цели сбора персональных данных

5. Обработка персональных данных осуществляется на законной и справедливой основе.

6. Целью обработки персональных данных сотрудников ГИО ОКН НСО и граждан Российской Федерации, направивших или обратившихся в ГИО ОКН НСО с обращением, является осуществление возложенных законодательством Российской Федерации на ГИО ОКН НСО функций, полномочий и обязанностей, а именно:

1) обеспечение доступа к информации о деятельности государственных органов;

2) оформление и регулирование трудовых отношений, ведение кадрового учета;

3) ведение воинского учета, проведение мобилизационной подготовки и мобилизации;

4) ведение бухгалтерского учета и начисление заработной платы;

5) соблюдение налогового законодательства;

6) учет и автоматизация обработки обращений граждан;

7) автоматизация контрольно-ревизионной деятельности;

8) обеспечение деятельности ГИО ОКН НСО по предоставлению государственных услуг, исполнению государственных функций.

7. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей, указанных в пункте 6 настоящей Политики.

8. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

III. Правовые основания обработки персональных данных

9. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми ГИО ОКН НСО осуществляет обработку персональных данных при осуществлении и выполнении возложенных законодательством Российской Федерации на него функций, полномочий и обязанностей для достижения целей обработки персональных данных, предусмотренных пунктом 6 настоящей Политики:

1) Трудовой кодекс Российской Федерации;

2) Налоговый кодекс Российской Федерации;

3) Гражданский кодекс Российской Федерации;

4) Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;

5) Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;

6) Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

7) Федеральный закон от 27.07.2004 № 79-ФЗ «О государственной гражданской службе»;

8) Федеральный закон от 31.05.1996 № 61-ФЗ «Об обороне»;

9) Федеральный закон от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе»;

10) Федеральный закон от 26.02.1997 № 31-ФЗ «О мобилизационной подготовке и мобилизации в Российской Федерации»;

11) Указ Президента от 01.02.2005 N 112 "Об утверждении Положения о конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации";

12) постановление Правительства РФ от 27.11.2006 №719 «Об утверждении Положения о воинском учете»;

13) постановление Правительства РФ от 24.10.2011 № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)»;

14) распоряжение Правительства Российской Федерации от 26.05.2005 № 667-р «Об утверждении формы анкеты, подлежащей представлению в государственный орган гражданином Российской Федерации, изъявившим желание участвовать в конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации»;

15) Методические рекомендации Генерального штаба Вооруженных Сил РФ от 11.07.2017;

16) Закон Новосибирской области от 15.10.2007 № 138-ОЗ «О государственных информационных системах, государственных информационных ресурсах, территориальной информационной системе Новосибирской области»;

17) Положение о государственной инспекции по охране объектов культурного наследия Новосибирской области, утвержденное постановлением Правительства Новосибирской области от 29.12.2018 № 576-п;

18) договоры, заключаемые между ГИО ОКН НСО и субъектом персональных данных;

19) согласие на обработку персональных данных субъектов персональных данных.

IV. Состав обрабатываемых персональных данных, категории субъектов персональных данных

10. В ГИО ОКН НСО ведется обработка персональных данных субъектов персональных данных как являющихся сотрудниками ГИО ОКН НСО, так и не являющихся таковыми.

11. Исходя из категорий субъектов персональных данных и принципов необходимости и достаточности для достижения целей обрабатывается следующий состав сведений, предоставляемых субъектами персональных данных:

1) фамилия, имя, отчество, дата и место рождения, гражданство;

2) прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);

3) фотография;

4) владение иностранными языками и языками народов Российской Федерации;

5) образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);

6) послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);

7) выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность);

8) классный чин федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации и (или) муниципальной службы, дипломатический ранг, воинское и (или) специальное звание, классный чин правоохранительной службы (кем и когда присвоены);

9) государственные награды, иные награды и знаки отличия, поощрения (кем награжден (поощрен) и когда);

10) семейное положение, состав семьи, степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены), в том числе бывших, супруги братьев и сестер, братья и сестры супругов;

11) места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены), в том числе бывших, супруги братьев и сестер, братья и сестры супругов;

12) пребывание за границей (когда, где, с какой целью);

13) близкие родственники (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывшие, супруги братьев и сестер, братья и сестры супругов, постоянно проживающие за границей и (или) оформляющие

документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей);

14) адрес регистрации и фактического места жительства, адреса прежних мест жительства;

15) дата регистрации по месту жительства;

16) паспорт (серия, номер, кем и когда выдан);

17) паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан);

18) информация, содержащаяся в свидетельствах о государственной регистрации актов гражданского состояния;

19) номера контактных телефонов или сведения о других способах связи;

20) отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);

21) идентификационный номер налогоплательщика;

22) номер страхового свидетельства обязательного пенсионного страхования;

23) наличие (отсутствие) судимости;

24) допуск к государственной тайне, оформленный за период работы, службы, учебы (форма, номер и дата);

25) наличие (отсутствие) заболевания, препятствующего поступлению на государственную гражданскую службу Российской Федерации или ее прохождению, подтвержденного заключением медицинского учреждения;

26) сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера членов семьи;

27) сведения о размещении информации в информационно-телекоммуникационной сети «Интернет»;

28) реквизиты полиса обязательного медицинского страхования;

29) номер расчетного счета;

30) сведения о последнем месте государственной или муниципальной службы.

12. ГИО ОКН НСО в связи с оказанием государственной услуги и осуществлением государственной функции обрабатывает следующие персональные данные:

1) фамилия, имя, отчество;

2) число, месяц, год и место рождения;

3) паспортные данные (серия, номер паспорта, кем и когда выдан, код подразделения);

4) сведения о регистрации и/или фактическом месте жительства;

5) номера контактных телефонов;

6) адрес электронной почты.

13. Обработка биометрических персональных данных (фотографическое изображение субъектов персональных данных) сотрудников ГИО ОКН НСО, лиц, ранее находящиеся на государственной гражданской службе в ГИО ОКН НСО, соискателей на замещение вакантных должностей государственной гражданской службы, осуществляется в соответствии с трудовым законодательством Российской Федерации и законодательством о государственной гражданской службе.

V. Порядок и условия обработки персональных данных

14. Перечень действий, совершаемых ГИО ОКН НСО с персональными данными субъектов персональных данных.

В ходе обработки персональных данных ГИО ОКН НСО возможно совершение следующих действий (операций) с персональными данными субъектов персональных данных: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Распространение персональных данных субъектов персональных данных (в том числе биометрических персональных данных) допускается при наличии согласия субъектов персональных данных (или их представителей), а также в иных случаях, предусмотренных законодательством Российской Федерации.

15. Используемые ГИО ОКН НСО способы обработки персональных данных.

Обработка полученных персональных данных осуществляется ГИО ОКН НСО как с использованием средств автоматизации, так и на бумажных носителях (без использования средств автоматизации).

16. Порядок передачи персональных данных третьим лицам.

В случае необходимости взаимодействия с третьими лицами в рамках достижения целей обработки персональных данных ГИО ОКН НСО обязуется не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Трансграничная передача персональных данных ГИО ОКН НСО не осуществляется.

17. Обеспечение конфиденциальности персональных данных.

ГИО ОКН НСО и иные лица, получившие доступ к персональным данным на законном основании, с целью обеспечения конфиденциальности персональных данных в соответствии со статьей 7 ФЗ «О персональных данных» обязуются не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено ФЗ «О персональных данных».

ГИО ОКН НСО вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

18. Порядок ознакомления с политикой ГИО ОКН НСО в отношении обработки персональных данных и принятых мерах по обеспечению безопасности персональных данных.

В соответствии с требованиями части 2 статьи 18.1 ФЗ «О персональных данных» настоящая Политика открыто опубликована и доступна для ознакомления в информационно-телекоммуникационной сети Интернет на официальном сайте ГИО ОКН НСО.

19. Условием прекращения обработки персональных данных является:

1) достижение целей обработки персональных данных;

2) отзыв согласия субъекта персональных данных (или его представителей) на обработку его персональных данных;

3) выявление неправомерной обработки персональных данных;

4) истечение установленного срока хранения персональных данных;

5) ликвидация ГИО ОКН НСО;

6) прекращение осуществления деятельности ГИО ОКН НСО;

7) обращение субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных.

20. Организация хранения персональных данных.

Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством Российской Федерации и (или) договором, стороной которого является субъект персональных данных.

21. Для организации хранения персональных данных в случае автоматизированной обработки ГИО ОКН НСО в соответствии с частью 5 статьи 18 ФЗ «О персональных данных» использует сервера и другие технические устройства хранения данных, находящиеся на территории Российской Федерации. При обработке персональных данных без использования средств автоматизации хранение организовано в соответствии с требованиями Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

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

22. Актуализация, исправление, удаление персональных данных.

При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность и актуальность по отношению к целям обработки персональных данных.

В соответствии со статьей 21 ФЗ «О персональных данных» в случае подтверждения факта неточности персональных данных или неправомерности их обработки ГИО ОКН НСО принимает необходимые меры, либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных и временному прекращению обработки до момента устранения выявленных нарушений.

23. Уничтожение персональных данных.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, а также в случае отзыва согласия субъекта персональных данных на обработку его персональных данных или в случае выявления неправомерной обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, или иным соглашением между ГИО ОКН НСО и субъектом персональных данных. Подтверждение уничтожения персональных данных в случаях, предусмотренных настоящим пунктом, осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.

В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 ФЗ «О персональных данных». Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

24. Порядок рассмотрения запросов субъектов персональных данных.

ГИО ОКН НСО обязуется сообщать субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по его запросу.

Сведения, указанные в абзаце втором настоящего пункта, предоставляются субъекту персональных данных или его представителю ГИО ОКН НСО в течение десяти рабочих дней с момента обращения либо получения ГИО ОКН НСО запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления ГИО ОКН НСО в адрес субъекта

персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

VII. Заключительные положения

25. ГИО ОКН НСО оставляет за собой право в любой момент изменить положения настоящей Политики и обязуется опубликовать обновленную Политику и предоставить к ней доступ для ознакомления путем размещения в информационно-телекоммуникационной сети Интернет на официальном сайте ГИО ОКН НСО.

Приложение № 23

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Правила
обработки персональных данных, осуществляемой без использования средств автоматизации

1. Общие положения

1.1. Настоящие правила определяют порядок обработки персональных данных без использования средств вычислительной техники в государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО) и являются обязательными для исполнения его сотрудниками и должны доводиться под роспись.

1.2. Правила разработаны в соответствии с требованиями постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и распространяются на документы, исполненные на бумажных носителях, в том числе полученные путем извлечения из информационных систем персональных данных (вывода на печать).

1.3. К документам на бумажных носителях, содержащим персональные данные (далее – документы), относятся:

типовые формы документов (бланки);

журналы (реестры, книги);

иные документы.

1.4. Не допускается в одном документе фиксация персональных данных, цели обработки которых заведомо не совместимы.

2. Порядок обращения с документами, содержащими персональные данные

2.1. Прием и учет (регистрация) документов, осуществляются структурным подразделением, которым поручен прием и учет несекретной документации.

2.2. Все документы подлежат обязательному учету в соответствии с правилами ведения делопроизводства.

Их подготовка, движение и уничтожение должны осуществляться в соответствии с требованиями, предусмотренными для документов, содержащих служебную информацию ограниченного распространения.

При этом в отношении каждого документа в любой момент времени должно быть документально установлено его местонахождение, а именно – сотрудник у которого находится документ.

2.3. Документы передаются сотрудникам под роспись. Документы хранятся сотрудниками в порядке, предусмотренном для документов, содержащих служебную информацию ограниченного распространения.

Передача документов от одного работника к другому осуществляется с разрешения руководителя подразделения, в котором находится документ на момент возникновения необходимости его передачи или по согласованному решению руководителей подразделений, между сотрудниками которых осуществляется передача.

2.4. Размножение (тиражирование) документов осуществляется только с письменного разрешения главы города или его заместителя.

2.5. Исполненные документы группируются в дела в соответствии с номенклатурой дел несекретного делопроизводства. При этом на обложке дела, в которое помещены такие документы, проставляется пометка «Для служебного пользования».

2.6. О фактах утраты документов, ставится в известность глава города, который принимает решение о необходимости и порядке расследования обстоятельств его утраты.

3. Особенности работы с типовыми формами и журналами

3.1. При использовании типовых форм документов, должны соблюдаться следующие условия:

типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, реквизиты ГИО ОКН НСО, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных;

типовая форма должна предусматривать раздел, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных (если согласие не предусмотрено законодательством Российской Федерации, то типовая форма должна содержать ссылку на Федеральный закон Российской Федерации с указанием статей);

типовая форма должна разрабатываться с учетом необходимости ознакомления субъектов персональных данных таким образом, чтобы не были нарушены права и интересы иных субъектов персональных данных;

3.2. При ведении журналов (реестров, книг), содержащих персональные данные, должны соблюдаться следующие условия:

необходимость ведения журнала должна быть предусмотрена нормативными правовыми актами Российской Федерации, ведомственными нормативными актами или локальными нормативными актами ГИО ОКН НСО;

определение круга лиц, которые имеют доступ к журналу, отвечают за его ведение и сохранность;

определение сроков хранения заполненных журналов.

Копирование содержащейся, в таких журналах (реестрах, книгах) информации не допускается.

Приложение № 24

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07.2023 г. № 115

Типовая форма согласия субъекта персональных данных на обработку персональных данных в государственной инспекции по охране объектов культурного наследия Новосибирской области (для государственных гражданских служащих государственной инспекции по охране объектов культурного наследия Новосибирской области)

Я, _____,
(фамилия, имя, отчество (при наличии))
паспорт серии _____ N _____, выдан _____
_____
(дата, кем)
адрес регистрации и фактического места жительства: _____
_____
_____

свободно, своей волей и в своем интересе даю согласие уполномоченным лицам государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО), находящегося по адресу: 630099, г. Новосибирск, ул. Мичурина, 6, на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение) следующих персональных данных:
фамилия, имя, отчество (при наличии), дата и место рождения, гражданство;
прежние фамилия, имя, отчество (при наличии), дата, место и причина изменения (в случае изменения);
фотография;
владение иностранными языками и языками народов Российской Федерации;
образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);
послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность);
классный чин федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации и (или) муниципальной службы, дипломатический ранг, воинское и (или) специальное звание, классный чин правоохранительной службы (кем и когда присвоены);
государственные награды, иные награды и знаки отличия, поощрения (кем награжден (поощрен) и когда);
семейное положение, состав семьи, степень родства, фамилии, имена, отчества (при наличии), даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены), в том числе бывших;
места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены), в том числе бывших;
пребывание за границей (когда, где, с какой целью);
близкие родственники (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывшие, постоянно проживающие за границей и (или) оформляющие документы для выезда на постоянное

место жительства в другое государство (фамилия, имя, отчество (при наличии), с какого времени проживают за границей);
адрес регистрации и фактического места жительства, адреса прежних мест жительства;
дата регистрации по месту жительства;
паспорт (серия, номер, кем и когда выдан);
паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан);
информация, содержащаяся в свидетельствах о государственной регистрации актов гражданского состояния;
номера контактных телефонов;
отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
идентификационный номер налогоплательщика;
номер страхового свидетельства обязательного пенсионного страхования;
наличие (отсутствие) судимости;
допуск к государственной тайне, оформленный за период работы, службы, учебы (форма, номер и дата);
наличие (отсутствие) заболевания, препятствующего поступлению на государственную гражданскую службу Российской Федерации или ее прохождению, подтвержденного заключением медицинского учреждения;
сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера членов семьи;
сведения об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети «Интернет», на которых государственным гражданским служащим, гражданином Российской Федерации, претендующим на замещение должности государственной гражданской службы Российской Федерации, размещались общедоступная информация, а также данные, позволяющие его идентифицировать;
реквизиты полиса обязательного медицинского страхования;
номер расчетного счета;
сведения о последнем месте государственной или муниципальной службы.

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации и Новосибирской области в сфере отношений, связанных с поступлением на государственную гражданскую службу Новосибирской области, ее прохождением и прекращением для реализации полномочий, возложенных на ГИО ОКН НСО законодательством Российской Федерации и Новосибирской области.

Я ознакомлен(а), что:
1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока государственной гражданской службы в ГИО ОКН НСО;
2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;
3) в случае отзыва согласия на обработку персональных данных, ГИО ОКН НСО вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
4) после увольнения с государственной гражданской службы персональные данные хранятся в ГИО ОКН НСО в течение сроков хранения документов, предусмотренных законодательством Российской Федерации;
5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации и Новосибирской области на ГИО ОКН НСО функций, полномочий и обязанностей;
6) персональные данные уничтожаются: по достижению целей обработки персональных данных; при упразднении или реорганизации ГИО ОКН НСО; на основании моего письменного обращения с требованием о прекращении обработки персональных данных (ГИО ОКН НСО прекратит обработку таких персональных данных в течение 3 (трех) рабочих дней со дня получения письменного обращения, о чем я буду письменно уведомлен (а) в течение 10 (десяти) рабочих дней со дня прекращения обработки персональных данных).

Отзыв согласия может быть произведен в письменной форме не ранее 5 лет с даты прекращения служебного контракта. При этом ГИО ОКН НСО хранит персональные данные в течение срока хранения документов, установленного архивным делопроизводством, но не менее 5 лет с даты прекращения трудового договора, а в случаях, предусмотренных законодательством, передает уполномоченным на то органам.

Дата начала обработки персональных данных: _____
(число, месяц, год)

_____ _____
(подпись) (Ф.И.О.)

Приложение № 25

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07.2023 г. № 115

Типовая форма согласия субъекта персональных данных на обработку персональных данных (для лиц, замещающих должности, не относящиеся к должностям государственной гражданской службы в государственной инспекции по охране объектов культурного наследия Новосибирской области)

Настоящим я, _____
зарегистрированный(ая), _____
_____
(указывается адрес, номер основного документа, удостоверяющего его
_____
личность, сведения о дате выдачи указанного документа и выдавшем
_____
органе)

даю согласие государственной инспекции по охране объектов культурного наследия Новосибирской области (далее – ГИО ОКН НСО) (местонахождение: Российская Федерация, 630099, г. Новосибирск, ул. Мичурина, 6) на обработку моих персональных данных, включая получение, систематизацию, накопление, обобщение, обезличивание, хранение, обновление и изменение, использование, уничтожение, с использованием, как автоматизированной информационной системы, так и бумажных носителей, а также иных предоставленных мною сведений, для целей заключения и исполнения трудового договора, в течение действия трудового договора и в течение пяти лет с даты прекращения трудового договора (в соответствии с архивным делопроизводством, но не менее 5 лет со дня прекращения трудовых отношений).

Осуществляется обработка следующих категорий персональных данных:
фамилия, имя, отчество (при наличии);
число, месяц, год и место рождения;
адрес регистрации и фактического места жительства;
номер телефона;
адрес электронной почты;
семейное положение;
фотография;
прежние фамилия, имя, отчество (при наличии);
гражданство;
образование (направление подготовки или специальность по диплому, квалификация);
послевузовское профессиональное образование;
ученая степень, ученое звание;
профессия;
сведения о владении иностранными языками;
классный чин федеральной гражданской службы; дипломатический ранг; воинское или специальное звание; классный чин правоохранительной службы; классный чин гражданской службы субъекта Российской Федерации; квалификационный разряд государственной службы;
сведения о допуске к государственной тайне, оформленном за период работы, службы, учебы (форма, номер и дата);

сведения о выполняемой работе с начала трудовой деятельности (включая учебу в ВУЗах, военную службу, работу по совместительству, предпринимательскую деятельность; месяц и год поступления и ухода, должность);
сведения о наградах и знаках отличия;
сведения о близких родственниках, о муже (жене) (фамилия, имя, отчество (при наличии), число, месяц год и место рождения);
сведения о пребывании за границей;
отношение к воинской обязанности, воинское звание;
паспортные данные или данные документа его заменяющего;
паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан);
номер страхового свидетельства обязательного пенсионного страхования;
реквизиты полиса обязательного медицинского страхования;
номер расчетного счета;
идентификационный номер налогоплательщика;
дополнительные сведения (участие в выборных представительных органах).

Я ознакомлен(а), что:
1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока работы в министерстве;
2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;
3) в случае отзыва согласия на обработку персональных данных, ГИО ОКН НСО вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
4) после увольнения персональные данные хранятся в ГИО ОКН НСО в течение сроков хранения документов, предусмотренных законодательством Российской Федерации;
5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации и Новосибирской области на министерство функций, полномочий и обязанностей;
6) персональные данные уничтожаются: по достижению целей обработки персональных данных; при упразднении или реорганизации ГИО ОКН НСО; на основании моего письменного обращения с требованием о прекращении обработки персональных данных (ГИО ОКН НСО прекратит обработку таких персональных данных в течение 3 (трех) рабочих дней со дня получения письменного обращения, о чем я буду письменно уведомлен (а) в течение 10 (десяти) рабочих дней со дня прекращения обработки персональных данных).

Отзыв согласия может быть произведен в письменной форме не ранее 5 лет с даты прекращения трудового договора. При этом ГИО ОКН НСО хранит персональные данные в течение срока хранения документов, установленного архивным делопроизводством, но не менее 5 лет с даты прекращения трудового договора, а в случаях, предусмотренных законодательством, передает уполномоченным на то органам.

Дата начала обработки персональных данных: _____
(число, месяц, год)

_____ _____
(подпись) (Ф.И.О. (последнее - при наличии))

Приложение № 26

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07. 2023 г. № 115

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные и (или) дать согласие на их обработку

Мне, _____,
(фамилия, имя, отчество (последнее при наличии))
паспорт (иной документ, удостоверяющий личность) _____,
(серия, номер,
_____
кем и когда выдан)
проживающему(ей) по адресу: _____
(указать адрес места жительства)
в соответствии с частью 2 статьи 18 с Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» разъяснены юридические последствия отказа предоставить персональные данные и (или) дать согласие на их обработку в _____
_____
(указать наименование структурного подразделения ГИО ОКН НСО)
в целях _____
(указать цели обработки персональных данных)
«____» _____ 20___ г. _____
(подпись, расшифровка подписи)
Юридические последствия отказа предоставить персональные данные и (или) дать согласие на их обработку разъяснил(а):

_____ _____ _____
(должность) (подпись) (Ф.И.О. (последнее при наличии))

Приложение № 27

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.01. 2023 г. № 115

ЖУРНАЛ

учета лиц, допущенных к работе в информационных системах персональных данных государственной инспекции по охране объектов культурного наследия

Журнал начат «____» _____ 20___ г.

Журнал завершен «____» _____ 20___ г.

_____ / ФИО, должность /

_____ / ФИО, должность /

На _____ листах

(Должность, Фамилия Имя Отчество)

№ п/п	Наименование информационной системы	Сведения о допуске к работе в информационной системе		Сведения о прекращении допуска к работе в информационной системе	
		Основание для допуска к работе в информационной системе (реквизиты документа)	Дата и подпись допускаемого лица	Основание для прекращения допуска к работе в информационной системе (реквизиты документа)	Дата и подпись лица об ознакомлении с документом, прекращающим работу в информационной системе
1.	2.	3.	4.	5.	6.

Приложение № 28

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 2207 2023 г. № 115

ЖУРНАЛ

учёта средств защиты информации, эксплуатационной и технической документации к ним

Журнал начат «____» _____ 20___ г.

Журнал завершен «____» _____ 20___ г.

_____ / ФИО, должность /

_____ / ФИО, должность /

На _____ листах

№ п/п	Наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание
1	2	3	4	5	6	7

Приложение № 29

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07.2023 г. № 115

ЖУРНАЛ

учёта машинных носителей информации в информационных системах персональных данных

Журнал начат «____» _____ 20___ г.

Журнал завершен «____» _____ 20___ г.

_____ / ФИО, должность /

_____ / ФИО, должность /

На _____ листах

№ п/п	Регистрационный номер /дата	Тип/ёмкость машинного носителя персональных данных/серийный номер	Номер экземпляра/ количество экземпляров	Место установки (использования) /дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)
1	2	3	4	5	6	7	8	9	10

Приложение № 30

Утверждено
приказом государственной
инспекции по охране объектов
культурного наследия
Новосибирской области
от 20.07.2023 г. № 115

ЖУРНАЛ

учёта обращений субъектов персональных данных обратившихся в государственную инспекцию по охране объектов культурного наследия Новосибирской области

Журнал начат «____» _____ 20___ г.

Журнал завершен «____» _____ 20___ г.

_____ / ФИО, должность /

_____ / ФИО, должность /

На _____ листах

№ п/п	Дата обращения	ФИО, дата рождения обратившегося	Номер основного удостоверяющего личность документа	Тематика обращения	ФИО и должность ответственного за рассмотрение	Дата передачи / отказа в предоставлении информации	Примечание