ИНСПЕКЦИЯ ПО НАДЗОРУ ЗА ТЕХНИЧЕСКИМ СОСТОЯНИЕМ САМОХОДНЫХ МАШИН И ДРУГИХ ВИДОВ ТЕХНИКИ РЕСПУБЛИКИ КРЫМ

ПРИКАЗ

03 ФЕВ 2022 г. Симферополь № 13/ОД

«Об утверждении документов, определяющих политику Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым в отношении обработки и защиты персональных данных»

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями), Перечнем 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, утвержденным постановлением Правительства Российской Федерации от 21.03.2012 № 211,

ПРИКАЗЫВАЮ:

1.Утвердить следующие организационно-распорядительные документы, регламентирующие вопросы обработки и защиты персональных данных в Инспекции Гостехнадзора РК;

1.1. Правила обработки персональных данных в Инспекции Гостехнадзора РК (приложение № 1);

1.2. Правила рассмотрения запросов субъектов персональных данных или их представителей в Инспекции Гостехнадзора РК (приложение № 2);

1.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Инспекции Гостехнадзора РК (приложение № 3).

1.4. Перечень должностей государственных гражданских служащих Инспекции Гостехнадзора РК, замещение которых предусматривает

осуществление обработки персональных данных либо осуществление доступа к персональным данным (в том числе персональных данных обрабатываемым в информационной системе) (приложение № 4).

1.5. Инструкцию Ответственного за организацию обработки персональных данных (приложение № 5).

1.6. Инструкцию Администратора безопасности в Инспекции Гостехнадзора РК (приложение № 6).

1.7. Инструкцию пользователя информационных систем персональных данных (приложение № 7).

1.8. Типовое обязательство государственного гражданского служащего Инспекции Гостехнадзора РК, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (приложение № 8).

1.9. Типовая форма согласия на обратоку персональных данных заявителей при их обращении в Инспекцию Гостехнадзора РК (приложение № 9).

1.10. Типовая форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения при их обращении в Инспекцию Гостехнадзора РК (приложение № 10).

1.11. Типовая форма согласия на обработку персональных данных государственных служащих Инспекции Гостехнадзора РК, а также иных субъектов персональных данных (приложение № 11).

1.12. Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (приложение № 12).

1.13. Порядок доступа государственных гражданских служащих Инспекции Гостехнадзора РК в помещения, в которых ведется обработка персональных данных (приложение № 13).

1.14. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (приложение № 14).

1.15. Перечень информационных систем персональных данных, в которых осуществляется обработка персональных данных в Инспекции Гостехнадзора РК (приложение № 15).

1.16. Перечень персональных данных подлежащих защите (приложение № 16).

1.17. Форму акта определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных в Инспекции Гостехнадзора РК (приложене № 17).

1.18. Инструкцию по организации антивирусной защиты (приложение № 18).

1.19. Инструкцию по организации парольной защиты (приложение № 19).

1.20. Инструкцию по организации резерного копирования и воостановления информации (приложение № 20).

1.21. Инструкцию по обращению с криптосредствами (приложение № 21).

1.22. Инструкцию по установке, модификации, ремонту, техническому

обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств информационных систем персональных данных (приложение № 22).

1.23. План внутренних проверок режима защиты персональных данных (приложение № 23).

1.24. Перечень персональных данных участвующих при неавтоматизированной обработке (приложение № 24).

1.25. План мероприятий по обеспечению безопасности персональных данных (приложение № 25).

1.26. Положение о порядке хранения и уничтожения носителей персональных данных (приложение № 26).

1.27. Форму акта об уничтожении персональных данных (приложение № 27).

1.28. Форма журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (приложение № 28).

1.29. Форма журнала учета хранилищ, сейфов, специальных хранилищ, шкафов и ключей от них (приложение № 29).

1.30. Форма журнала уничтожения носителей персональных данных (приложение № 30).

1.31. Форма журнала учета машинных носителей персональных данных (приложение № 31).

1.32. Форма журнала учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных (приложение № 32).

1.33. Форма журнала учета мероприятий по контролю обеспечения защиты персональных данных (приложение № 33).

1.34. Форма журнала учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств ИСПДн (приложение № 34).

1.35. Форму журнала учета инцидентов информационной безопасности (приложение № 35).

1.36. Форму журнала учета средств защиты информации (приложение № 36).

1.37. Форму журнала программного обеспечения, разрешенного к установке (приложение № 37).

2. Назначить ответственными:

за организацию обработки персональных данных в информационных системах персональных данных Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым (далее - Инспекция Гостехнадзора РК) - Ан Владимира Борисовича, заместителя начальника Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым – заместителя главного государственного инженера-инспектора Республики Крым;

за обеспечение безопасности персональных данных в информационных системах персональных данных Инспекции Гостехнадзора РК (Администратор безопасности) – Непомнящего Олега Алексеевича, ведущего специалиста – ведущего государственного инженера-инспектора Отдела аналитической работы,

информационного обеспечения и административной практики Инспекции Гостехнадзора РК;

3. Признать утратившими силу:

приказ Инспекции Гостехнадзора РК от 03.10.2018г. № 154/ОД «Об определении должностных лиц ответственных за организацию обработки обеспечение безопасности персональных данных в информационной системе персональных данных, а также утверждении документов, определяющих политику в отношении обработки персональных данных в Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым»;

приказ Инспекции Гостехнадзора РК от 07.09.2020г. № 205/ОД «Об утверждении организационно-распорядительных документов, регламентирующих вопросы обработки и защиты персональных данных в Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым»;

приказ Инспекции Гостехнадзора РК от 27.11 2020г. № 251/ОД «О внесении изменений в приказ Инспекции Гостехнадзора 30.10.2018 № 154/ОД «Об определении должностных лиц ответственных за организацию обработки обеспечение безопасности персональных данных в информационной системе персональных данных, а также утверждении документов, определяющих политику в отношении обработки персональных данных в Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым».

4. Ведущему специалисту – ведущему государственному инженеру - инспектору Отдела аналитической работы, информационного обеспечения и административной практики Инспекции Гостехнадзора РК Непомнящему О.А. ознакомить с настоящим приказом и утвержденными документами государственных гражданских служащих Республики Крым, замещающих должности государственной гражданской службы Республики Крым в Инспекции Гостехнадзора РК под личную подпись.

5. Контроль за выполнением настоящего приказа возложить на заместителя начальника Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым – заместителя главного государственного инженера-инспектора Республики Крым Ан В.Б.

Начальник **А. ИГНАТЕНКО**

Список
Сотрудников ознакомленных приказом Инспекции Гостехнадзора РК
от 03.02.2022 года № 13/ОД

№ п/п	Ф.И.О. должностного лица Инспекции Гостехнадзора РК	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				
29.				
30.				
31.				

Приложение № 1
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

Правила
обработки персональных данных в Инспекции Гостехнадзора РК

I. Общие положения

1.1. Правила обработки персональных данных в Инспекции Гостехнадзора РК (далее - Правила) определяют цели, содержание и порядок обработки персональных данных, меры, процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в Инспекции Гостехнадзора РК (далее – Инспекция).

1.2. Настоящие Правила определяют политику Инспекции Гостехнадзора РК как оператора, самостоятельно или совместно с другими лицами организующего и (или) осуществляющего обработку персональных данных и определяющего цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.3. Основные понятия, используемых в Правилах:

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

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

Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 № 152-ФЗ;

Обработка персональных данных - любое действие (операция) 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, передачу (распространение, предоставление, доступ), удаление, уничтожение персональных данных.

Учет персональных данных - все процедуры по записи, систематизации и накоплению информации персонального характера.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.4. Настоящие Правила разработаны в соответствии с Трудовым кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»), Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 мая 2003 года № 58-ФЗ «О системе государственной службы Российской Федерации" (далее - Федеральный закон «О системе государственной службы Российской Федерации»), Федеральным законом от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации» (далее - Федеральный закон «О государственной гражданской службе Российской Федерации»), Федеральным законом от 25 декабря 2008 года № 273-ФЗ «О противодействии коррупции» (далее - Федеральный закон «О противодействии коррупции»), Указом Президента Российской Федерации от 30 мая 2005 года № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Российской Федерации от 10 сентября 2009 года № 723 «О порядке ввода в эксплуатацию отдельных государственных информационных систем», постановлением Правительства Российской Федерации от 27 января 2009 года № 63 «О предоставлении федеральным государственным гражданским служащим единовременной субсидии на приобретение жилого помещения» (далее - постановление Правительства Российской Федерации «О предоставлении федеральным государственным гражданским служащим единовременной субсидии на приобретение жилого помещения»), распоряжением Правительства Российской Федерации от 26 мая 2005 года № 667-р об

утверждении формы анкеты, подлежащей представлениюв государственный орган, орган местного самоуправления, аппарат избирательной комиссии муниципального образования гражданином Российской Федерации, изъявившим желание участвовать в конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации, поступающим на государственную гражданскую службу Российской Федерации или на муниципальную службу в Российской Федерации, распоряжением Правительства Российской Федерации от 6 октября 2011 года №1752-р об утверждении перечня документов, прилагаемых заявителем к заявлению о регистрации (перерегистрации) средства массовой информации.

1.5. Обработка персональных данных в Инспекции осуществляется с соблюдением принципов и условий, предусмотренных настоящими Правилами и законодательством Российской Федерации в области персональных данных.

II. Условия и порядок обработки персональных данных

2.1. Персональные данные государственных гражданских служащих, замещающих должности в Инспекции (далее гражданские служащие) и граждан, претендующих на замещение вакантных должностей государственной гражданской службы в Инспекции (далее - граждане, претендующие на замещение вакантных должностей) обрабатываются в целях обеспечения кадровой работы, в том числе в целях содействия гражданским служащим в прохождении гражданской службы, формирования кадрового резерва государственной гражданской службы, обучения и должностного роста, учета результатов исполнения гражданскими служащими должностных обязанностей, обеспечения личной безопасности гражданских служащих и членов их семьи, обеспечения гражданским служащим установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества, а также в целях противодействия коррупции, осуществления и выполнения функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Инспекцию.

2.2. В целях, указанных в пункте 2.1 настоящих Правил, обрабатываются следующие категории персональных данных гражданских служащих и граждан, претендующих на замещение вакантных должностей:

2.2.1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

2.2.2. число, месяц, год рождения;

2.2.3. место рождения;

2.2.4. реквизиты страхового свидетельства государственного пенсионного страхования;

2.2.5. идентификационный номер налогоплательщика;

2.2.6. реквизиты страхового медицинского полиса обязательного медицинского страхования;

2.2.7. реквизиты свидетельства государственной регистрации актов гражданского состояния;

2.2.8. семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

2.2.9. сведения о трудовой деятельности;

2.2.10. сведения о воинском учете и реквизиты документов воинского учета;

2.2.11. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

2.2.12. сведения об ученой степени;

2.2.13. информация о владении иностранными языками, степень владения;

2.2.14. медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению;

2.2.15. фотография;

2.2.16. сведения о прохождении государственной гражданской службы, в том числе: дата, основания поступления на государственную гражданскую службу и назначения на должность государственной гражданской службы, дата, основания назначения, перевода, перемещения на иную должность государственной гражданской службы, наименование замещаемых должностей государственной гражданской службы с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности государственной гражданской службы, а также сведения о прежнем месте работы;

2.2.17. информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту;

2.2.18. сведения о пребывании за границей;

2.2.19. информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы;

2.2.20. информация о наличии или отсутствии судимости;

2.2.21. информация об оформленных допусках к государственной тайне;

2.2.22. государственные награды, иные награды и знаки отличия;

2.2.23. сведения о профессиональной переподготовке и (или) повышении квалификации;

2.2.24. информация о ежегодных оплачиваемых отпусках, учебных отпусках, отпусках по временной нетрудоспособности и отпусках без сохранения денежного содержания;

2.2.25. сведения о доходах, расходах, об имуществе и обязательствах имущественного характера (в том числе членов семьи);

2.2.26. номер расчетного счета;

2.2.27. номер банковской карты;

2.2.28. иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 2.1. настоящих Правил.

2.3. Обработка персональных данных гражданских служащих и граждан,

претендующих на замещение вакантных должностей, может осуществляться без согласия указанных лиц в рамках целей, определенных пунктом 2.1 настоящих Правил, в соответствии с пунктом 2 части 1 статьи 6, частью 2 статьи 11 Федерального закона «О персональных данных» и положениями Федерального закона «О системе государственной службы Российской Федерации», Федерального закона «О государственной гражданской службе Российской Федерации», Федерального закона «О противодействии коррупции», Трудового кодекса Российской Федерации.

2.4. Обработка специальных категорий персональных данных гражданских служащих, а также граждан, претендующих на замещение вакантных должностей, осуществляется без согласия указанных граждан в рамках целей, определенных пунктом 2.1. Правил, в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10 Федерального закона «О персональных данных» и положениями Трудового кодекса Российской Федерации.

2.5. Обработка персональных данных гражданских служащих и граждан, претендующих на замещение вакантных должностей, осуществляется при условии получения согласия указанных лиц в следующих случаях:

2.5.1. при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации о государственной гражданской службе и Трудовым кодексом Российской Федерации;

2.5.2. при трансграничной передаче персональных данных;

2.5.3. при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

2.6. В случаях, предусмотренных пунктом 2.5. настоящих Правил, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

2.7. Обработка персональных данных гражданских служащих и граждан, претендующих на замещение вакантных должностей, осуществляется должностным лицом Инспекции, ответственным за организацию и ведение кадрового учета (далее - должностное лицо, ответственное за ведение кадрового учета), должностным лицом Инспекции, ответственным за организацию и ведение бухгалтерского учета (далее - должностное лицо, ответственное за ведение бухгалтерского учета), должностным лицом Инспекции, ответственным за профилактику коррупционных и иных правонарушений, должностным лицом Инспекции, ответственным за обеспечение безопасности персональных данных в информационной системе персональных данных и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных гражданских служащих и граждан,

претендующих на замещение вакантных должностей, осуществляется путем:

2.8.1. получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые должностному лицу, ответственному за ведение кадрового учета);

2.8.2. копирования оригиналов документов;

2.8.3. внесения сведений в учетные формы на бумажных носителях (в информационную систему обработки персональных данных);

2.8.4. формирования персональных данных в ходе кадровой работы (в ходе работы должностного лица, ответственного за ведение бухгалтерского учета).

2.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляются путем получения персональных данных непосредственно от гражданских служащих и граждан, претендующих на замещение вакантных должностей.

2.10. В случае возникновения необходимости получения персональных данных гражданского служащего у третьей стороны следует известить об этом гражданского служащего заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных.

2.11. Запрещается получать, обрабатывать и приобщать к личному делу гражданского служащего, а также вносить в информационную систему обработки персональных данных, персональные данные, не предусмотренные пунктом 2.2 настоящих Правил, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.12. При сборе персональных данных должностное лицо, ответственное за ведение кадрового учета, осуществляющее сбор (получение) персональных данных непосредственно от гражданских служащих и граждан, претендующих на замещение вакантных должностей, обязан разъяснить в соответствии с установленной формой (приложение № 9) указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

2.13. Передача (распространение, предоставление) и использование персональных данных гражданских служащих и граждан, претендующих на замещение вакантных должностей, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

2.14. Гражданским служащим, замещающим должности, предусматривающие в соответствии с их должностными обязанностями осуществление обработки персональных данных, могут получать и обрабатывать лишь те персональные данные гражданских служащих, доступ к которым им разрешен.

III. Условия и порядок обработки персональных данных, необходимых для осуществления и выполнения функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Инспекцию

3.1. В Инспекции обработка персональных данных граждан и организаций, обратившихся в Инспекцию, осуществляется, в том числе в целях осуществления и выполнения функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Инспекцию.

3.2. Персональные данные граждан, обратившихся в Инспекцию лично (через законного представителя), а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением граждан о результатах рассмотрения.

В соответствии с законодательством Российской Федерации в Инспекции подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан, лиц без гражданства, а также обращения организаций.

3.3. При рассмотрении обращений граждан Российской Федерации, иностранных граждан, лиц без гражданства подлежат обработке их следующие персональные данные:

3.3.1. фамилия, имя, отчество (последнее при наличии);

3.3.2. почтовый адрес;

3.3.3. адрес электронной почты;

3.3.4. указанный в обращении контактный телефон;

3.3.5. иные персональные данные, указанные в обращении, а также ставшие известными в ходе личного приема граждан или в процессе рассмотрения обращения.

3.4. Обработка персональных данных субъектов персональных данных, необходимых для осуществления и выполнения функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Инспекцию, осуществляется в случаях и порядке, предусмотренных федеральным законом.

IV. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения

4.1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных (приложение № 10). Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

4.2. Обработка персональных данных, разрешенных субъектом персональных данных для распространения осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 ФЗ-152 «О Персональных данных».

V. Порядок обработки персональных данных в автоматизированныхинформационных системах

5.1. Обработка персональных данных в Инспекции осуществляется:

5.1.1. В локальной базе данных автоматизированной информационной системы управления органами гостехнадзора (далее — АИС «Гостехнадзор Эксперт»), которая содержит следующие персональные данные, внесённые на основании документов, предусмотренных действующим законодательством Российской Федерации и Республики Крым:

- форм, утвержденных Постановлением Госкомстата России от 05.01.2004 № 1, «Личная карточка государственного (муниципального) служащего» (Т2-ГС) для государственных гражданских служащих и «Личная карточка работника» (Т2);
- для иных работников;
- трудовой книжки;
- документов об образовании;
-документов о повышении квалификации, профессиональной переподготовке;
- справки о соблюдении гражданином ограничений, связанных с замещением государственной должности;
- копии удостоверений о наградах и прочих документов, приобщённых к личному делу.

5.1.2. В базе данных АИС «Гостехнадзор-Эксперт» которая содержит следующие персональные данные, внесённые на основании документов, предусмотренных действующим законодательством Российской Федерации:

- фамилия, имя, отчество (при наличии);
- дата рождения;
- адрес регистрации (фактическое место проживания);
- идентификационный номер налогоплательщика;
- паспорт (серия, номер, кем и когда выдан);
- номер телефона (домашний, мобильный);
- водительское удостоверение (серия, номер, кем и когда выдан);
- фотография.

5.1.3. На аттестованных под обработку персональных данных автоматизированных рабочих местах.

5.2. Информация может вноситься как в автоматическом режиме, так и в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять её автоматическую регистрацию.

5.3. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Инспекции, достигается путём исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

5.3.1. определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных Инспекции;

5.3.2. применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Инспекции, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищённости персональных

данных;

5.3.3. применения прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

5.3.4. оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5.3.5. учёта машинных носителей персональных данных;

5.3.6. обнаружения фактов несанкционированного доступа к персональным данным и принятие мер;

5.3.7. восстановления персональных данных, модифицированных или удалённых, уничтоженных вследствие несанкционированного доступа к ним;

5.3.8. установления правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных Инспекции, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Инспекции;

5.3.9. контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищённости информационных систем персональных данных.

5.3.10. недопущения воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

5.3.11. обеспечения возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.3.12. осуществления постоянного контроля за обеспечением уровня защищенности персональных данных;

5.3.13. соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

5.3.14. учёта применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

5.3.15. при обнаружении нарушений порядка предоставления персональных данных, незамедлительного приостановления предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;

5.3.16. разбирательства и составления заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищённости персональных данных, разработку и принятия мер по предотвращению возможных опасных последствий подобных нарушений.

5.4. Обмен персональными данными при их обработке в информационных системах персональных данных Инспекции осуществляется по каналам связи, защита которых обеспечивается путём реализации соответствующих организационных мер и путём применения программных и технических средств.

5.5. Доступ государственных служащих (работников) Инспекции к персональным данным, находящимся в информационных системах персональных данных Инспекции, предусматривает обязательное прохождение процедуры идентификации и аутентификации.

5.6. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных Инспекции уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

VI. Работа с обезличенными данными

6.1. Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

6.2. Обезличивание персональных данных может быть проведено с целью ведения статистического учета и отчетности, снижения ущерба от разглашения персональных данных, снижения уровня защищенности автоматизированных информационных систем, если иное не предусмотрено действующим законодательством Российской Федерации.

6.3. Обезличивание персональных данных осуществляется в соответствии с приказом Роскомнадзора от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

6.4. Обезличенные персональные данные не подлежат разглашению.

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

VII. Сроки обработки и хранения персональных данных

7.1. В соответствии с утвержденной номенклатурой дел Инспекции в порядке, предусмотренном законодательством Российской Федерации, определяются иустанавливаются сроки обработки и хранения персональных данных гражданских служащих, а также граждан, претендующих на замещение вакантных должностей:

7.1.1. персональные данные, содержащиеся в приказах по личному составу (о приеме, о переводе, об увольнении, об установлении надбавок);

7.1.2. персональные данные, содержащиеся в личных делах и личных карточках гражданских служащих;

7.1.3. персональные данные, содержащиеся в приказах о поощрениях, материальной помощи гражданских служащих;

7.1.4. персональные данные, содержащиеся в приказах о предоставлении отпусков, о краткосрочных внутрироссийских и зарубежных командировках, о дисциплинарных взысканиях гражданских служащих;

7.1.5. персональные данные, содержащиеся в документах граждан, претендующих на замещение вакантных должностей, не допущенных к участию в

конкурсе на замещение вакантных должностей гражданской службы в Инспекции (далее - конкурс), и кандидатов, участвовавших в конкурсе;

7.1.6. Сроки обработки и хранения персональных данных, предоставляемых в связи с осуществлением и выполнением функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Инспекцию, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

7.2. Персональные данные граждан, обратившихся в Инспекцию лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в соответствии с утвержденной номенклатурой дел Инспекции в порядке, предусмотренном законодательством Российской Федерации.

7.3. Персональные данные, предоставляемые на бумажном носителе в связи с осуществлением и выполнением функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Инспекцию, хранятся государственными служащими Инспекции, к полномочиям которых относится обработка персональных данных в соответствии с утвержденной номенклатурой дел Инспекции, в порядке, предусмотренном законодательством Российской Федерации.

7.4. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

7.5. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в целях, определенных Правилами.

7.6. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители структурных подразделений Инспекции.

7.7. Срок хранения персональных данных, внесенных в автоматизированные информационные системы, должен соответствовать сроку хранения бумажных оригиналов.

VIII. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

8.1. Структурным подразделением Инспекции, ответственным за документооборот и архивирование, осуществляется контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

8.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании Комиссии по уничтожению

персональных данных Инспекции (далее - КУПД Инспекции), состав которой утверждается приказом Инспекции.

По итогам заседания КУПД Инспекции составляются протокол и акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами КУПД Инспекции и утверждается начальником Инспекции.

8.3. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации с последующей утилизацией.

IX. Обработка персональных данных в рамках межведомственного информационного взаимодействия с применением единой системы межведомственного электронного взаимодействия

9.1. Инспекция в соответствии с законодательством Российской Федерации может осуществлять обработку персональных данных в рамках межведомственного электронного информационного взаимодействия в электронном виде с применением единой системы межведомственного электронного взаимодействия.

X. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных субъектов персональных данных

10.1. Лица, виновные в нарушении требований, регулирующих получение, обработку и защиту персональных данных субъектов персональных данных, несут предусмотренную законодательством Российской Федерации ответственность.

10.2. Моральный вред, причинённый субъекту персональных данных вследствие нарушения Инспекцией его прав, нарушения правил обработки персональных данных, установленных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», а также требований к защите персональных данных, установленных в соответствии сданным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесённых субъектом персональных данных убытков.

Приложение № 2
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

Правила
рассмотрения запросов субъектов персональных данных или их представителей в Инспекции Гостехнадзора РК

1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей в Инспекции Гостехнадзора РК (далее - Правила) определяют порядок учета (регистрации) и рассмотрения запросов субъектов персональных данных или их представителей.

2. Настоящие Правила разработаны в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), Федеральным законом от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами.

3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных Инспекцией Гостехнадзора РК (далее - Инспекция);

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Инспекцией способы обработки персональных данных;

4) наименование и место нахождения Инспекции, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Инспекцией 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 № 152-ФЗ;

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

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Инспекции, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

4. Субъект персональных данных вправе требовать от Инспекции уточнения его персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5. Информация, указанная в пункте 3 настоящих Правил, (далее информация) должна быть предоставлена субъекту персональных данных оператором в доступной форме в течение тридцати дней с даты получения такого запроса. В ней не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6. Информация предоставляется субъекту персональных данных или его представителю при его обращении либо при получении от него или его представителя запроса. Запрос должен содержать:

1) номер, серию документа, удостоверяющего личность субъекта персональных данных или его представителя, дату выдачи, наименование органа, выдавшего его;

2) информацию, подтверждающую участие субъекта персональных данных в правоотношениях с Инспекцией, либо информацию, иным образом подтверждающую факт обработки персональных данных в Инспекции, заверенную подписью субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7. Все поступившие запросы подлежит обязательной регистрации в день поступления в Инспекции в журнале регистрации и учета запросов (обращений) субъектов персональных данных, по форме согласно приложению к Правилам.

8. Запрос проверяется на повторность, а при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если информация, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных, субъект персональных данных вправе повторно обратиться в Инспекцию лично или направить повторный запрос в целях получения указанной информации и ознакомления с персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен законодательством Российской Федерации или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

9. Субъект персональных данных вправе повторно обратиться в Инспекцию лично или направить повторный запрос в целях получения информации, а также в целях ознакомления с обрабатываемыми персональными данными до истечения

срока, указанного в пункте 8 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 6 Правил, должен содержать обоснование направления повторного запроса.

10. Инспекция вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 8 и 9 Правил. Такой отказ должен быть мотивированным.

11. Инспекция обязана предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. 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, государственные гражданские служащие Инспекции, уполномоченными на обработку персональных данных (далее - гражданские служащие Инспекции), обязаны внести в них необходимые изменения. 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, гражданские служащие Инспекции обязаны уничтожить такие персональные данные. Инспекция обязана 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.

12. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных, гражданские служащие Инспекции обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Инспекции) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, гражданские служащие Инпсекции обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Инспекции) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

13. В случае подтверждения факта неточности персональных данных

уполномоченные гражданские служащие на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, обязаны уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Инспекции) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

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

Приложение
к Правилам рассмотрения запросов субъектов персональных данных или их представителей в Инспекции Гостехнадзора РК

Журнал
регистрации и учета запросов (обращений) субъектов персональных данных

№ п/п	Дата и рег. Номер запроса (обращения)	Сведения о запрашивающем лице (ФИО, паспортные данные)	Краткое содержание запроса (обращения)	Отметка о предоставлении и (отказе в предоставлении) информации	Дата и рег. Номер ответа на запрос (обращение)	Подпись ответственного лица
1	2	3	4	5	6	7

Приложение № 3
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

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

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым (далее - Инспекции Гостехнадзора РК) требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Правила), устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют порядок проведения процедур внутреннего контроля исполнения требований законодательства.

2. В настоящих правилах используются основные понятия, определенные в статье 3 Федерального закона «О персональных данных».

3. Действие правил распространяется на все персональные данные субъектов, обрабатываемые в Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым с применением средств автоматизации и без применения таких средств.

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым организовывается проведение периодических проверок условий обработки персональных данных (далее - проверки).

5. Проверки осуществляются Ответственным за организацию обработки персональных данных в Инспекции Гостехнадзора РК, либо комиссией, утвержденной приказом НачальникаИнспекции Гостехнадзора РК.

6. Проверки соответствия обработки персональных данных установленным требованиям проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в Инспекция Гостехнадзора РК письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

7. Плановые проверки проводятся не чаще чем один раз в год.

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

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

- порядок и условия применения организационных и технических мер по

обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;

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

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

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

- осуществление мероприятий по обеспечению целостности персональных данных.

10. Ответственный за организацию обработки персональных данных или Комиссия в ходе проверки имеет право:

- запрашивать у работников Инспекции Гостехнадзора РК информацию, необходимую для реализации полномочий;

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

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

- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

11. В отношении персональных данных, ставших известными комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

12. По результатам проведения проверки оформляется акт проверки, который подписывается членами комиссии. Срок проведения проверки и оформления акта составляет 30 календарных дней со дня начала проверки, указанного в правовом акте о назначении проверки.

13. О результатах проверки и мерах, принятых для устранения нарушений, ответственное лицо (председатель комиссии) докладывает Начальнику Инспекции Гостехнадзора РК.

Утверждаю
Начальник Инспекции Гостехнадзора РК
_____
(Ф.И.О.)
«_____»_____20__г.

Приложение к Правилам
осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям
к защите персональных данных
в Инспекции Гостехнадзора РК

Акт №
проведения проверки соблюдения порядка и условий обработки персональныхданных

Настоящий Акт составлен в том, что «___»_____ 20__года, комиссией (лицом, ответственным за организацию обработки персональных данных) для проведения проверки соблюдения порядка и условий обработки персональных данных в составе:

председателя комиссии:

_____
(замещаемая должность гражданской службы, Ф.И.О. гражданского служащего)

Членов комиссии:

_____
(замещаемая должность гражданской службы, Ф.И.О. гражданского служащего)
_____
(замещаемая должность гражданской службы, Ф.И.О. гражданского служащего)
_____
(замещаемая должность гражданской службы, Ф.И.О. гражданского служащего), действующей в соответствии с приказом начальника Инспекции Гостехнадзора РК от _____№_____
проведена проверка_____
(тематика проверки)
Проверка соблюдения порядка и условий обработки персональных данных осуществлялась в соответствии с требованиями _____
_____
_____
_____
_____
_____
(наименование и реквизиты (дата регистрации и номер) документа/нормативного правового акта)

В ходе проверки проведены следующие мероприятия:_____

_____

_____

_____

_____

В процессе проведения проверки выявлены нарушения:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Меры по устранению нарушений:

_____

_____

_____

_____

_____

_____

_____

Сроки устранения выявленных нарушений: _____

Председатель комиссии _____**(Ф.И.О.)**

Члены комиссии: _____**(Ф.И.О.)**

_____**(Ф.И.О.)**

_____**(Ф.И.О.)**

«___»_____ _____г.

Приложение № 4
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

Перечень
должностей государственных гражданских служащих Инспекции Гостехнадзора РК, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (в том числе персональных данных обрабатываемым в информационной системе).

Наименование	Должность государственной гражданской службы
Руководство	Начальник инспекции – главный государственный инженер-инспектор Республики Крым
	Заместитель начальника инспекции - заместитель главного государственного инженера-инспектора Республики Крым
Управление правового, кадрового, финансового, документального и материально-технического обеспечения	Начальник управления
	Заместитель начальника управления
Отдел финансового и документального обеспечения	Ведущий специалист
Отдел правовой, кадровой и антикоррупционной работы	Заведующий отделом
	Консультант
	Ведущий специалист
Отдел надзора и государственной регистрации аттракционов	Заведующий отделом – главный государственный инженер-инспектор города, района Республики Крым
	Главный консультант – главный государственный инженер-инспектор города, района Республики Крым
	Специалист 1 категории - государственный инженер-инспектор
Отдел надзора и государственной регистрации самоходных машин и других видов техники	Заведующий отделом – главный государственный инженер-инспектор города, района Республики Крым
	Заместитель заведующего отделом – главный государственный инженер-инспектор города,

	района Республики Крым
	Главный консультант – главный государственный инженер-инспектор города, района Республики Крым
	Консультант – главный государственный инженер-инспектор города, района Республики Крым
Отдел аналитической работы, информационного обеспечения и административной практики	Заведующий отделом – главный государственный инженер-инспектор города, района Республики Крым
	Ведущий специалист – ведущий государственный инженер-инспектор
	Специалист 1 категории - государственный инженер-инспектор

Приложение № 5
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

ИНСТРУКЦИЯ
Ответственного за организацию обработки персональных данных

1. Общие положения

1.1. Инструкция ответственного за организацию обработки персональных данных (далее – Инструкция) в Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым (далее - Инспекции Гостехнадзора РК) определяет основные обязанности и права ответственного за организацию обработки персональных данных в Инспекции Гостехнадзора РК.

1.2. Инструкция регулирует отношения и порядок взаимодействия между Ответственным за организацию обработки персональных данных в Инспекции Гостехнадзора РК и сотрудниками Инспекции Гостехнадзора РК, которые обрабатывают персональные данные, в связи с реализацией трудовых отношений, в соответствии с действующим законодательством Российской Федерации.

1.3. Ответственный за организацию обработки персональных данных в Инспекции Гостехнадзора РК в своей деятельности руководствуется действующим законодательством Российской Федерации, правовыми актами Инспекции Гостехнадзора РК, а также настоящей Инструкцией.

2. Должностные обязанности

Ответственный за организацию обработки персональных данных в Инспекции Гостехнадзора РК обязан:

1.1. Организовывать работу в Инспекции Гостехнадзора РК по разработке и принятию правил обработки персональных данных в Инспекции Гостехнадзора РК, которые определяют:

- порядок доступа к персональным данным в Инспекции Гостехнадзора РК;
- организацию приема и обработки в Инспекции Гостехнадзора РК обращений и запросов субъектов персональных данных или их представителей;
- процедуры, направленные на предотвращение и выявление в Инспекции Гостехнадзора РК нарушений действующего законодательства Российской Федерации о персональных данных и устранение последствий таких нарушений;

1.2. Организовывать ознакомление сотрудников Инспекции Гостехнадзора РК, непосредственно осуществляющих обработку персональных данных, с действующим законодательством Российской Федерации о персональных данных и правовыми актами Инспекции Гостехнадзора РК, определяющими правила обработки персональных данных в Инспекции Гостехнадзора РК и требования по

защите персональных данных;

1.3. Руководить осуществлением принятия необходимых правовых, организационных и технических мер для защиты персональных данных в Инспекции Гостехнадзора РК в соответствии с действующим законодательством Российской Федерации о персональных данных;

1.4. Осуществлять согласование мероприятий при создании в Инспекции Гостехнадзора РК новых информационных систем персональных данных;

1.5. Координировать работу в структурных подразделениях Инспекции Гостехнадзора РК по формированию и ведению перечней:

- должностей сотрудников Инспекции Гостехнадзора РК, замещение которых предусматривает осуществление обработки персональных данных;
- персональных данных, обрабатываемых в Инспекции Гостехнадзора РК;
- информационных систем персональных данныхИнспекции Гостехнадзора РК;

1.6. Организовывать своевременное направление в Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций уведомления об обработке персональных данных в Инспекции Гостехнадзора РК при намерении осуществлять обработку персональных данных в Инспекции Гостехнадзора РК или изменении положений уведомления об обработке персональных данных в Инспекции Гостехнадзора РК;

1.7. Организовывать и руководить проведением внутренних проверок организации состояния работ по вопросам информационной безопасности в Инспекции Гостехнадзора РК для осуществления периодического контроля:

- условий обработки персональных данных в Инспекции Гостехнадзора РК и их соответствие требованиям действующего законодательства Российской Федерации о персональных данных и принятыми в соответствии с ним правовыми актами Инспекции Гостехнадзора РК;
- организации приема и обработки в Инспекции Гостехнадзора РК обращений и запросов субъектов персональных данных или их представителей;
- выполнения, установленных в соответствии с действующим законодательством Российской Федерации и правовыми актами Инспекции Гостехнадзора РК требований к защите персональных данных, обрабатываемых в Инспекции Гостехнадзора РК;
- соотношения оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения действующего законодательства Российской Федерации о персональных данных и принимаемых Инспекцией Гостехнадзора РК мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством Российской Федерации и правовыми актами Инспекции Гостехнадзора РК;

1.8. Представлять доклады Начальнику Инспекции Гостехнадзора РК о результатах проведенных внутренних проверок организации состояния работ по вопросам информационной безопасности в Инспекции Гостехнадзора РК и мерах, необходимых для устранения выявленных нарушений;

1.9. Координировать работу в Инспекции Гостехнадзора РК на принятие мер, направленных на совершенствование защиты персональных данных, обрабатываемых в Инспекции Гостехнадзора РК;

1.10. Осуществлять методическое руководство при разработке условий обработки персональных данных и эффективности мер по защите персональных данных в Инспекции Гостехнадзора РК;

1.11. Организовывать работу по планированию прохождения обучения сотрудников Инспекции Гостехнадзора РК по вопросам обеспечения защиты персональных данных, обрабатываемых в Инспекции Гостехнадзора РК.

3. Права

Ответственный за организацию обработки персональных данных в Инспекции Гостехнадзора РК имеет право:

1.1. Запрашивать в структурных подразделениях Инспекции Гостехнадзора РК, в которых ведется обработка персональных данных или планируется ведение обработки персональных данных, любые сведения, необходимые для организации условий обработки персональных данных и принятия необходимых правовых, организационных и технических мер для защиты персональных данных в Инспекции Гостехнадзора РК;

1.2. Принимать участие в рассмотрении жалоб и обращений граждан или юридических лиц по вопросам, связанным с обработкой персональных данных в Инспекции Гостехнадзора РК, а также вырабатывать предложения для принятия в пределах своих полномочий решений по результатам рассмотрения указанных жалоб и обращений;

1.3. Участвовать в расследовании нарушений в области защиты персональных данных в Инспекции Гостехнадзора РК и разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений;

1.4. Требовать от структурных подразделений Инспекции Гостехнадзора РК уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных, при обращении (запросе) субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных либо по результатам проведенной внутренней проверки организации состояния работ по вопросам информационной безопасности в Инспекции Гостехнадзора РК;

1.5. Принимать меры по приостановлению или прекращению обработки персональных данных в Инспекции Гостехнадзора РК, осуществляемой с нарушением требований действующего законодательства Российской Федерации о персональных данных;

1.6. Вносить предложения о совершенствовании нормативного правового регулирования обработки и защиты персональных данных в Инспекции Гостехнадзора РК.

4. Взаимоотношения (связи по должности)

Ответственный за организацию обработки персональных данных в Инспекции Гостехнадзора РК взаимодействует:

1.1. С должностными лицами структурных подразделений Инспекции Гостехнадзора РК и других организаций всех организационно-правовых форм – по вопросам организации и выполнения условий обработки и защиты персональных данных в Инспекции Гостехнадзора РК;

1.2. С территориальными органами федеральных органов, обеспечивающими защиту прав субъектов персональных данных, контроль организации работы с персональными данными и эффективность защиты персональных данных в Инспекции Гостехнадзора РК, в соответствии со своими полномочиями.

5. Ответственность

Ответственный за организацию обработки персональных данных в Инспекции Гостехнадзора РК несет ответственность за ненадлежащее выполнение возложенных на него обязанностей, прописанных в настоящей Инструкции, в соответствии с действующим законодательством Российской Федерации и правовыми актами Инспекции Гостехнадзора РК.

6. Заключительные положения

Инструкция подлежит пересмотру в случае изменения законодательства Российской Федерации о персональных данных, определяющего должностные обязанности ответственного за организацию обработки персональных данных в Инспекции Гостехнадзора РК.

Приложение № 6
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

ИНСТРУКЦИЯ
Администратора безопасности в Инспекции Гостехнадзора РК

1. Обозначения и сокращения

АРМ – автоматизированное рабочее место;

ИСПДн–информационная система персональных данных;

АРМ – автоматизированное рабочее место;

ВТСС – вспомогательные технические средства и системы;

ИБ – информационная безопасность;

ОТСС – основные технические средства и системы;

ПДн – персональные данные;

ПЭВМ – персональная электронно-вычислительная машина;

СВТ – средства вычислительной техники;

СЗИ – средства защиты информации;

СЗПДн – система (подсистема) защиты персональных данных;

УБПДн – угрозы безопасности персональным данным;

ПО – программное обеспечение;

ОРД – организационно-распорядительная документация;

ОС – операционная система;

Машинные носители информации (МНИ)–накопители на жестких магнитных дисках (HDD);

Съемные носители информации (СНИ) – USB-флэш-накопители информации.

2. Общие положения

2.1. Настоящий документ определяет основные обязанности, права и ответственность Администратора безопасности.

2.2. Администратор безопасности осуществляет контроль выполнения требований организационных и технических мероприятий по обеспечению безопасности информации в ИСПДн.

2.3. Методическое руководство и контроль работы Администратора безопасности осуществляется Ответственным за организацию обработки

персональных данных в Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым.

3. Особенности организации работы в ИСПДн

Администратор безопасности должен знать, что:

ИСПДн относится к многопользовательским с разными правами доступа пользователей к ресурсам ИСПДн.

Группы пользователей, работающих в ИСПДн: администратор информационной безопасности, пользователи ИСПДн.

Данные группы пользователей имеют права доступа к ресурсам ИСПДн в соответствии с разрешительной системой доступа пользователей к сведениям конфиденциального характера ИСПДн.

4. Обязанности Администратора безопасности

4.1. Администратор безопасности должен:

4.1.1. Знать нормативно-методические документы в области безопасности информации и организационно-распорядительные документы в части его касающейся;

4.1.2. Знать состав ОТСС ИСПДн и контролировать их соответствие техническому паспорту на ИСПДн. Вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения);

4.1.3. Контролировать процесс управления (заведения, активации, блокирования, уничтожения) учетными записями пользователей ИСПДн:

- Проверять соответствие прав доступа пользователей к объектам доступа ИСПДн в соответствии с задачами, решаемыми пользователями в ИСПДн и взаимодействующими с ней ИСПДн и Разрешительной системой доступа к ИСПДн;
- Контролировать однозначное соответствие идентификатора и пользователя;
- Контролировать назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы персональных данных;
- Проверять отсутствие в ИСПДн учетных записей уволенных (отстраненных) сотрудников;
- Оповещать администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;
- Проверять своевременность удаления временных учетных записей, предоставленных для однократного (ограниченного по времени) выполнения задач в ИСПДн.

4.1.4. Контролировать неизменность настроек средств защиты информации:

- Настройки средств защиты информации должны препятствовать передаче защищаемой информации через сеть Интернет (или) другие информационно-телекоммуникационные сети международного информационного обмена по незащищенным линиям связи;

- Средства защиты информации должны ограничивать доступ к ИСПДн на 10 минут при 5 неудачных попытках входа в ИСПДн;

- Должен быть запрещен доступ к ИСПДн до прохождения процедур аутентификации и идентификации;

- Должен обеспечиваться запрет удаленного доступа к ИСПДн.

4.1.5. Контролировать запрет использования в ИСПДн технологий беспроводного доступа и мобильных технических средств.

4.1.6. Контролировать в случае доступа к ИСПДн со стороны пользователей информационных систем сторонних организаций:

- наличие договора (соглашения) об информационном взаимодействии с владельцем внешней информационной системы персональных данных;

- подтверждать выполнение во внешней информационной системе персональных данных предъявленных к ней требований о защите информации.

4.1.7. Контролировать установку на АРМ ИСПДн ПО с целью отсутствия в составе АРМ ИСПДн стороннего ПО, не связанного с задачами, решаемыми пользователями в ИСПДн.

4.1.8. Вести учет машинных носителей персональных данных. В том числе выборочно проверять носители информации и хранящуюся на них информацию.

4.1.9. Обеспечивать уничтожение (стирание) защищаемой информации с машинных носителей АРМ ИС, при их передаче в сторонние организации для ремонта или утилизации, либо контролировать процесс уничтожения (стирания). Уничтожение защищаемой информации должно исключать возможность восстановления защищаемой информации.

4.1.10. Контролировать регистрацию в информационной системе персональных данных следующих событий безопасности:

- входа (выхода), а также попытки входа субъектов доступа в информационную систему персональных данных и загрузки (останова) операционной системы (дата (время) входа/выхода в систему (из системы) или загрузки/останова операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа).

- подключения машинных носителей информации и вывода информации на носители информации (дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации).

- запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации (дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)).

- попыток доступа программных средств к защищаемым объектам доступа (дата и время попытки доступа к защищаемому файлу с указанием ее результата

(успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого файла (логическое имя, тип)).

- попыток удаленного доступа (дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе персональных данных).

4.1.11. Контролировать права на доступ к информации о событиях безопасности: доступ должен предоставляться исключительно администраторам ИСПДн, обеспечивающим функционирование ИСПДн, а также администратору информационной безопасности.

4.1.12.Обеспечивать постоянный контроль за выполнением пользователями ИСПДн установленного комплекса мероприятий по обеспечению безопасности информации и соблюдения действующего законодательства в области информационной безопасности, а также инструкции пользователя и других организационно-распорядительных документов в части обеспечения безопасности информации;

4.1.13. Требовать от пользователей ИСПДн и выполнять самому требования «Инструкции по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств информационных систем персональных данных» и вести «Журнал учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств ИСПДн»;

4.1.14. Контролировать порядок учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов;

4.1.15. Контролировать использование пользователями только учтенных съемных носителей. После того как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.) информация незамедлительно удаляется с носителей;

4.1.16. Контролировать настройки ОС и СЗИ АРМ пользователей

4.1.17. Проводить инструктаж пользователей по правилам работы с используемыми средствами и системами зашиты информации;

4.1.18. Устанавливать права доступа пользователей к информационным и техническим ресурсам ИСПДн в соответствии с принятой и утвержденной разрешительной системой доступа;

4.1.19. Следить за изменением программной среды ИСПДн и полномочиями пользователей;

4.1.20. Хранить дистрибутивы СЗИ, производить при необходимости восстановление программной среды СЗИ или настройки защитных механизмов операционной системы и привилегий пользователей по доступу к ресурсам ИС.

При необходимости для данных мероприятий привлекать других технических специалистов Инспекции Гостехнадзора РК;

4.1.21. Фиксировать и пресекать невыполнение пользователями ИСПДн требований или норм нормативно-методических документов в области безопасности информации и организационно-распорядительных документов в информационной сфере, а также создания пользователями возможностей утечки информации;

4.1.22. При получении информации о фактах нарушения политики и правил безопасности, а также попыток использования внешними нарушителями атак, в том числе с использованием методов социальной инженерии – немедленно докладывать Ответственному за организацию обработки персональных данных, инициировать проведение служебной проверки (при нарушениях со стороны Ответственного за организацию обработки персональных данных докладывать необходимо непосредственно вышестоящему руководству), регистрировать в «Журнале учёта инцидентов информационной безопасности».

4.1.23. Не реже 1 раза в месяц просматривать журналы учёта и регистрации событий СЗИ на предмет выявления подключения неучтённых носителей, попыток НСД и т.п.

4.1.24. Требовать от пользователей ИСПДн и выполнять самому порядок пропускного и внутриобъектового режима в здании.

4.1.25. Контролировать отсутствие в составе ПО АРМ, входящих в ИСПДн, средств разработки и отладки программ.

4.1.26. Реагировать на поступление в ИСПДн спама (в случае присутствия данной информации в журналах событий межсетевого экрана) путем блокирования атакующего хоста.

4.1.27. Выполнять мероприятия по периодическому резервному копированию защищаемой информации в соответствии с «Инструкцией по организации резервного копирования и восстановления информации»;

4.1.28. Знать эксплуатационную документацию на применяемые СЗИ. Устанавливать и эксплуатировать СЗИ в соответствии с документацией;

4.1.29. Хранить документацию и дистрибутивы СЗИ в соответствии с техническими условиями. Компакт-диск с программным обеспечением системы должен упаковываться согласно требованиям, предусмотренным для оптических носителей;

4.1.30. Поддерживать настройки СЗИ, соответствующие требованиям нормативных документов по безопасности информации и протоколу аттестационных испытаний, при этом система должна реализовывать в совокупности на каждой АРМ ИСПДн функции необходимые для выполнения требований по защите от НСД для ИСПДн;

4.1.31. Контролировать срок действия сертификатов соответствия на СЗИ и обеспечить их продление в соответствии с порядком продления, приведённым ниже.

4.1.32. Контролировать заведение, активацию, блокирование и уничтожение учетных записей пользователей;

4.1.33. Пересматривать и, при необходимости, корректировать учетные записи пользователей не менее одного раза в 90 дней;

4.1.34. Контролировать порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;

4.1.35. Уничтожать временные учетные записи пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе персональных данных;

4.1.36. Предоставлять пользователям права доступа к объектам доступа информационной системы персональных данных, основываясь на задачах, решаемых пользователями в информационной системе персональных данных и взаимодействующими с ней.

4.2. Администратор безопасности оказывает методическую помощь и контролирует выполнение руководителем подразделения, эксплуатирующего ИСПДн следующих действий:

- При смене пользователя руководитель подразделения, эксплуатирующего ИС, инициирует внесение изменений в перечень лиц, допущенных к работе в данной ИС и в разрешительную систему доступа;

- При исключении пользователя ИСПДн из «Перечня лиц, имеющих право доступа к обработке персональных данных, содержащихся в информационных системах персональных данных руководителем подразделения, эксплуатирующего ИСПДн, принимаются меры по исключению возможности нарушения данным пользователем характеристик безопасности информации ИС. Администратору информационной безопасности необходимо до момента доведения до сотрудника информации о прекращении его работы в ИСПДн, лишить сотрудника возможности доступа к защищаемой информации.

4.3. Администратору безопасности запрещается:

4.3.1. Фиксировать учетные данные пользователя (пароли, идентификаторы, ключи и др.) на твердых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя;

4.3.2. Раскрывать информацию об организации СЗПДн ИСПДн и любую информацию, которая может создать предпосылки для возникновения канала утечки информации или создания угрозы безопасности информации.

5. Права Администратора безопасности

5.1. Требовать от пользователей ИСПДн соблюдения установленных технологий обработки информации, выполнения нормативно-методических

документов в области безопасности информации и организационно-распорядительных документов на ИСПДн;

5.2. Давать своему непосредственному начальнику свои предложения по совершенствованию мер защиты в ИСПДн.

6. Ответственность

6.1. Администратор безопасности несет ответственность по действующему законодательству за разглашение сведений ограниченного распространения, ставших известными ему по роду деятельности.

6.2. Ответственность за защиту ИСПДн от несанкционированного доступа к информации и за неукоснительное соблюдение положений настоящего руководства возлагается на Администратора безопасности.

7. Порядок использования съемных и машинных носителей информации

Под использованием съемных носителей информации в ИСПДн понимается их подключение к АРМ с целью обработки, приема/передачи информации между АРМ и носителями информации.

В ИСПДн допускается использование только учтенных съемных носителей информации, которые являются собственностью Инспекции Гостехнадзора РК и подвергаются регулярной ревизии и контролю.

Съемные носители информации предоставляются пользователю ИСПДн по инициативе руководителя структурного подразделения, в котором он числится, в случае:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника Инспекции Гостехнадзора РК производственной необходимости.

8. Порядок учета, хранения и обращения со съемными и машинными носителями, твердыми копиями и их утилизации

Все находящиеся на хранении и в обращении в ИСПДн съемные и машинные носители подлежат учёту.

Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера. Учет съемных машинных носителей персональных данных ведется в «Журнале учета съемных машинных носителей персональных данных».

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

Для получения электронного внешнего носителя, для использования в ИСПДн, пользователь обращается к непосредственному руководителю, руководитель пишет служебную записку на имя Ответственного за организацию

обработки персональных данных о выдаче пользователю съемного электронного носителя, далее Ответственный за организацию обработки персональных данных принимает решение и передает служебную записку Администратору безопасности.

Учет и выдачу съемных носителей для использования в ИСПДн осуществляет Администратор безопасности, на которого возложена эта функция. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

При использовании сотрудниками съемных носителей информации необходимо:

- соблюдать требования настоящей Инструкции;
- использовать носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность Администратора безопасности о любых фактах нарушения требований настоящей Инструкции;
- бережно относится к носителям информации;
- извещать Администратора безопасности о фактах утраты (кражи) носителей информации.

При использовании носителей конфиденциальной информации запрещено:

- использовать носители конфиденциальной информации в личных целях;
- передавать носители конфиденциальной информации другим лицам (за исключением Администратора безопасности);
- хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с конфиденциальной информацией (персональными данными) за пределы контролируемой зоны для работы с ними на дому и т. д.

Любое взаимодействие (обработка, прием/передача информации) инициированное пользователем ИСПДн между АРМ и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с Администратором безопасности). Администратор безопасности оставляет за собой право блокировать или ограничивать использование носителей информации.

В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется Начальником Инспекции Гостехнадзора РК.

По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Инспекции Гостехнадзора РК и действующему законодательству.

Информация, хранящаяся на съемных носителях, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журнал учета съемных носителей конфиденциальной информации (персональных данных).

Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение таких съемных носителей с конфиденциальной информацией осуществляется администратором информационной безопасности после сдачи пользователями, с отметкой в журнале.

В случае увольнения или перевода работника в другое структурное подразделение предоставленные носители конфиденциальной информации сдаются Администратору безопасности.

9. Установка и обновление программного обеспечения

Установка или обновление подсистем ИСПДн должны проводиться уполномоченными сотрудниками (администраторы сети (серверов) и администраторы баз данных) обязательно по согласованию с Администратором безопасности. После установки модифицированных модулей на сервер (рабочую станцию) администратор информационной безопасности проводит антивирусный контроль.

Установка и обновление общего программного обеспечения (системного, тестового и т.п.) на рабочие станции и сервера производится с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком.

Факты установки или обновления фиксируются в «Журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств ИСПДн».

Приложение № 7
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 20_г. №13/08

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных

1. Обозначения и сокращения

АРМ – автоматизированное рабочее место;

ИСПДн – информационная система персональных данных;

ИБ – информационная безопасность;

ЗИ – защита информации;

ОТСС – основные технические средства и системы;

ПДн – персональные данные;

ПЭВМ – персональная электронно-вычислительная машина;

СВТ – средства вычислительной техники;

СЗИ – средства защиты информации;

СЗПДн – система (подсистема) защиты персональных данных;

УБПДн – угрозы безопасности персональным данным;

НСД – не санкционированный доступ.

2. Общие положения

2.1. Инструкция пользователя (далее Инструкция) ИС предназначена для пользователей всех уровней (руководителей и сотрудников) и регулирует порядок работы пользователей в ИСПДн, определяет общие обязанности, права и ответственность по обеспечению информационной безопасности при работе в ИСПДн.

2.2. Пользователем ИСПДн (далее Пользователь) является сотрудник Инспекции Гостехнадзора РК, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, в соответствии с перечнем лиц, допущенных к ИСПДн. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

2.3. Положения Инструкции обязательны для исполнения всеми пользователями.

2.4. Все пользователи должны быть ознакомлены под расписку с Инструкцией и предупреждены об ответственности за её нарушение.

2.5. По уровню ответственности и правам доступа к ИС пользователи разделяются на следующие категории: администратор информационной безопасности и пользователи.

3. Основные положения Инструкции

3.1. При первичном допуске к работе в ИСПДн Пользователь изучает требования настоящей инструкции, разрешительную систему доступа к ИСПДн, и руководящие, нормативно-методические и организационно-распорядительные документы по вопросам обеспечения безопасности информации.

3.2. Каждый пользователь ИСПДн, имеющий в рамках своих обязанностей доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн, в том числе положения настоящей Инструкции;

– знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции;

– располагать ОТСС в соответствии с техническим паспортом;

– хранить в тайне свой пароль (пароли). Парольную защиту организовывать в соответствии с Инструкцией по организации парольной защиты;

– выполнять требования Инструкции по проведению антивирусного контроля;

– немедленно вызывать администратора информационной безопасности и ставить в известность руководителя подразделения при подозрении компрометации личных ключей и паролей или при обнаружении фактов совершения в его отсутствие попыток НСД к ОТСС ИСПДн;

– в случае появления у пользователя сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах или попытках несанкционированного удаленного доступа к информации, размещенной на контролируемом в ИСПДн компьютере, пользователь должен немедленно сообщить об этом администратору информационной безопасности;

– немедленно сообщать администратору информационной безопасности об обнаруженных фактах нарушения настоящей Инструкции кем-либо;

– сообщать администратору информационной безопасности об отклонениях в нормальной работе установленных на АРМ средств защиты информации;

– при работе в ИСПДн выполнять только служебные задания;

– при отсутствии необходимости работы выключить компьютер;

– при работе в ИСПДн использовать только учтенные съемные носители, при обоснованной необходимости использования неучтённых носителей согласовывать использование с администратором информационной безопасности. После того как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.) информация незамедлительно удаляется с носителей;

– осуществлять установленным порядком уничтожение информации (сочетанием клавиш Shift+Del), содержащей сведения конфиденциального характера, с машинных (съемных) носителей информации;

– немедленно выполнять предписания администратора информационной безопасности в части обеспечения безопасности информации;

– экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;

– соблюдать установленный режим разграничения доступа к информационным ресурсам;

– не разглашать известную им информацию, составляющую ПДн лицам, не имеющим допуска к этой информации;

– все изменения конфигурации технических и программных средств ИСПДн, ремонт, модификация и техническое обслуживание технических средств и систем, входящих в состав ИСПДн производить только на основании инструкции по модернизации, ремонту, техобслуживанию;

Пользователю запрещается:

– Какие-либо действия до прохождения процедур идентификации и аутентификации;

– самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств, устанавливать или удалять установленные техническим специалистом (администратором информационной безопасности) сетевые программы на компьютерах, вскрывать компьютеры, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование, вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства без согласования с администратором информационной безопасности;

– привлекать посторонних лиц для производства ремонта ОТСС без письменной заявки и согласования с администратором информационной безопасности;

– запускать любые системные или прикладные программы, не входящие в состав программного обеспечения;

– работать с неучтенными машинными (съемными) носителями информации;

– отключать (блокировать) средства защиты информации;

– производить какие-либо изменения в размещении технических средств;

– обрабатывать на СВТ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам;

– сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам АРМ;

– хранить на учтенных носителях программы и данные, не относящиеся к рабочей информации;

– выполнять работы с документами ограниченного распространения на дому, выносить их за пределы контролируемой зоны;

– передавать свои учтённые носители кому-либо;

– вводить в ОТСС персональные данные под диктовку или с микрофона;

– осуществлять попытки несанкционированного доступа к ресурсам ИСПДн, проводить или участвовать в сетевых атаках и сетевом взломе;

– производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и серверов;

– закрывать доступ к информации паролями без согласования с администратором информационной безопасности;

– оставлять без личного присмотра на рабочем месте или где бы то ни было персональное устройство идентификации, машинные (съемные) носители и распечатки, содержащие защищаемую информацию;

3.3. Пользователь обязан обеспечить:

– блокирование своей учетной записи в случае кратковременного оставления АРМ (нажатием клавиш Windows+L);

– обязательное выключение компьютера после завершения работы;

3.4. Права пользователя:

– участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн, если данное нарушение произошло под его идентификационными данными;

– своевременно получать доступ к информационным ресурсам ИСПДн, необходимым ему для выполнения своих должностных обязанностей;

– требовать от администратора информационной безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

3.5. Ответственность:

3.5.1. Пользователь несет персональную ответственность за соблюдение установленных требований во время работы. Пользователи, виновные в нарушении законодательства Российской Федерации о защите прав собственности и охраняемых по Закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно-распорядительными документами;

3.5.2. Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники;

3.5.3. Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей или

ИСПДн в целом, может повлечь ответственность в соответствии с действующим законодательством.

4. Порядок использования съемных носителей информации

4.1. Под использованием съемных носителей информации в ИСПДн понимается их подключение к АРМ с целью обработки, приема/передачи информации между АРМ и носителями информации.

4.2. В ИСПДн допускается использование только учтенных съемных носителей информации, которые являются собственностью Инспекции Гостехнадзора РК и подвергаются регулярной ревизии и контролю.

4.3. Съемные носители информации предоставляются пользователям ИСПДн по инициативе руководителей структурных подразделений в случаях:

– необходимости выполнения вновь принятым работником своих должностных обязанностей;

– возникновения у сотрудника Инспекции Гостехнадзора РК производственной необходимости.

5. Порядок учета, хранения и обращения со съемными носителями, твердыми копиями и их утилизации

5.1. Все находящиеся на хранении и в обращении съемные носители в ИСПДн подлежат учёту.

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

5.3. Для получения электронного внешнего носителя, пользователь обращается к руководителю структурного подразделения, руководитель структурного подразделения пишет служебную записку на имя ответственного за организацию обработки персональных данных о выдаче пользователю внешнего электронного носителя, далее ответственный за организацию обработки персональных данных принимает решение и передает служебную записку администратору информационной безопасности.

5.4. Учет и выдачу съемных носителей осуществляет администратор информационной безопасности, на которого возложена эта функция. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

5.5. При использовании сотрудниками съемных носителей информации необходимо:

– соблюдать требования настоящей Инструкции;

– использовать носители информации исключительно для выполнения своих служебных обязанностей;

– ставить в известность администратора информационной безопасности о любых фактах нарушения требований настоящей Инструкции;

– бережно относиться к носителям информации;

– извещать администратора информационной безопасности о фактах утраты (кражи) носителей информации;

– при использовании носителей конфиденциальной информации запрещено:

– использовать носители конфиденциальной информации в личных целях;

– передавать носители конфиденциальной информации другим лицам (за исключением администратора информационной безопасности);

– хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

– выносить съемные носители с конфиденциальной информацией (персональными данными) за пределы контролируемой зоны для работы с ними на дому и т. д.

5.6. Любое взаимодействие (обработка, прием/передача информации), инициированное пользователем ИСПДн между АРМ и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администратором информационной безопасности). Администратор информационной безопасности оставляет за собой право блокировать или ограничивать использование носителей информации.

5.7. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется ответственным за организацию обработки персональных данных.

5.8. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Инспекции Гостехнадзора РК и действующему законодательству.

5.9. Информация, хранящаяся на съемных носителях, подлежит обязательной проверке на отсутствие вредоносного ПО.

5.10. В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

5.11. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение таких съемных носителей с конфиденциальной информацией осуществляется администратором информационной безопасности после сдачи пользователями, с отметкой в журнале.

5.12. В случае увольнения или перевода работника в другое структурное подразделение предоставленные носители конфиденциальной информации сдаются администратору информационной безопасности.

6. Правила работы в сетях общего доступа

Работа в сетях общего доступа (далее – Сеть) на элементах ИСПДн должна проводиться при служебной необходимости.

При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств защиты каналов связи;
- нецелевое использование подключения к Сети.

Приложение № 8
Утверждено
приказом Инспекции
Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

Типовое обязательство
государственного гражданского служащего Инспекции Гостехнадзора РК, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я,_____
(фамилия, имя, отчество)
_____
(должность)
_____
обязуюсь прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта.

В соответствии со статьей 7 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

О характере обработки, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки уведомлен (а).

Ответственность, предусмотренная законодательством Российской Федерации, мне разъяснена.

«__»_____20__г. _____ _____
(подпись) (расшифровка подписи)

Приложение № 9
Утверждено
приказом Инспекции
Гостехнадзора РК
от «03» 02 2022г. № 13/ОД

Типовая форма
согласия на обработку персональных данных заявителей при их обращении в Инспекцию Гостехнадзора РК

В соответствии с Федеральным законом от 27.07.2006г. №152-ФЗ «О персональных данных»

Я, _____
(фамилия, имя, отчество заявителя)
Зарегистрированный (ная) по адресу: _____
_____
Паспорт серии _____№ _____выдан_____
(дата, кем выдан)
_____ свободно, своей волею и в своем интересе даю свое согласие на обработку, хранение и предоставление моих персональных данных третьим лицам Инспекции Гостехнадзора РК в целях осуществления деятельности, предусмотренной Положением, при предоставлении государственной услуги по _____
(указать государственную услугу)

_____ _____ _____
(число, месяц, год) (подпись) (фамилия, инициалы)

Приложение № 10
Утверждено
приказом Инспекции
Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

Типовая форма
согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения при их обращении в Инспекцию Гостехнадзора РК

В соответствии со статьей 9 Федерального закона от 27 июля 2006 г. N152-ФЗ «О персональных данных»
Я, _____
(фамилия, имя, отчество заявителя)
даю свое согласие _____
(полное наименование оператора получающего согласие субъекта
_____
персональных данных)
на распространение (передачу, предоставление) своих персональных данных посредством _____
(указать сведения об информационных ресурсах оператора (адрес, состоящий из наименования протокола (httpили https), сервера (www), домена, имени каталога на сервере, и имя файла веб-страницы), посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных)_____
_____
с целью_____
(сформулировать цель (цели) обработки персональных данных)

Категории и перечень персональных данных, на обработку которых дает согласие:

№ п/п	Персональные данные	Согласие	
		ДА	НЕТ
	1. Общие персональные данные		
	Фамилия		
	Имя		
	Отчество (при наличии)		
	Год, месяц, дата и место рождения		
	Адрес		
	Семейное положение		
	Социальное положение		
	Имущественное положение		
	Образование		

	Профессия		
	Доходы		
	Другая информация относящаяся к субъекту персональных данных		
	2. Специальные категории персональных данных 3.		
	Расовая принадлежность		
	Национальная принадлежность		
	Политические взгляды		
	Религиозные убеждения		
	Философские убеждения		
	Состояние здоровья		
	Состояние интимной жизни		
	Сведения о судимости		
	3. Биометрические персональные данные		
	ДНК		
	Радужная оболочка глаз		
	Дактилоскопическая информация		
	Цветное цифровое фотографическое изображение лица		
	Голос		
	Фотоизображение рисунка вен ладони, полученного в диапазоне, близком к инфракрасному		
	Иные сведения		

Категории и перечень персональных данных, для обработки которых устанавливаются условия и запреты:

№ п/п		**устанавливаемые условия и запреты**
	Категория персональных данных	
	Перечень персональных данных	

Настоящее согласие действует _____

_____ _____ _____

(число, месяц, год) (подпись) (фамилия, инициалы)

Приложение № 11
Утверждено
приказом Инспекции
Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

Типовая форма
согласия на обработку персональных данных государственных служащих Инспекции Гостехнадзора РК, а также иных субъектов персональных данных

г. Симферополь «__»_____20__г.

Я, _____
(Ф.И.О.)
зарегистрированный (ная) по адресу: _____
_____
Паспорт серия _____№_____,выдан_____
_____,
(дата)
_____
(дата, кем выдан)

свободно, своей волей и в своем интересе даю согласие уполномоченным должностным лицам Инспекции Гостехнадзора РК, зарегистрированного по адресу: ул. Кечкеметская, 198, г. Симферополь, Республика Крым, 295022, 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, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) следующих персональных данных: фамилия, имя, отчество, дата и место рождения, гражданство; прежние фамилия, имя, отчество, дата, место и причина их изменения (в случае изменения);

владение иностранными языками и языками народов Российской Федерации: образование (когда и какие образовательные, научные и иные организации 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 и т.п.);

классный чин федеральной государственной гражданской службы Российской Федерации и (или) государственной 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 (кем награжден и когда);

степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);

места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);

фамилии, имена, отчества, даты рождения, места рождения, места работы и домашние адреса бывших мужей (жен);

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, с какого времени проживают за границей); адрес регистрации и фактического проживания; дата регистрации по месту жительства; паспорт (серия, номер, когда и кем выдан);

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

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 Республики Крым или ее прохождению, подтвержденного заключением медицинского учреждения;

результаты обязательных медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования;

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

сведения о расходах и об источниках получения средств, за счет которых совершены сделки, а также о расходах и об источниках получения средств, за счет которых совершены сделки членов семьи;

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 законодательства Республики Крым в сфере отношений, связанных с поступлением на государственную гражданскую службу Республики Крым, ее

прохождением и прекращением (трудовых и непосредственно связанных с ними отношений) для реализации полномочий, возложенных на Инспекцию Гостехнадзора РК действующим законодательством.

Я ознакомлен(а) с тем, что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока прохождения государственнойгражданской службы Российской Федерации в Инспекции Гостехнадзора РК;

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, Инспекция Гостехнадзора РК вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 6,9, 10, 11 части 1 статьи 6, пунктах 2, 3, 7, 8, 10 части 2 статьи 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

4) после увольнения с государственной гражданской службы (прекращения трудовых отношений) персональные данные будут храниться в Инспекции Гостехнадзора РК в течение срока хранения документов, предусмотренного действующим законодательством Российской Федерации;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения, возложенных законодательством Российской Федерации на Инспекцию Гостехнадзора РК функций, полномочий и обязанностей.

Дата начала обработки персональных данных:

_____	_____	_____
(число, месяц, год)	(подпись)	(фамилия, инициалы)

Приложение № 12
Утверждено
приказом Инспекции
Гостехнадзора РК
от «03» 02 2022 г. № 13/02

Типовая форма разъяснения
субъекту персональных данных юридических последствий отказа
предоставить свои персональные данные

Мне, _____
(фамилия, имя, отчество)
зарегистрирован (а) по адресу _____ .
Паспорт серии _____ № _____ выдан _____

разъяснены юридические последствия отказа предоставить свои персональные данные уполномоченным лицам Инспекции Гостехнадзора РК.

В соответствии со статьей 42 Федерального закона от 27 июля 2004 года № 79-ФЗ "О государственной гражданской службе Российской Федерации", Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденным Указом Президента Российской Федерации от 30 мая 2005 года № 609, Инспекцией по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым определен перечень персональных данных, которые субъект персональных данных обязан представить уполномоченным лицам Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым в связи с поступлением на государственную гражданскую службу Республики Крым, ее прохождением и увольнением с государственной гражданской службы Республики Крым.

_____ _____
(дата) (подпись)

Приложение № 13
Утверждено
приказом Инспекции
Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

Порядок
доступа государственных гражданских служащих Инспекции Гостехнадзора РК в помещения, в которых ведется обработка персональных данных

1. Порядок доступа государственных гражданских служащих Инспекции Гостехнадзора РК в помещения, в которых ведется обработка персональных данных (далее - Порядок) устанавливает единые требования к доступу государственных гражданских служащих Инспекции Гостехнадзора РК (далее - гражданские служащие) в служебные помещения, в которых ведется обработка персональных данных, в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в Инспекции Гостехнадзора РК, и обеспечения соблюдения требований законодательства о персональных данных.

2. Доступ в помещения Инспекции Гостехнадзора РК, в которых ведется обработка персональных данных, имеют лица, включенные в Перечень должностей государственной гражданской службы в Инспекции Гостехнадзора РК, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, утверждаемый приказом начальника Инспекции Гостехнадзора РК (далее - Перечень).

3. Нахождение в помещениях, в которых ведется обработка или хранение персональных данных, лиц, не являющихся гражданскими служащими, замещающими должности государственной гражданской службы в Инспекции Гостехнадзора РК (далее - должности гражданской службы), включенные в Перечень, возможно только в сопровождении гражданского служащего, замещающего должность гражданской службы, включенную в Перечень.

4. Для помещений, в которых хранятся и обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащих персональные данные, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Данный режим должен обеспечиваться, в том числе:

запиранием помещения на ключ, в том числе при выходе из него в рабочее время;

закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие персональные данные, во время отсутствия в помещении гражданских служащих, замещающих должности гражданской службы, включенные в Перечень.

5. Лицу, ответственному за организацию обработки персональных данных, а также гражданским служащим, осуществляющим обработку персональных данных,

запрещается передавать ключи от служебных помещений и печати для опечатывания служебных помещений третьим лицам.

6. Внутренний контроль за соблюдением в Инспекции Гостехнадзора РК настоящего Порядка и требований к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных.

Приложение № 14
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/08

Положение
об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации

I. Общие положения

1.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее материальные носители), в специальных разделах или на полях форм (бланков).

2.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.3. Государственные гражданские служащие Инспекции Гостехнадзора РК (далее - гражданские служащие), осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

2.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Инспекции Гостехнадзора РК (далее - Инспекция), фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Инспекцией способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

2.5. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных па территорию, па которой находится Инспекция, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Инспекции, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждою субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится Инспекция.

2.6. При несовместимости целей обработки персональных данных, зафиксированных па одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в

частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

2.7. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

2.8. Правила, предусмотренные пунктами 2.6 и 2.7 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

2.9. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

III. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень гражданских служащих, осуществляющих обработку персональных данных либо имеющих к ним доступ.

3.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Инспекцией.

Приложение № 15
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2021 г. №13/ОД

ПЕРЕЧЕНЬ
информационных систем персональных данных, в которых осуществляется обработка персональных данных в Инспекции Гостехнадзора РК

№ п/п	Наименование ИСПДн	Место расположения ИСПДн	Структура	Категория субъектов ПДн	Цели обработки
1	«Автоматизированная информационная система управления органами гостехнадзора»	295022, Республика Крым, г. Симферополь, ул. Кечкеметская, д. 198	Комплекс автоматизированных рабочих мест;	Субъекты, являющиеся и не являющиеся сотрудниками оператора	Персональные данные в ИСПДн«Автоматизированная информационная система управления органами гостехнадзора» обрабатываются в целях ведения учета, регистрации, постановки и снятия с учета самоходной и аттракционной техники.
2	«Экзаменационный класс» Спектр ПДД	295022, Республика Крым, г. Симферополь, ул. Кечкеметская, д. 198	Комплекс автоматизированных рабочих мест	Субъекты, не являющиеся сотрудниками оператора	Персональные данные в ИСПДн «Экзаменационный класс» обрабатываются с целью приема экзаменов на право управления самоходными машинами и выдачу удостоверения тракториста-машиниста (тракториста).
3	Кадры	295022, Республика Крым, г. Симферополь, ул. Кечкеметская, д. 198	Комплекс автоматизированных рабочих мест	Субъекты, являющиеся сотрудниками оператора	Персональные данные в ИСПДн «Кадры» обрабатываются в целях ведения кадрового учета сотрудников Инспекции Гостехнадзора РК, ведения учета внутренних приказов

					Инспекции Гостехнадзора РК, передачи личных дел сотрудников, устроившемся на другую Госслужбу, составление вакансий приема на работу.
4	«Бухгалтерия»	295022, Республика Крым, г. Симферополь, ул. Кечкеметская, д. 198	Комплекс автоматизированных рабочих мест	Субъекты, являющиеся сотрудниками оператора	Персональные данные в ИСПДн «Бухгалтерия» обрабатываются в целях начисления и выплаты заработной платы и иных выплат, установленных законодательством Российской Федерации и внутренними локальными нормативными актами;обеспечения соблюдения законных прав субъектов персональных данных, и исполнения обязанностей, установленных Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации и иными нормативно-правовыми и внутренними локальными нормативными актами;обеспечения управленческой деятельности.
5	«Обращения граждан и документооборот»	295022, Республика Крым, г. Симферополь, ул. Кечкеметская, д. 198	Комплекс автоматизированных рабочих мест	Субъекты, являющиеся и не являющиеся сотрудниками оператора	Персональные данные в ИСПДн «Обращения граждан и документооборот» обрабатываются в целях предоставления отчетов по обращениям граждан в Инспекцию Гостехнадзора РК;

					межведомственное с органами власти.

Приложение № 16
Утверждено
приказом Инспекции
Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

ПЕРЕЧЕНЬ
персональных данных, подлежащих защите

В ИСПДн «Автоматизированная информационная система управления органами гостехнадзора»» Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым обрабатываются следующие персональные данные субъектов персональных данных:

Персональные данные физического лица:

- фамилия, имя, отчество;
- дата рождения;
- пол;
- ИНН;
- место рождения;
- место жительства;
- фактический адрес проживания;
- данные водительского удостоверения;
- ОКТМО;
- данные документа удостоверяющего личность;
- контактные данные;
- фамилия, имя, отчество законного представителя;
- данные документа удостоверяющего личность законного представителя;
- сведения о транспортном средстве.

Персональные данные юридического лица:

- тип организации;
- наименование организации;
- ИНН;
- ОГРН;
- КПП;
- КПП доп.;
- место регистрации;
- дата регистрации;
- фактический адрес;
- ОКТМО;
- ОКОПФ;
- контактные данные (телефон, факс, эл. почта);
- фамилия, имя, отчество доверенного лица;

- данные документа удостоверяющего личность доверенного лица;
- данные документа подтверждающего полномочия;
- сведения о транспортном средстве.

В ИСПДн «Экзаменационный класс» Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым обрабатываются следующие персональные данные субъектов персональных данных:

Персональные данные получателей услуг:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- СНИЛС;
- гражданство;
- данные документа удостоверяющего личность;
- место работы;
- контактные данные;
- данные водительского удостоверения.

В ИСПДн «Кадры» Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым обрабатываются следующие персональные данные субъектов персональных данных:

Персональные данные работников Инспекции Гостехнадзора РК:

- фамилия, имя, отчество;
- дата рождения,
- место рождения;
- данные документов удостоверяющих личность;
- сведения об образовании;
- сведения о трудовой деятельности;
- сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;
- сведения о допуске к государственной тайне;
- сведения о воинском учете;
- сведения о близких родственниках;
- сведения о назначении и освобождении от должности;
- сведения о служебном контракте/трудовом договоре;
- сведения о денежном содержании;
- сведения о материальном стимулировании и социальной поддержки;
- сведения о графике рабочего времени;
- сведения отклонений от графика рабочего времени;
- сведения о чинах и званиях;
- стаж работы;

- участие в кадровом резерве;
- сведения об отпусках;
- сведения о взысканиях;
- сведения о листах нетрудоспособности;
- сведения о пенсионном обеспечении;
- сведения об инвалидности;
- сведения о социальных льготах;
- сведения об аттестации;
- сведения о командировках;
- сведения о наградах и поощрениях.

В ИСПДн «Бухгалтерия» Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым обрабатываются следующие персональные данные субъектов персональных данных:

Персональные данные работников Инспекции Гостехнадзора РК:

- фамилия, имя, отчество;
- пол;
- гражданство;
- паспортные данные (номер и серия паспорта, дата выдачи, код и наименование органа выдавшего паспорт);
- дата рождения;
- место рождения;
- адрес по месту регистрации;
- адрес места жительства;
- контактный телефон;
- адрес электронной почты;
- номер полиса обязательного медицинского страхования;
- идентификационный номер налогоплательщика (ИНН);
- страховой номер индивидуального лицевого счета (СНИЛС);
- сведения об образовании, в том числе данные об образовательных организациях и о документах об образовании и (или) о квалификации;
- сведения о банковских счетах;
- сведения о семейном положении и о составе семьи;
- социальные льготы;
- сведения о трудовой деятельности;
- сведения о повышении квалификации;
- классный чин;
- занимаемая должность;
- род занятий;
- стаж работы;
- стаж муниципальной службы;
- сведения о заработной плате;

- сведения о доходах, расходах, имуществе и обязательствах имущественного характера;
- сведения о денежных средствах, находящихся на счетах в банках или иных кредитных организациях;
- сведения о ценных бумагах;
- номер расчетного счета в банке и сумма начислений; сведения о временной нетрудоспособности;
- сведения об отпусках;
- сведения о больничных листах;
- сведения налогового статуса.

В ИСПДн «Обращения граждан и документооборот» Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым обрабатываются следующие персональные данные субъектов персональных данных:

Персональные данные лица, подавшего обращение:

- фамилия, имя, отчество;
- социальное положение;
- контактные данные;
- сведения о почтовом адресе для ответа.

.

Приложение № 17
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2024 г. № 19/ОД

(ФОРМА)
Акт

определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных в Инспекции Гостехнадзора РК

Комиссия в составе:

_____ – _____, председатель комиссии;
_____ – _____, член комиссии;
_____ – _____, член комиссии;

рассмотрев исходные данные в информационной системе персональных данных *«Наименование* ИСПДн» в соответствии с Постановлением Правительства Российской Федерации №1119 от 1 ноября 2012г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» определила:

1. Категории персональных данных (далее – ПДн), обрабатываемых в информационной системе персональных данных: специальные категории персональных данных;
2. Объем обрабатываемых ПДн: менее 100 000;
3. Угрозы, актуальные для ИСПДн: актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн, т.е. угрозы 3-го типа;
4. Тип субъектов ПДн, обрабатываемых в ИСПДн: субъекты ПДн, являющиеся и не являющиеся сотрудниками оператора.

Вывод: по результатам анализа исходных данных в информационной системе персональных данных в Инспекции Гостехнадзора РК требуется обеспечение __ уровня защищенности персональных данных.

Председатель комиссии: _____

Члены комиссии: _____

_____

Приложение № 18
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

ИНСТРУКЦИЯ
по организации антивирусной защиты

1. Термины и определения

Вирус - программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области автоматизированного рабочего места (АРМ), компьютерные сети, а также осуществлять иные деструктивные воздействия. При этом копии сохраняют способность дальнейшего распространения.

Владелец информации – сотрудник Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым, в непосредственном ведении которого, в соответствии с действующим законодательством и/или документами распорядительного характера находится информация, использование которой осуществляется посредством организации доступа к информационным системам персональных данных Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым.

Информационная система персональных данных (ИСПДн) - взаимосвязанная совокупность программного, аппаратного и организационного обеспечения, предназначенная для автоматической и/или автоматизированной обработки информации.

Сетевой ресурс (СР) - совокупность информации, хранящейся на АРМ, доступ к которому может быть осуществлён удалённо с другого компьютера через локальную компьютерную сеть.

Сетевой сервис (СС) - сетевое программное обеспечение, предоставляющее определенные услуги по обработке информации и взаимодействующее с распределенными клиентскими приложениями через свой внешний интерфейс.

Инцидент информационной безопасности (инцидент ИБ) - любое событие (случайное или преднамеренное), указывающее на свершившееся, предпринимаемое или вероятное нарушение политик или регламентов информационной безопасности Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым, которое может привести к потере или изменению информации, блокировке доступа авторизованных пользователей, разглашению, несанкционированному доступу к информации или информационным системам.

Пользователь ИСПДн, СС, СР - лицо, участвующее в функционировании ИСПДн, СС, СР или использующее результаты ее

функционирования.

Роль - именованный набор функций и полномочий, однозначно определяющий совокупность прав доступа к различным блокам информации и функциям информационных систем.

Средство антивирусной защиты (САВЗ) - программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Троян - вредоносная программа, маскирующаяся под безвредные или полезные программы, для установки пользователем на АРМ.

Удаленный доступ - доступ к ИСПДн, СС, СР с рабочих мест или локальной вычислительной сети, не подключенных непосредственно к локальной вычислительной сети Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым, осуществляемый с использованием телефонной сети или иных общедоступных и/или выделенных каналов и/или сетей связи.

2. Общие положения

2.1. Настоящая Инструкция по организации антивирусной защиты (далее – Инструкция) устанавливает единые для Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым требования по обеспечению антивирусной защиты ИСПДн, СР и СС Инспекции Гостехнадзора РК.

2.2.Настоящая Инструкция является обязательной для исполнения всеми сотрудниками Инспекции Гостехнадзора РК, включая пользователей сторонних организаций и агентов, использующих в работе средства электронно-вычислительной техники Инспекции Гостехнадзора РК.

2.3. Основное назначение настоящей Инструкции заключается в формализации механизмов предотвращения вирусных эпидемий и связанных с ними угроз информационной безопасности в Инспекции Гостехнадзора РК Настоящая Инструкция предназначена для обеспечения:

- целостности, надежности и надлежащей производительности вычислительных ресурсов Инспекции Гостехнадзора РК;
- максимальной безопасности методов взаимодействия пользователей и ресурсов;
- соответствующих мер, позволяющих обоснованно гарантировать соблюдение требований данной Инструкции.

2.4. В САВЗ должны быть реализованы следующие функции безопасности:

- разграничение доступа к управлению САВЗ;
- управление работой САВЗ;

- управление параметрами САВЗ;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ) САВЗ;
- аудит безопасности САВЗ;
- сигнализация САВЗ.

2.5. Состав функциональных требований безопасности (ФТБ) обеспечивает следующие функциональные возможности САВЗ:
- отображение сигнала тревоги на автоматизированное рабочее место (АРМ) Администратора безопасности, указывающего на обнаружение КВ на пользовательских автоматизированных рабочих местах;
- получение и установка обновлений БД ПКВ без применения средств автоматизации и в автоматизированном режиме с сетевого ресурса;
- управление Администратором безопасности режимом выполнения функций безопасности САВЗ (обработка зараженных объектов на АРМ и серверах вычислительной сети; выполнение автоматизированного запуска САВЗ на АРМ и серверах вычислительной сети с заданными условиями поиска КВ и режимами реагирования по расписанию; выполнение удаленного администрирования процессов обнаружения КВ, обновления БД ПКВ и компонентов САВЗ);
- возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ;
- поддержка определенных ролей для САВЗ и их ассоциации с конкретными пользователями;
- генерация записи аудита для событий, подвергаемых аудиту;
- чтение информации из записей аудита;
- ассоциация событий аудита с идентификаторами субъектов;
- ограничение доступа к чтению записей аудита;
- поиск, сортировка, упорядочение данных аудита.

2.6. В отношении любого сотрудника, допустившего нарушения требований настоящей Инструкции, могут быть применены дисциплинарные меры наказания.

3. Принципы построения и функционирования антивирусной системы

3.1. Объектами антивирусной защиты являются:
- внешние носители (флэш-карты, дискеты, компакт-диски и др.);
- серверы и автоматизированные рабочие места (далее - АРМ) пользователей в Инспекции Гостехнадзора РК;
- объекты виртуальной инфраструктуры;
- почтовый трафик (на уровне почтового сервера и на уровне почтового клиента), включая почтовые вложения;
- веб-трафик (на уровне Интернет-шлюза и на уровне обозревателя Интернет), включая скачиваемые файлы.

3.2. САВЗ должны быть установлены, настроены и активизированы на всех допускающих такую установку средствах вычислительной техники

(далее - СВТ) до начала их использования для работы с ИСПДнИнспекции Гостехнадзора РК.

3.3. По возможности все обновления должны быть автоматизированными и запланированными (если нет веских причин для иного). Если функции выбранного ПО позволяют инициировать обновление со стороны сервера, то должен быть выбран именно такой механизм обновления.

3.4. САВЗ и базы данных вирусных сигнатур должны поддерживаться в актуальном состоянии. Интервал между обновлениями САВЗ не должен превышать 48 часов.

3.5. Антивирусный контроль всех дисков и файлов рабочих станций и серверов должен проводиться по мере необходимости, но не реже одного раза в две недели.

3.6. САВЗ могут быть интегрированы с другими решениями обеспечения информационной безопасности, в части регистрации и консолидации событий безопасности.

3.7. Контролю на предмет обнаружения вредоносных программ подвергается вся информация, создаваемая и/или обрабатываемая в ИСПДнИнспекции Гостехнадзора РК.

3.8. Антивирусному контролю подлежат все съемные машинные носители информации, которые подключаются к информационно-телекоммуникационным системам, включая компакт-диски, флэш-карты или иные устройства, имеющие в своем составе носители информации.

3.9. Все ПО до установки на СВТ должно быть проверено с помощью САВЗ.

3.10. После установки или изменения состава ПО СВТ должна быть выполнена полная антивирусная проверка.

3.11. С помощью САВЗ производится контроль СВТ на наличие вредоносного кода в режиме реального времени.

3.12. Эффективная антивирусная защита достигается путем комплексного использования организационных мероприятий и программно-технических методов защиты.

4. Меры обеспечения антивирусной безопасности

4.1. Административные меры:

4.1.1. Наличие и своевременное обновление документов, регламентирующих правила и порядок функционирования системы антивирусной защиты Инспекции Гостехнадзора РК, в том числе настоящей Инструкции.

4.1.2. Выполнение сотрудниками Инспекции Гостехнадзора РК требований настоящей Инструкции контролируется Администратором безопасности.

4.2. Процедурные меры

4.2.1. Установка и обслуживание САВЗ на АРМ производится Администратором безопасности.

4.2.2. Администратор безопасности должен составлять регулярные сводки о результатах работы САВЗ.

4.3. Программно-технические меры

4.3.1. Ресурсы централизованного управления САВЗ должны располагаться на отдельном АРМ (АРМ администратора информационной безопасности ИСПДн) и обеспечивать ведение журналов событий.

4.3.2. САВЗ должно осуществлять:

- просмотр в реальном времени каждого поступающего в ИСПДн файла на наличие подозрительных действий;
- сканирование критических компонентов ПО серверов и АРМ (файлы запуска и др.);
- мониторинг поведения приложений (электронная почта, веб-браузеры и др.), которые могут быть использованы для заражения вирусами ИСПДн;
- обнаружение и блокировку проникновения вредоносных программ, а также распознавание их опасного кода (троянский конь, сетевые черви и др.);
- автоматическое уведомление о случаях обнаружения вирусов Администратора безопасности.

4.3.3. САВЗ должно быть совместимо с ОС серверов и АРМ и обеспечивать:

- фильтрацию трафика в разных системах обработки и передачи данных, особенно в точках, где происходит обмен информацией с сетями связи общего пользования Интернет;
- фильтрацию почтовых потоков. На серверах электронной почты должно быть установлено САВЗ, проверяющее всю принимаемую и отправляемую электронную почту на наличие вредоносных программ, обеспечивающее обнаружение и удаление потенциально опасных фрагментов кода.

4.3.4. Антивирусная защита должна обеспечивать выполнение следующих основных функций:

- предоставление сведений для восстановления работоспособности сети и системы защиты в случае, если вредоносная программа все-таки воздействовала на объект связи и информатизации;
- своевременное и быстрое реагирование на появление новых видов угроз;
- регулярный контроль за своевременным обновлением САВЗ;
- архивирование и резервное копирование информации, а также ведение базы данных о вирусах и их характеристиках;
- своевременное оповещение пользователей об обнаруженных вирусах, их признаках и их характеристиках;
- своевременная техническая поддержка пользователей по вопросам антивирусной защиты.

4.3.5. САВЗ должны блокировать проникновение вирусов на АРМ, которое может произойти при помощи:

- инфицированных файлов на съемных носителях информации

(оптических дисках, магнитных дискетах, съемных и USB жестких дисках и т.п.);

- инфицированного ПО и файлов, полученных из глобальных информационных сетей;
- удаленных зараженных серверов или рабочих станций, подключенных к информационной сети Инспекции Гостехнадзора РК;
- зараженных сообщений электронной почты.

5. Характерные проявления вирусов и реагирование на инциденты безопасности

5.1. Обо всех случаях проявления вирусов пользователь обязан немедленно сообщить Администратору безопасности.

5.2. Наиболее характерными проявлениями вирусов являются:

- осыпание различных символов с экрана;
- появление на экране дисплея световых пятен, черных областей или символов, не запланированных рабочими программами;
- самопроизвольная перезагрузка операционной системы;
- замедление работы АРМ;
- зависание АРМ;
- невозможность загрузки операционной системы;
- подача непредусмотренных звуковых сигналов;
- появление неисправных участков (кластеров) на жестком диске;
- неожиданные действия прикладного и специализированного ПО (не предусмотренные документацией на программы);
- искажения данных в обрабатываемых файлах;
- существенное уменьшение размера свободной оперативной памяти;
- неожиданное значительное увеличение количества файлов на диске;
- несанкционированное изменение даты и времени создания файла;
- появление на экране дисплея информации рекламного характера.

6. Ответственность

6.1. Администратор безопасности несет ответственность за:

- организацию программно-технических мер обеспечения антивирусной информационной безопасности ИСПДн Инспекции Гостехнадзора РК;
- разработку эксплуатационной документации и инструкций по антивирусной защите;
- реализацию требований настоящей Инструкции;
- координацию процесса инсталляции и настройки САВЗ на АРМ пользователей сети и серверах;
- построение и поддержку системы оповещения пользователей о вирусных эпидемиях;
- отслеживание состояния САВЗ и инициирование при необходимости соответствующих защитных мер;
- хранение информации о событиях в системе антивирусной защиты,

позволяющей эффективно выполнять анализ этой информации.

- анализ работы системы антивирусной защиты и регулярное составление аналитических отчетов на базе статистической информации;
- контроль своевременного обновления антивирусных баз на объектах, входящих в состав ИСПДн (серверах, рабочих станциях, шлюзах);
- контроль правильности настроек антивирусных пакетов и выполнение пользователями рекомендаций по их применению в процессе работы АРМ;
- контроль сроков действий лицензий установленных САВЗ;
- плановый контроль состояния защиты от вирусов ИСПДн Инспекции Гостехнадзора РК;
- соблюдение требований настоящей Инструкции сотрудниками Инспекции Гостехнадзора РК.

6.2. Все сотрудники Инспекции Гостехнадзора РК несут ответственность за выполнение требований настоящей Инструкции и обязаны:

- не допускать к работе на вверенном им АРМ посторонних лиц;
- не открывать для прочтения почтовые сообщения и вложенные файлы от неизвестных подозрительных отправителей;
- извещать Администратора безопасности о случаях неуспешного лечения, неработоспособности САВЗ на вверенном им АРМ;
- при обнаружении на вверенном им АРМ признаков работы постороннего лица и искажения информации, оставить АРМ без изменений и сообщить Администратору безопасности.

Приложение № 19
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 19/02

ИНСТРУКЦИЯ
по организации парольной защиты

1. Термины и определения

Информационная система персональных данных (ИСПДн) - взаимосвязанная совокупность программного, аппаратного и организационного обеспечения, предназначенная для автоматической и/или автоматизированной обработки персональных данных.

Пароль - идентификатор субъекта доступа, который является его (субъекта) секретом.

2. Общие положения

2.1. Настоящая Инструкция по организации парольной защиты (далее – Инструкция) в информационных системах персональных данныхИнспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым (далее - Инспекция Гостехнадзора РК) определяет порядок использования, генерации, смены и прекращения действия паролей и личных идентификаторов пользователей в Инспекции Гостехнадзора РК, а также контроль действий пользователей при работе с паролями.

2.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль действий пользователей при работе с паролями возлагается на Администратора безопасности.

2.3. Настоящая Инструкция является обязательной для исполнения всеми сотрудниками Инспекции Гостехнадзора РК, включая пользователей сторонних организаций и агентов, использующих в работе средства электронно-вычислительной техники Инспекции Гостехнадзора РК.

2.4. В отношении любого сотрудника, допустившего нарушения требований настоящей Инструкции, могут быть применены дисциплинарные меры наказания.

3. Требования к формированию пароля

3.1 Пароли для всех учетных записей пользователей Инспекции Гостехнадзора РК должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 6 буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования организации и т.д.), а также общепринятые сокращения

(USER, ADM, ADMIN, PASSWORD и т.п.);

- максимальный срок действия пароля - не более 120 дней;
- новый пароль не должен повторять старый;
- при вводе пароля должен иметь значение регистр;
- в состав пароля должна входить минимум одна цифра и одна буква;
- количество попыток неправильного ввода пароля не должно превышать 5 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки Администратором безопасностиИнспекции Гостехнадзора РК.

3.2 Администратор безопасностиИнспекции Гостехнадзора РК должен обеспечить пользователям возможность самостоятельного формирования паролей.

4. Требования к использованию пароля

4.1 При использовании пароля необходимо соблюдать следующие требования:

- при первой авторизации в системе пользователь самостоятельно должен изменить личный пароль;
- по истечении 120 дней со дня последней смены пароль пользователя должен быть изменен;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- повторное использование одного и того же пароля пользователем допускается по истечении 365 дней.

5. Требования к защите пароля

5.1 Пользователи обязаны хранить свой личный пароль втайне от других и не передавать любым способом пароль третьим лицам.

5.2 Запрещается записывать и хранить пароль в форме визуального представления.

5.3 В случае утери пароля, пользователь должен немедленно доложить об этом Администратору безопасности.

5.4 В случае прекращения полномочий учетной записи пользователя ИСПДн (увольнение, переход на другую работу, в другое структурное подразделение или помещение, а также другие обстоятельства) учетная запись должна быть удалена, а её идентификатор должен быть сдан Администратору безопасности после окончания последнего сеанса работы данного пользователя в ИСПДн.

5.5 В случае компрометации личного пароля или утери личного идентификатора пользователя Администратором безопасности должны быть немедленно предприняты меры в соответствии с «Инструкцией Администратора безопасности».

5.6 Внеплановая полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри структурного подразделения и другие обстоятельства) Администратора

безопасности и других сотрудников, которым по роду деятельности могли быть известны пароли других пользователей системы.

5.7 Администратор безопасности должен провести служебное расследование для выяснения причин компрометации пароля с целью выработки новых или совершенствования, принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен в результате компрометации пароля.

5.8 Пользователи ИСПДн должны быть ознакомлены под роспись с требованиями настоящей Инструкции.

6. Ответственность

Все пользователи ИСПДн несут ответственность за соблюдение требований настоящей Инструкции.

Приложение № 20
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/02

ИНСТРУКЦИЯ
по организации резервного копирования и восстановления информации

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями законодательства Российской Федерации в области защиты информации (в том числе персональных данных), с целью обеспечения возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

1.2. Порядок определяет правила и объёмы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных (ИСПДн) Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым (далее – Инспекция Гостехнадзора РК).

1.3. Носители информации, используемые для резервирования конфиденциальной информации в Инспекции Гостехнадзора РК (в том числе и персональных данных), подлежат защите в той же степени, что и резервируемая конфиденциальная информация.

1.4. Ответственность за исполнение настоящей инструкции несет Администратор безопасностиИнспекции Гостехнадзора РК.

1.5. Данная инструкция предназначена для Администратора безопасностиИнспекции Гостехнадзора РК.

2. Информационные ресурсы, подлежащие резервированию

2.1. Резервному копированию подлежат все информационные ресурсы каждой ИСПДн Инспекции Гостехнадзора РК, содержащие персональные данные субъектов.

3. Порядок резервирования

3.1. Резервирование информационных ресурсов ИСПДнИнспекции Гостехнадзора РК, выполняется Администратором безопасности.

3.2. Определяется 2 вида резервирования информации:

- полное резервирование информации – резервное копирование всей информации, хранящейся в ИСПДн;
- неполное резервирование информации – резервное копирование части информации, хранящейся в ИСПДн.

Целью неполного резервирования является сохранение изменений в ИСПДн с момента полного резервирования информации.

3.3. Периодичность проведения работ по резервированию информации определяется Ответственным за организацию обработки персональных данных, обрабатываемых в ИСПДн Инспекции Гостехнадзора РК, но не реже 1 раза в месяц для полного резервирования и 1 раза в неделю для неполного резервирования.

3.4. Администратор безопасности использует средства резервного копирования ИСПДн для резервирования информации на отчуждаемый носитель. В случаях, когда резервирование информации средствами ИСПДн не представляется возможным, администратор информационной безопасности ИСПДн может использовать средство резервного копирования, не входящее в состав ИСПДн.

3.5. Резервное копирование с использованием незащищённых каналов связи общего пользования не допустимо.

3.6. Резервное копирование по локальной сети на устройство, находящееся вне ИСПДн, не допустимо.

3.7. Администратор безопасности не имеет право ознакомляться с резервируемой информацией. Факт ознакомления администратора информационной безопасности ИСПДн с резервируемой информацией может быть расценен как превышение служебных полномочий в соответствии с Трудовым Кодексом Российской Федерации и Кодексом об Административных Правонарушениях Российской Федерации.

3.8. В случае удаления информации из ИСПДн должна быть так же удалена ее резервная копия.

4. Порядок хранения резервных копий

4.1. Хранение резервных копий информации должно исключать любой несанкционированный доступ посторонних лиц к носителям информации.

4.2. Хранение резервных копий необходимо осуществлять в сейфах, несгораемых шкафах, металлических шкафах с устройством опечатывания. Доступ к местам хранения резервных копий должен быть предоставлен только Администратору безопасности.

4.3. На носителе информации, содержащем резервные копии защищаемой информации (в том числе персональных данных), не должна храниться посторонняя информация.

4.4. Должно быть обеспечено одновременное хранение не менее двух носителей информации, хранящих полную резервную копию защищаемой информации ИСПДн.

5. Порядок восстановления информации после сбоя

5.1. В случае сбоя в работе ИСПДн, восстановление данных из резервных копий осуществляет Администратор безопасности.

5.2. Администратор безопасности обязан срочно уведомить Ответственного за организацию обработки персональных данных о факте сбоя в работе ИСПДн, повлёкшего нарушение целостности данных.

Приложение № 21
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

ИНСТРУКЦИЯ
по обращению с криптосредствами

1. Термины и определения

В настоящей Инструкции по обращению с криптосредствами (далее – Инструкция) применяются следующие термины и определения:

Доступ к информации - возможность получения информации и ее использования.

Информационная система персональных данных- совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами.

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой блокнот - набор бумажных ключевых документов одного вида (таблиц, перфолент, перфокарт и т.п.), сброшюрованных и упакованных по установленным правилам.

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт - диск, DataKey, SmartCard, TouchMemory и т.п.).

Компрометация криптоключей – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате

которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Контролируемая зона - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Лицензиат ФСБ – оператор конфиденциальной связи и лица, имеющие лицензию ФСБ и не являющиеся операторами конфиденциальной связи.

Орган криптографической защиты – организация, структурное подразделение организации - лицензиата ФСБ, обладателя конфиденциальной информации или физическое лицо.

Пользователи СКЗИ – физические лица, непосредственно допущенные к работе с СКЗИ.

Средства криптографической защиты информации (СКЗИ) – сертифицированные ФСБ (ФАПСИ) России средства:

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно - программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ;
- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно - программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении;
- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно - программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и «электронной подписи»;
- аппаратные, программные и аппаратно - программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.

Специализированные помещения - помещения, где установлены СКЗИ или хранятся ключевые документы к ним.

2. Общие положения

2.1. Настоящий документ определяет порядок учета, хранения и использования СКЗИ и криптографических ключей, в целях обеспечения безопасности эксплуатации СКЗИ в Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым (далее – Учреждение).

2.2. Настоящая Инструкция разработана в соответствии с:

- Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66;
- Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной Приказом ФАПСИ от 13 июня 2001 г. № 152;
- Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденными Приказом ФСБ России от 10 июля 2014 г. № 378.

2.3. Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами приказом Начальника Учреждения назначается Администратор безопасности, выполняющий функции органа криптографической защиты информации и имеющий необходимый уровень квалификации.

Администратор безопасности осуществляет:

- поэкземплярный учет СКЗИ;
- контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;
- расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации.

2.4. Список Пользователей СКЗИ утверждается приказом Начальника Учреждения.

2.5. Пользователь СКЗИ обязан:

- строго соблюдать правила пользования СКЗИ и требования настоящей Инструкции;
- не допускать установки на ПЭВМ нештатных программ, предупреждать возможность занесения вирусов и других вредоносных программ;

- не разглашать информацию, к которой они допущены, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;
- соблюдать требования к обеспечению безопасности информации ограниченного доступа, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;
- сообщать о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- немедленно уведомлять Администратора безопасности о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемой информации;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с установленным порядком при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- не допускать снятие копий с ключевых документов;
- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;
- не допускать записи на ключевой носитель посторонней информации;
- не допускать установки ключевых документов в другие ПЭВМ.

2.6. Непосредственно к работе с СКЗИ Пользователи допускаются только после соответствующего обучения. Обучение пользователей правилам работы с СКЗИ осуществляет Администратор безопасности.

2.7. Текущий контроль, обеспечение функционирования и безопасности СКЗИ возлагается на Администратора безопасности.

2.8. Администратор безопасности и Пользователи СКЗИ должны быть ознакомлены с положениями настоящей Инструкцией под расписку.

3. Учет, хранение СКЗИ и криптографических ключей

3.1. Учет криптографических средств

3.1.1. Криптосредства, эксплуатационная и техническая документация к ним, используемые для обеспечения безопасности информации ограниченного доступа, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

3.1.2. Все поступившие СКЗИ, эксплуатационная и техническая документации к ним, а также ключевые документы должны быть взяты на поэкземплярный учет и внесены в «Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов» (далее – журнал поэкземплярного учета). При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие

криптосредства учитываются также совместно с соответствующими аппаратными средствами.

3.1.3. Поэкземплярный учет СКЗИ имеет цель обеспечить контроль за снабжением СКЗИ, их наличием, движением, расходованием и исключить обезличенное пользование ими. В журнале поэкземплярного учета должно отражаться полное прохождение каждого в отдельности экземпляра СКЗИ, эксплуатационной и технической документации к ним, ключевых документов с момента получения до уничтожения.

3.1.4. Единицей поэкземплярного учета криптографических средств, ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3.1.5. Журнал поэкземплярного учета ведет Администратор безопасности.

3.1.6. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов выдаются под расписку в соответствующем журнале поэкземплярного учета Пользователям СКЗИ, несущим персональную ответственность за их сохранность.

3.1.7. При увольнении, перемещении Пользователя СКЗИ все числящие за ним СКЗИ и другие документы передаются по акту сотруднику, которому поручено исполнять его обязанности. При временном убытии сотрудника (в том числе командировку, отпуск, по болезни) по акту могут быть переданы только СКЗИ и документы, необходимые для работы в период его отсутствия. Остальные числящие СКЗИ и документы должны находиться в опечатанном хранилище (упаковке). Акты составляются в одном экземпляре.

3.2. Хранение криптографических средств

3.2.1. Незадействованные в эксплуатации СКЗИ, дистрибутивы СКЗИ на магнитных носителях, эксплуатационная и техническая документация к ним хранится у Администратора безопасности. Криптографические ключи хранятся у Пользователей СКЗИ.

3.2.2. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

3.2.3. Инсталлирующие СКЗИ носители, эксплуатационная и техническая документация к СКЗИ, ключевые документы хранятся в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.2.4. Действующие и резервные ключевые документы, предназначенные для применения в случае компрометации действующихкриптоключей, хранятся раздельно.

3.3. Рассылка СКЗИ, ключевых документов

3.3.1. Криптосредства и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными нарочными, которыми могут быть Администратор безопасности или Пользователи СКЗИ, при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки. Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

3.3.2. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

3.3.3. Полученные упаковки вскрывают пользователи СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю.

3.3.4. При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний изготовителя.

3.3.5. Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме.

3.4. Уничтожение СКЗИ, ключевых документов

3.4.1. СКЗИ уничтожают (утилизируют) в соответствии с требованиями эксплуатационной и технической документации к ним.

3.4.2. Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и они полностью отсоединены от аппаратных средств.

3.4.3. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может

оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

3.4.4. СКЗИ, ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета.

3.4.5. О проведенном уничтожении СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, делаются отметки в соответствующих журналах учета.

3.4.6. Не реже одного раза в год пользователи СКЗИ должны направлять Администратору безопасности письменные отчеты об уничтоженных ключевых документах.

3.5. Компрометация криптоключей

3.5.1. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. О выводе криптоключей из действия сообщают Администратору безопасности. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению Администратора безопасности, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированныхкриптоключей должен быть максимально коротким, а передаваемая информация как можно менее ценной.

3.5.2. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации, Пользователи СКЗИ обязаны сообщать Администратору безопасности. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

3.5.3. Необходимо провести мероприятия по розыску и локализации последствий компрометации информации, передававшейся (хранящейся) с использованием СКЗИ.

4. Размещение, охрана и организация режима в помещениях, где установлены СКЗИ

4.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее – специализированные помещения), должны

обеспечивать сохранность информации ограниченного доступа, криптосредств и ключевых документов к ним.

4.2. При оборудовании специализированных помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с криптосредствами.

4.3. Специализированные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Специализированные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в специализированные помещения.

4.4. Размещение, специальное оборудование, охрана и организация режима в специализированных помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

4.5. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает Администратор безопасности по согласованию с Начальником Учреждения. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны. Внутриобъектовый режим устанавливается отдельной инструкцией.

4.6. Для предотвращения просмотра извне специализированных помещений их окна должны быть защищены.

4.7. Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в специализированных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

4.8. На время отсутствия Пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с Администратором безопасности необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

4.9. В специализированных помещениях Пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ)

индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих Пользователей СКЗИ.

4.10. При утрате Пользователем СКЗИ ключа от хранилища или от входной двери в специализированное помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

4.11. В обычных условиях опечатанные хранилища Пользователей СКЗИ могут быть вскрыты только самими пользователями.

4.12. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в специализированные помещения или несанкционированное вскрытие хранилищ посторонними лицами, о случившемся должно быть немедленно сообщено Начальнику и Администратору безопасности. Администратор безопасности должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации информации ограниченного доступа и к замене скомпрометированных криптоключей.

5. Правила доступа в специализированные помещения в нештатных ситуациях

5.1. В случае возникновения нештатной ситуации сотрудникам необходимо незамедлительно сообщать о происшествии руководителю своего структурного подразделения.

5.2. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в специализированные помещения всем сотрудникам организации.

5.3. Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в специализированные помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении администратора информационной безопасности, либо лица его замещающего.

Приложение № 22
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

ИНСТРУКЦИЯ

по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств информационных систем персональных данных

1. Обозначения и сокращения

ИСПДн — информационная система персональных данных;

ПЭВМ — персональная электронно-вычислительная машина;

СВТ — средства вычислительной техники;

СЗИ — средства защиты информации.

2. Общие положения

2.1. Настоящая инструкция определяет порядок проведения работ по установке, настройке, обновлению и устранению нештатных ситуаций, связанных с эксплуатацией технических средств и программного обеспечения (далее — Работы), входящих в состав ИСПДнИнспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым (далее – Учреждение).

2.2. Ответственность за организацию проведения Работ и контроль их выполнения, в соответствии с настоящей инструкцией, возлагается на Администратора безопасности.

2.3. Ответственные за эксплуатацию технического средства и сотрудники Учреждения, допущенные к работе в ИСПДн, несут персональную ответственность за выполнение Работ, в соответствии с настоящей инструкцией.

3. Порядок выполнения Работ в плановом режиме

3.1. Работы в плановом режиме выполняются только на основании письменных заявок, которые должны быть согласованы ответственным за эксплуатацию технического средства и Администратором безопасности. Форма заявки представлена в Приложении 1.

3.2. Согласованная заявка на выполнение Работ передается ответственному исполнителю:

- Администратору безопасности, если выполнение Работ касаются СЗИ;

- техническому специалисту Учреждения, ответственному за сопровождение технических средств и программного обеспечения, не относящегося к СЗИ.

Ответственный исполнитель после получения согласованной заявки на выполнение Работ организует её выполнение:

- определяет исполнителя (в случае необходимости может привлекаться сторонняя организация), и согласовывает его с Администратором безопасности;

- определяет срок выполнения и согласовывает его с Администратором безопасности и ответственным за эксплуатацию технического средства, на котором будут выполняться Работы.

3.3. Выполнение Работ осуществляется исполнителем в присутствии Администратора безопасности и ответственного за эксплуатацию технического средства, на котором выполняются Работы.

3.4. После проведения Работ исполнителем Администратор безопасности производит пересчет контрольных сумм с помощью установленных СЗИ и проводит антивирусный контроль.

3.5. Все проведенные работы фиксируются Администратором безопасности в «Журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств ИСПДн».

Обязательной регистрации в «Журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств ИСПДн» подлежат следующие виды работ:

- замена (модификация) СВТ, входящих в состав ИСПДн, в соответствии с техническим паспортом на ИСПДн, в том числе изменения линий локально-вычислительной сети и т.п.;

- замена, изъятие, добавление средств информатизации ИСПДн (средства электронно-вычислительной техники, комплектующие, системы и сети ИСПДн, системы и сети электросвязи, программные средства);

- техническое обслуживание и ремонт СВТ без замены комплектующих и составных частей;

- ремонт инженерных коммуникаций (линий силового питания, слаботочных линий и т.п.), изменения в системе силового питания СВТ;

- обновление (замена) на конкретном автоматизированном рабочем месте или сервере программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);

- изменение местоположения СВТ и вспомогательных средств и систем, указанных в схеме технического паспорта.

3.6. По результатам выполненных Работ, связанных со СЗИ, Администратором безопасности составляется «Акт установки и настройки средств защиты информации», подтверждающий работоспособность и правильность функционирования СЗИ.

3.7. Передача СВТ в другое подразделение или в распоряжение другой организации для проведения ремонта и сервисного обслуживания осуществляется только после того, как администратор информационной безопасности снимет средства защиты и предпримет необходимые меры для затирания или резервного копирования защищаемой информации, которая хранилась на дисках данного СВТ.

4. Порядок выполнения Работ при возникновении нештатной ситуации

4.1. В условиях, когда необходимо оперативное реагирование на нештатные ситуации, разрешается выполнение Работ без согласованной с Администратором безопасности заявки. К нештатным ситуациям относятся:

- выход из строя или неустойчивое функционирование узлов ПЭВМ, периферийных устройств, СЗИ по различным причинам;

- выход из строя системы электроснабжения.

4.2. При возникновении необходимости оперативного выполнения Работ, сотрудник Учреждения (при наличии возможности) немедленно сообщает об этом Администратору безопасности любым доступным способом (телефон, электронная почта и т.д.).

4.3. Необходимые Работы выполняются под контролем сотрудника Учреждения, ответственного за эксплуатацию технического средства с последующим написанием им объяснительной записки на имя

Администратора безопасности, с обоснованием необходимости оперативного проведения Работ и описанием произведенных действий.

4.4. По результатам рассмотрения объяснительной записки, Администратор безопасности выполняет действия, описанные в пунктах 3.4. - 3.6. настоящей инструкции.

5. Условия выполнения Работ, порядок установки и обновления ПО

5.1. Для выполнения Работ должны привлекаться только специалисты, имеющие необходимый уровень подготовки для обслуживания технических средств и программного обеспечения, из числа сотрудников Учреждения или сторонней организации, привлекаемой на договорной основе.

5.2. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

5.3. Установка и обновление программного обеспечения (общесистемного и прикладного) на рабочие станции и сервера ИСПДн осуществляется только с оригинальных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных в установленном порядке.

5.4. При контроле установки обновлений следует производить проверку соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, установленного в информационной системе персональных данных и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

5.5. В ИСПДн должны использоваться только лицензионные программные обеспечения и СЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

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

5.7. После установки (обновления) ПО, Администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки.

Приложение 1
к инструкции по модернизации, ремонту,
техобслуживанию технических средств
ИСПДн

ЗАЯВКА
на проведение ремонта и сервисного обслуживания
средств вычислительной техники

Прошу осуществить установку (модификацию, ремонт, техническое обслуживание, восстановление работоспособности программного обеспечения и аппаратных средств) в помещение №_____ отдела _____
_____
рабочее место _____ закрепленным за _____
_____
должность _____

Краткое описание необходимых работ и обоснование_____
_____
_____
_____

Дата _____/_____/

Приложение № 23
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 73/ОД

ПЛАН
внутренних проверок режима защиты персональных данных

1. Общие положения

План внутренних проверок режима защиты персональных данных, содержит перечень внутренних проверок.

План составляется для мероприятий, в соответствии с Планом мероприятий по обеспечению защиты персональных данных, и определяет периодичность проведения проверок.

План внутренних проверок содержит следующую информацию:

- название проверяемого мероприятия;
- периодичность проведения проверки;
- исполнитель мероприятия.

План внутренних проверок распространяется на все информационные системы персональных данных Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым.

2. План внутренних проверок режима защиты персональных данных

Мероприятие	Периодичность	Ответственный
Контроль соблюдения организационно-режимных требований в помещениях, в которых осуществляется обработка ПДн	Ежегодно	Ответственный за организацию обработки персональных данных
Контроль доступа к приложениям информационных систем персональных данных, в которых осуществляется обработка ПДн	Ежеквартально	Администратор безопасности
Контроль порядка обращения с носителями ПДн	Ежеквартально	Ответственный за организацию обработки персональных данных
Проверка выполнения запросов субъектов персональных данных	Ежеквартально	Ответственный за организацию обработки персональных данных
Контроль нейтрализации выявленных нарушений режима обработки ПДн	Ежеквартально	Администратор безопасности
Контроль за обновлениями программного обеспечения и	Ежеквартально	Ответственный за обеспечение

единообразия применяемого ПО на всех элементах ИСПДн		безопасности персональных данных
Организация анализа и пересмотра имеющихся угроз безопасности ПДн	Ежегодно	Администратор безопасности
Поддержание в актуальном состоянии нормативно-организационных документов по вопросам обеспечения безопасности ПДн	Ежегодно	Ответственный за организацию обработки персональных данных
Контроль над выполнением антивирусной защиты	Еженедельно	Администратор безопасности
Контроль над соблюдением режима защиты	Ежедневно	Администратор безопасности

Приложение № 24
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

ПЕРЕЧЕНЬ
персональных данных участвующих при неавтоматизированной обработке

№ п/п	Категории персональных данных	Наименование сведений	Субъекты ПДн	Цели обработки	Типы документов, где возможно появление сведений конфиденциального характера	Место хранения
1.	Иные	; фамилия, имя, отчество; пол; гражданство; паспортные данные (номер и серия паспорта, дата выдачи, код и наименование органа выдавшего паспорт); дата рождения; место рождения; адрес по месту регистрации; адрес места жительства; контактный телефон; адрес электронной почты; номер полиса обязательного медицинского страхования; идентификационный номер налогоплательщика (ИНН); страховой номер индивидуального лицевого счета (СНИЛС); сведения об образовании, в том числе данные об образовательных	Сотрудники оператора	Персональные данные в ИСПДн «Бухгалтерия» обрабатываются в целях начисления и выплаты заработной платы и иных выплат, установленных законодательством Российской Федерации и внутренними локальными нормативными актами; обеспечения соблюдения законных прав субъектов персональных данных, и исполнения обязанностей, установленных	- личная карточка формы Т2; - трудовая книжка; - личное дело; - трудовой договор; - приказы по личному составу; - штатное расписание; - справки; - анкеты.	295022, Республика Крым, г. Симферополь, ул. Кечкеметская, д. 198; *запираемые на замок шкафы и ящики столов.*

		организациях и о документах об образовании и (или) о квалификации; сведения о банковских счетах; сведения о семейном положении и о составе семьи; социальные льготы; сведения о трудовой деятельности; сведения о повышении квалификации; классный чин; занимаемая должность; род занятий; стаж работы; стаж муниципальной службы; сведения о заработной плате; сведения о доходах, расходах, имуществе и обязательствах имущественного характера; сведения о денежных средствах, находящихся на счетах в банках или иных кредитных организациях; сведения о ценных бумагах; номер расчетного счета в банке и сумма начислений; сведения о временной нетрудоспособности; сведения об отпусках.		Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации и иными нормативно-правовыми и внутренними локальными нормативными актами;обеспечения управленческой деятельности.		

Приложение № 25
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

ПЛАН

мероприятий по обеспечению безопасности персональных данных

№ п/п	Мероприятие	Срок исполнения	Ответственный
1	Создание комиссии по определению уровня защищенности персональных данных при их обработке в ИСПДн	Первый, второй квартал 2022	Начальник Инспекции Гостехнадзора РК
2	Определение уровня защищенности персональных данных при их обработке во всех выявленных ИСПДн	Первый, второй квартал 2022	Комиссия по определению уровня защищенности ПДн
3	Уточнение актуальности угроз безопасности персональных данных	Первый, второй квартал 2022	Администратор безопасности
4	Определение помещений для установки аппаратных средств ИСПДн с целью исключения несанкционированного доступа лиц, не допущенных к обработке персональных данных	Первый, второй квартал 2022	Ответственный за организацию обработки персональных данных
5	Разработка/уточнение организационно-распорядительных документов по защите персональных данных	Первый, второй квартал 2022	Администратор безопасности
6	Организация информирования и обучения работников о порядке обработки персональных данных	Первый, второй квартал 2022	Ответственный за организацию обработки персональных данных
7	Закупка, установка и настройка средств защиты информации	Первый, второй квартал 2022	Администратор безопасности
8	Аттестация ИСПДн	Первый, второй квартал 2022	Администратор безопасности

Приложение № 26
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. №13/ОД

ПОЛОЖЕНИЕ
о порядке хранения и уничтожения носителей персональных данных

1. Общие положения

1.1. Настоящее Положение о порядке хранения и уничтожения носителей персональных данных (далее – Положение) определяет условия хранения, вывода из эксплуатации и уничтожения сотрудниками Инспекции по надзору за техническим состоянием самоходных машин и других видов техники Республики Крым (далее - Инспекция Гостехнадзора РК) защищаемых носителей информации.

1.2. Цель настоящего Положения заключается в доведении до всех сотрудников правил использования защищаемых носителей информации (в том числе персональных данных) и достижения эффективного использования защищаемых носителей информации.

1.3. Все защищаемые носители информации делятся на съемные машинные носители информации (далее – СМНИ) и накопители на жёстких магнитных дисках (НЖМД).

1.4. СМНИ являются средством передачи и хранения различной информации в электронном виде. Нарушения правил использования СМНИ приводят к утечке информации ограниченного доступа, нарушению функционирования телекоммуникационных систем, утрате и искажению информации, что может нанести ущерб Инспекции Гостехнадзора РК. Наиболее часто встречаются СМНИ в виде USB-флеш накопителей, CD (DVD)-R или CD-RW дисков, различных типов карт флеш памяти, мультимедийных устройств, сотовых телефонов (смартфонов коммуникаторов), внешних жестких дисков, цифровых фотоаппаратов и видеокамер.

1.5. Требования настоящего Положения обязательны для всех сотрудников Инспекции Гостехнадзора РК.

1.6. Настоящее Положение распространяется на любые устройства независимо от интерфейсов подключения, способные подключаться к телекоммуникационному оборудованию, компьютерам, иным служебным техническим средствам и использоваться в качестве СМНИ.

1.7. Настоящее Положение не распространяется на СМНИ, предназначенные для записи и хранения сведений, составляющих государственную тайну.

1.8. СМНИ регистрируются в Журнале учёта машинных носителей информации (далее - журнал учета СМНИ) в структурном подразделении, использующем этот СМНИ.

2. Организация хранения СМНИ

2.1. Хранение СМНИ осуществляется в условиях, исключающих

несанкционированное копирование, изменение или уничтожение информации ограниченного доступа, а также хищение носителей. Носители должны храниться в служебных помещениях, в металлических шкафу (сейфах).

2.2. Запрещается хранить СМНИ вместе с носителями открытой информации, на рабочих столах, оставлять их без присмотра или передавать на хранение другим лицам, выносить СМНИ из служебных помещений для работы с ними на дому, а также использовать СМНИ в личных целях.

2.3. В случае утраты СМНИ, содержащих персональные данные, либо разглашения содержащихся в них сведений, необходимо поставить в известность Администратор безопасности. Соответствующие отметки вносятся в журнал учета машинных носителей информации.

3. Вывод СМНИ из эксплуатации

3.1. Процедуре вывода из эксплуатации подлежат только служебные СМНИ. Выводу из эксплуатации подлежат СМНИ в следующих случаях:

- выход из строя СМНИ;
- утеря СМНИ;
- передача СМНИ за пределы Инспекции Гостехнадзора РК.

3.2. Перед выводом из эксплуатации пользователь обязан убедиться в существовании актуальной копии информации, содержащейся на выводимом из эксплуатации СМНИ.

3.3. Факт вывода СМНИ из эксплуатации регистрируется в журнале учета машинных носителей информации Администратором безопасности.

3.4. Сотрудник, отвечающий за учет СМНИ, уничтожает имеющуюся на СМНИ информацию путем использования средств гарантированного уничтожения информации, в случае если СМНИ подлежит уничтожению или передаче третьему лицу. В случае передачи информации, хранимой на СМНИ, за пределы Инспекции Гостехнадзора РК уничтожение информации не проводится, а проверяется соответствие хранящейся на СМНИ информации и информации, требующей передачи.

4. Уничтожение СМНИ

4.1.Уничтожению подлежат только служебные СМНИ, выводимые из эксплуатации, которые невозможно использовать повторно, т.е. вышедшие из строя (поврежденные).

4.2.Уничтожение СМНИ проводится путем гарантированного уничтожения информации и физического разрушения, а в случае повреждения СМНИ проводится только физическое разрушение.

4.3.Факт уничтожения СМНИ регистрируется в журнале учета машинных носителей информации.

4.4.При уничтожении СМНИ, содержащего персональные данные, в обязательном порядке должен быть составлен акт уничтожения носителей персональных данных.

Приложение № 27
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

Акт №___
об уничтожении персональных данных

Комиссия в составе:
Председатель _____
Члены комиссии _____

Провела отбор носителей персональных данных и установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 2, подлежат уничтожению сведения, составляющие персональные данные:

№ п/п	Сведения, содержащие персональные данные	Тип носителя	Регистрационный номер носителя ПДн	Дата	Примечание
	1	2	3	4	6
1					
2					

Всего носителей_____.
(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПДн уничтожены путем
_____.
(разрезания, сжигания, механического уничтожения и т.п.)

Председатель комиссии: _____/_____/
Члены комиссии: _____/_____/
_____/_____/

Приложение № 28
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 1-3/00

(ФОРМА)
ЖУРНАЛ
поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

На ___ листах

Начат «__» _____ 20__ г. Окончен «__» _____ 20__ г.

Ответственный за журнал: _____ «__» _____ 20__ г.
Должность, ФИО, подпись

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийный номер СКЗИ эксплуатационной и технической документации к ним, ключевых документов	Номера экземпляров (криптографические номер) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	ФИО пользователя	Дата и расписка в получении	ФИО сотрудников органа криптографической защиты	Дата подключения (установки) и подписи лиц, производивших подключение	Номера аппаратных средств, в которые установлены СКЗИ	Дата изъятия (уничтожения)	ФИО сотрудников органа криптографической защиты	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение № 29
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

(ФОРМА)
ЖУРНАЛ
учета хранилищ, сейфов, специальных хранилищ, шкафов и ключей от них

На ___ листах

Начат «__» _____ 20__ г. Окончен «__» _____ 20__ г.

Ответственный за журнал: _____ «__» _____ 20__ г.
Должность, ФИО, подпись

№ п/п	Наименование (хранилищ, сейфов, специальное хранилище, шкаф, ключи от …)	Номер (хранилища, сейф, специальное хранилище, шкаф)	Местонахождение (хранилищ, сейф, специальное хранилище, шкаф)	Ответственный (хранилища, сейф, специальное хранилище, шкаф) Должность, ФИО	Дата/Подпись ответственного (хранилища, сейф, специальное хранилище, шкаф)	Количество ключей, № ключей (хранилища, сейф, специальное хранилище, шкаф)	Дата/Подпись ответственного За ключи	Примечание
1	2	3	4	5	6	7	8	9

Приложение № 30
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

(ФОРМА)
ЖУРНАЛ
уничтожения носителей персональных данных

На ___ листах

Начат «__» _____ 20__ г. Окончен «__» _____ 20__ г.

Ответственный за журнал: _____ «__» _____ 20__ г.
Должность, ФИО, подпись

№ п/п	Учетный № носителя	Тип носителя	Обоснование уничтожения	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных
1	2	3	4	6	7	8

Приложение № 31
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

(ФОРМА)
ЖУРНАЛ
учета машинных носителей персональных данных

На ___ листах

Начат «__» _____ 20__ г. Окончен «__» _____ 20__ г.

Ответственный за журнал: _____ «__» _____ 20__ г.
Должность, ФИО, подпись

№ п/п	Серийный/ инвентарный № АРМ	Дата постановки на учет	Подпись администратора информационной безопасности, производившего учет	Сведения об уничтожении носителя	Примечание
1	2	3	4	5	6

Приложение № 32
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

(ФОРМА)

ЖУРНАЛ

учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных

На ___ листах

Начат «__» _____ 20__ г. Окончен «__» _____ 20__ г.

Ответственный за журнал: _____ «__» _____ 20__ г.

Должность, ФИО, подпись

№ п/п	Должность и ФИО работника	Сведения о допуске к персональным данным			Работник, проводивший инструктаж	Подпись инструктируемого лица	Сведения о прекращении допуска к персональным данным		
		Наименование информационной системы персональных данных	Дата утверждения «Перечня лиц…»	Дата и подпись допускаемого лица			Дата утверждения «Перечня лиц…» или дата приказа об увольнении	Номер приказа об увольнении	Дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн
1	2	3	4	5	6	7	8	9	10

Приложение № 33
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

(ФОРМА)
ЖУРНАЛ
учета мероприятий по контролю обеспечения защиты персональных данных

На ___ листах

Начат «__» _____ 20__ г. Окончен «__» _____ 20__ г.

Ответственный за журнал: _____ «__» _____ 20__ г.
Должность, ФИО, подпись

№ п/п	Мероприятие	Дата	Исполнитель	Результат
1.				
2.				
3.				
4.				
5.				

Приложение № 34
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

(ФОРМА)

ЖУРНАЛ

учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств ИСПДн

На ___ листах

Начат «__» _____ 20__ г. Окончен «__» _____ 20__ г.

Ответственный за журнал: _____ «__» _____ 20__ г.

Должность, ФИО, подпись

№ п\п	Дата записи	Наименование объекта	Краткое описание выполненной работы	Дата и время начала работы	Ф.И.О. исполнителей работ и их подписи	Подпись лица, ответственного за защиту информации	Номера наклейки для опечатывания системного блока	Примечание
1	2	3	4	5	6	7	8	9

Приложение № 35
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

(ФОРМА)

ЖУРНАЛ

учета инцидентов информационной безопасности

На ___ листах

Начат «__» _____ 20__ г. Окончен «__» _____ 20__ г.

Ответственный за журнал: _____ «__» _____ 20__ г.

Должность, ФИО, подпись

№	Дата и время возникновения инцидента	Дата и время обнаружения инцидента	Сотрудник, обнаруживший инцидент	Краткое описание инцидента	Кому направлено для разрешения	Дата и время направлена сообщения об инциденте	Причины инцидента	Предпринятые действия для устранения инцидента	Дата и время разрешения инцидента	Предпринятые действия для предупреждения возникновения инцидента
1	2	3	4	5	6	7	8	9	10	11

Приложение № 36
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/02

(ФОРМА)

ЖУРНАЛ

учета средств защиты информации

На ___ листах

Начат «__» _____ 20__ г. Окончен «__» _____ 20__ г.

Ответственный за журнал: _____ «__» _____ 20__ г.

Должность, ФИО, подпись

№	Наименование СЗИ	Дата установки	Место установки	Место хранения дистрибутива	Ответственный за дистрибутив	Номер СЗИ
1	2	3	4	5	6	7
2						
3						
4						
7						

Приложение № 37
Утверждено приказом
Инспекции Гостехнадзора РК
от «03» 02 2022 г. № 13/ОД

(ФОРМА)
ЖУРНАЛ
учета программного обеспечения, разрешенного к установке

На ___ листах

Начат «__» _____ 20__ г. Окончен «___» _____ 20__ г.

Ответственный за журнал: _____«___» _____ 20__ г.
Должность, ФИО, Подпись

№	Наименование программного обеспечения	Версия программного обеспечения	Подпись ответственного	Примечание
1	2	3	4	5
1.				
2.				
3.				