

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ |
|  | Генеральный директорООО "МАСКОМ-Техлайн" |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | А.В. Кравченко |
|  |  | (подпись) |  |
|  | "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |

ТОМ 08

ОТЧЕТ

по результатам обследования информационных систем департамента по охране и надзору за использованием объектов животного мира и среды их обитания
Магаданской области

на 34 листах

г. Хабаровск

2016

Содержание

[Список использованных сокращений 3](#_Toc478048032)

[Нормативно-методическое обеспечение 4](#_Toc478048033)

[1 Информация об объекте информатизации 6](#_Toc478048034)

[1.1 Основание для проведения работ 6](#_Toc478048035)

[1.2 Общие сведения 6](#_Toc478048036)

[1.3 Сведения о расположении и структуре ОИ 8](#_Toc478048037)

[1.4 Перечень информации, обрабатывающейся на объекте информатизации 9](#_Toc478048038)

[2 Характеристика комплекса ОТСС, ПО, режимов работы, технологического процесса обработки информации 11](#_Toc478048039)

[2.1 Характеристика каналов связи объекта информатизации 12](#_Toc478048040)

[3 Технология обработки ЗИ на ОИ 12](#_Toc478048041)

[3.1 Технология обработки защищаемой информации без использования средств вычислительной техники 13](#_Toc478048042)

[3.2 Технология обработки защищаемой информации с использованием средств вычислительной техники 14](#_Toc478048043)

[4 Технология функционирования информационных систем 20](#_Toc478048044)

[5 Выполнение требований к защите информации на момент обследования 25](#_Toc478048045)

[6 Классификация информационных систем 25](#_Toc478048046)

[6.1 Определение требуемого уровня защищенности персональных данных 26](#_Toc478048047)

[6.2 Определение класса защищенности информационной системы 27](#_Toc478048048)

[7 Состав мер защиты информации 30](#_Toc478048049)

[Выводы и рекомендации 33](#_Toc478048050)

Список использованных сокращений

АРМ автоматизированное рабочее место

БД база данных

ГИС государственная информационная система

ДСП для служебного пользования

ЗИ защищаемая информация

ИБ информационная безопасность

ИС информационная система

ИСПДн информационная система персональных данных

ЛВС локальная вычислительная сеть

МО Магаданская область

ОИ объект информатизации

ОС операционная система

ОТСС основные технические средства и системы

ПДн персональные данные

ПО программное обеспечение

РФ Российская Федерация

СКЗИ средство криптографической защиты информации

СрЗИ средства защиты информации

ТС техническое средство

УЗ уровень защищенности

УО условное обозначение

УФК Управление федерального казначейства

ФЗ Федеральный закон

ФСБ Федеральная служба безопасности

ФСТЭК Федеральная служба по техническому и экспортному контролю

ЭП электронная подпись

Нормативно-методическое обеспечение

1. Федеральный закон от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации".
2. Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных";
3. Перечень сведений конфиденциального характера, утвержденный Указом Президента РФ от 06.03.1997 №188.
4. Постановление Правительства РФ от 15.09.2008 №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".
5. Постановление Правительства Российской Федерации от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
6. Приказ ФАПСИ России от 13.06.2001 №152 "Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну".
7. Приказ ФСТЭК России от 11.02.2013 №17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
8. Приказ ФСТЭК России от 18.02.2013 №21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
9. Приказ ФСБ России от 10.07.2014 №378 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности".
10. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Председателя Гостехкомиссии России от 30.08.2002 №282.
11. Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14.02.2008 заместителем директора ФСТЭК России).
12. Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15.02.2008 заместителем директора ФСТЭК России).
13. Информационное сообщение ФСТЭК России по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11.02.2013 №17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и приказа ФСТЭК России от 18.02.2013 №21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" от 15.07.2013 №240/22/2637.
14. Методический документ "Меры по защите информации в государственных информационных система", утвержденных ФСТЭК России 11.02.2014.
15. ГОСТ 34.601-90 "Информационная технология. Автоматизированные системы. Стадии создания".
16. ГОСТ Р 51624-2000 Автоматизированные информационные системы в защищенном исполнении.
17. ГОСТ Р 51583-2000 Порядок создания автоматизированных систем в защищенном исполнении.
18. ГОСТ Р 51275-2006 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения".

# Информация об объекте информатизации

## Основание для проведения работ

Основание для проведения работ описано в п.п. 1 "Аналитического отчета по результатам обследования информационных систем в Правительстве Магаданской области, органах исполнительной власти Магаданской области и их подведомственных учреждениях, в целях обеспечения защиты информации ограниченного доступа".

## Общие сведения

Департамент по охране и надзору за использованием объектов животного мира и среды их обитания Магаданской области (далее – Департамент, ОИ, объект информатизации) образован на основании Постановления правительства Магаданской области от 09.01.2014 № 2-пп "[Об утверждении Положения о [по охране и надзору за использованием объектов животного мира и среды их обитания Магаданской области](http://ohotnadzor.49gov.ru/documents/one/index.php?id=3786)](http://leshoz.49gov.ru/documents/one/index.php?id=3791)".

Полное наименование ОИ: Департамент по охране и надзору за использованием объектов животного мира и среды их обитания Магаданской области.

Сокращенное название: Департамент госохотнадзора.

Объект информатизации по охране и надзору за использованием объектов животного мира и среды их обитания Магаданской области является органом исполнительной власти Магаданской области, осуществляющим полномочия в области охраны и использования объектов животного мира, охоты и сохранения охотничьих ресурсов, в том числе отдельные полномочия Российской Федерации в указанных сферах, переданные органам исполнительной власти субъектов Российской Федерации, а также полномочия в области организации и функционирования особо охраняемых природных территорий регионального значения, деятельность которых направлена на охрану и воспроизводство животного мира.

Объект информатизации в своей деятельности руководствуется Конституцией Российской Федерации, международными договорами Российской Федерации, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, Уставом Магаданской области, законами Магаданской области, постановлениями и распоряжениями губернатора Магаданской области, постановлениями и распоряжениями Правительства Магаданской области, иными нормативными правовыми актами.

Объект информатизации осуществляет свою деятельность во взаимодействии с органами исполнительной власти Магаданской области, федеральными органами исполнительной власти, территориальными органами федеральных органов исполнительной власти, государственными учреждениями Магаданской области, органами местного самоуправления муниципальных образований Магаданской области, организациями независимо от их форм собственности, а также гражданами.

Основными целями создания и деятельности ОИ являются:

* организация и осуществление сохранения и использования охотничьих ресурсов и среды их обитания на территории Магаданской области, за исключением охотничьих ресурсов, находящихся на особо охраняемых природных территориях федерального значения;
* осуществление федерального государственного охотничьего надзора на территории Магаданской области, за исключением особо охраняемых природных территорий федерального значения;
* организация и осуществление охраны и воспроизводства объектов животного мира на территории Магаданской области, а также охрана их среды обитания, в том числе на особо охраняемых природных территориях регионального значения;
* федеральный государственный надзор в области охраны и использования объектов животного мира и среды их обитания на территории Магаданской области, за исключением объектов животного мира и среды их обитания, находящихся на особо охраняемых природных территориях федерального значения, расположенных на территории Магаданской области.

В соответствии с целями своей деятельности ОИ выполняет следующие функции:

* в области охоты и сохранения охотничьих ресурсов:
* организация и осуществление сохранения и использования охотничьих ресурсов и среды их обитания;
* регулирование численности охотничьих ресурсов;
* ведение государственного охотхозяйственного реестра и осуществление государственного мониторинга охотничьих ресурсов и среды их обитания на территории Магаданской области;
* заключение охотхозяйственных соглашений, организация и проведение аукционов на право заключения таких соглашений;
* выдача разрешений на добычу охотничьих ресурсов;
* выдача разрешений на содержание и разведение охотничьих ресурсов в полувольных условиях и искусственно созданной среде обитания;
* осуществление контроля за использованием капканов и других устройств, используемых при осуществлении охоты;
* осуществление контроля за оборотом продукции охоты;
* осуществление федерального государственного охотничьего надзора на территории Магаданской области.
* выдача и аннулирование охотничьих билетов.
* в области охраны и использования объектов животного мира:
* организация и осуществление охраны и воспроизводства объектов животного мира, а также охрана среды обитания объектов животного мира;
* регулирование численности объектов животного мира;
* ведение государственного учета численности объектов животного мира, государственного мониторинга и государственного кадастра объектов животного мира в пределах территории Магаданской области;
* выдача разрешений на использование объектов животного мира;
* выдача разрешений на содержание и разведение объектов животного мира в полувольных условиях и искусственно созданной среде обитания;
* осуществление мер по воспроизводству объектов животного мира и восстановлению среды их обитания, нарушенных в результате стихийных бедствий и по иным причинам;
* Федеральный государственный надзор в области охраны и использования объектов животного мира и среды их обитания на территории Магаданской области.
* в области организации и функционирования особо охраняемых природных территорий регионального значения, деятельность которых направлена на охрану и воспроизводство животного мира:
* осуществление государственного управления и государственного контроля в области организации и функционирования особо охраняемых природных территорий регионального значения;
* ведение государственного кадастра особо охраняемых природных территорий регионального значения.

## Сведения о расположении и структуре ОИ

Юридический и фактический адрес ОИ: 685000, Магаданская область, г. Магадан, ул. Портовая, 8.

Объект информатизации расположен в административном здании на правах аренды. Арендодателем является Областное государственное бюджетное учреждение "Магаданский областной эксплуатационный центр" (далее – ОГБУ "МОЭЦ").



Рисунок 1 – Расположение здания ОИ в пределах улиц

Объект информатизации входит в структуру исполнительных органов государственной власти МО.

Структура и штатное расписание ОИ утверждаются приказом руководителя ОИ.

В структуру ОИ входят следующие подразделения и отделы:

* **Отдел воспроизводства объектов животного мира**;
* **Отдел обеспечения основной деятельности**;
* **Отдел надзора, охраны и использования объектов животного мира и среды их обитания**;
* **Отдел бухгалтерского учета и финансов**;
* **Отдел правового, информационного и кадрового обеспечения**.

Сведения о режимах работы ОИ представлены в таблице 1.

Таблица 1 – Режим работы объекта информатизации

|  |  |  |
| --- | --- | --- |
| Наименование ОИ | Периодичность | Режим работы |
| 1 | 2 | 3 |
| Департамент госохотнадзора | Понедельник - пятница | 09:00 – 18:15 |
| Обеденное время | 12:45 – 14:00 |
| Суббота, воскресение | Выходной |

Работа на ОИ может осуществляться в режиме ненормированного рабочего дня, в соответствии с Трудовым кодексом РФ работники могут по распоряжению представителя нанимателя (работодателя), при необходимости, эпизодически привлекаться к выполнению своих трудовых функций за пределами установленной для них продолжительности рабочего времени.

Эпизодическое привлечение работников к работе на условиях ненормированного рабочего дня осуществляется при возникновении необходимости служебного или организационного (управленческого) характера, в случаях и в пределах, предусмотренных действующим законодательством.

Работа в выходные и праздничные дни осуществляется с соблюдением требований действующего трудового законодательства РФ.

Основные технические средства и системы ОИ, за исключением серверов и АРМ дежурного персонала, работают в соответствии с нормированным рабочим днем. Серверы и АРМ дежурного персонала работают круглосуточно.

## Перечень информации, обрабатывающейся на объекте информатизации

Обследование информационных систем на ОИ, предназначенных для обработки сведений, составляющих государственную тайну, в соответствии с Государственным контрактом - не проводилось.

Согласно проведенному обследованию методом интервьюирования и анкетирования на ОИ осуществляется обработка информации следующих видов: служебная информация, информация ограниченного доступа, общедоступная информация (далее – защищаемая информация, ЗИ).

К служебной информации, обрабатывающейся ОИ, относится информация о функционировании ОИ, не отнесенная к категории общедоступной или конфиденциальной.

К информации ограниченного доступа, обрабатываемой на ОИ, относится [3]:

* информация о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющая идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
* сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с [Конституцией](http://base.garant.ru/10103000/2/#block_23) РФ и федеральными законами.

К общедоступной информации относится общеизвестные сведения и иная информация, доступ к которой не ограничен.

На ОИ обрабатываются следующие категории субъектов персональных данных:

1. персональные данные работников ОИ, находящихся на кадровом обеспечении (далее - Работники);
2. персональные данные лиц, принимающих участие в конкурсе на замещение вакантных должностей государственной гражданской службы МО и (или) на включение в кадровый резерв для замещения вакантных должностей государственной гражданской службы МО (далее– Кандидаты);
3. персональные данные граждан, обратившихся в соответствии с действующим законодательством, обратившихся с вопросами (просьбами), обратившихся за получением государственных и муниципальных услуг (далее - Граждане);
4. персональные данные граждан, совершивших административное правонарушение в сфере надзора и охраны объектов животного мира (далее - Нарушители);
5. персональные данные граждан, ведущих охотничье хозяйство на основании долгосрочной лицензии на пользование животным миром и договора о предоставлении охотничьих угодий (далее - Охотпользователи);
6. персональные данные граждан, подавших заявление на обладание охотничьим билетом (далее - Заявители на обладание охотничьим билетом);
7. персональные данные граждан, подавших заявление на добычу охотничьих ресурсов (далее - Заявители на разрешение на добычу охотничьих ресурсов).

Правовые основания обработки персональных данных для каждого субъекта ПДн указаны в таблице 2.

Таблица 2 – Правовое основание обработки персональных данных

| № п/п | Субъект ПДн | Правовое основание обработки персональных данных |
| --- | --- | --- |
| 1 | 2 | 3 |
|  | Работники | Конституция РФ;Трудовой кодекс РФ от 30.12.2001 №197-ФЗ;Гражданский кодекс РФ от 30.11.1994 №51-ФЗ (часть 1);Семейный кодекс РФ от 29.12.1995 №223-ФЗ;Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных";ст. 20, 42, 52 Федерального закона от 27.07.2004 № 79-ФЗ "О государственной гражданской службе РФ";ст. 8 Федерального закона от 25.12.2008 № 273-ФЗ "О противодействии коррупции";Устав Правительства МО;Закон МО от 09.02.2005 №553-ОЗ "О государственной гражданской службе МО" |
|  | Кандидаты | Конституция РФ;Трудовой кодекс РФ от 30.12.2001 №197-ФЗ;Гражданский кодекс РФ от 30.11.1994 №51-ФЗ (часть 1);Семейный кодекс РФ от 29.12.1995 №223-ФЗ;Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных";ст. 64 Федерального закона от 27.07.2004 №79-ФЗ "О государственной гражданской службе РФ";ст. 8 Федерального закона от 25.12.2008 № 273-ФЗ "О противодействии коррупции";Устав Правительства МО;Закон МО от 09.02.2005 №553-ОЗ "О государственной гражданской службе МО" |
|  | Граждане | Конституция РФ;Гражданский кодекс РФ от 30.11.1994 №51-ФЗ (часть 1);Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных";Федеральный закон от 02.05.2006 №59-ФЗ "О порядке рассмотрения обращений граждан РФ";Устав Правительства МО |
|  | Нарушители | Конституция РФ;Гражданский кодекс РФ от 30.11.1994 №51-ФЗ (часть 1);Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ;Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных";Устав Правительства МО;Положение о департаменте по охране и надзору за использованием объектов животного мира и среды их обитания Магаданской области (Утверждено Постановлением Правительства МО от 09.01.2014 №2-пп) |
|  | Охотпользователи | Конституция РФ;Гражданский кодекс РФ от 30.11.1994 №51-ФЗ (часть 1);Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных";Устав Правительства МО;Положение о департаменте по охране и надзору за использованием объектов животного мира и среды их обитания Магаданской области (Утверждено Постановлением Правительства МО от 09.01.2014 №2-пп);Постановление губернатора Магаданской области от 26.07.2016 №159-п «Об утверждении лимитов добычи охотничьих ресурсов и квот их добычи на период с 01 августа 2016 года до 01 августа 2017 года на территории Магаданской области» |
|  | Заявители на обладание охотничьим билетом | Конституция РФ;Гражданский кодекс РФ от 30.11.1994 №51-ФЗ (часть 1);Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных";Устав Правительства МО;Положение о департаменте по охране и надзору за использованием объектов животного мира и среды их обитания Магаданской области (Утверждено Постановлением Правительства МО от 09.01.2014 №2-пп);[Приказ от 26.01.2016 № 4-О «Об утверждении Административного регламента по предоставлению государственной услуги по выдаче и аннулированию охотничьего билета единого федерального образца на территории Магаданской области](https://ohotnadzor.49gov.ru/documents/one/index.php?id=14563)" |
|  | Заявители на разрешение на добычу охотничьих ресурсов | Конституция РФ;Гражданский кодекс РФ от 30.11.1994 №51-ФЗ (часть 1);Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных";Устав Правительства МО;Положение о департаменте по охране и надзору за использованием объектов животного мира и среды их обитания Магаданской области (Утверждено Постановлением Правительства МО от 09.01.2014 №2-пп) |

# Характеристика комплекса ОТСС, ПО, режимов работы, технологического процесса обработки информации

Все технические средства и системы ОИ располагаются в пределах контролируемой зоны. Схема занимаемых помещений в здании с указанием границ контролируемой зоны и с расположением технических средств и систем представлена в приложение А. Режим работы ОТСС совпадает с режимом работы структурных подразделений ОИ.

Обработка ЗИ осуществляется в системном и прикладном программном обеспечении. Режим обработки ЗИ – многопользовательский с разграничением прав пользователей.

Характеристики комплексов основных технических средств и систем ОИ, а также перечень программного обеспечения, используемого на ОИ указаны в приложении Б.

## Характеристика каналов связи объекта информатизации

Все технические средства и системы ОИ находятся в собственной ЛВС. Локальная вычислительная сеть ОИ построена на основе кабелей симметричной витой пары и коммутационного оборудования. Коммутационное оборудование ОИ располагается в пределах занимаемых помещений в административном здании.

Объект информатизации имеет доступ к объединенной вычислительной сети Правительства МО.

Доступ к сети Интернет имеют все пользователи ИС ОИ. Доступ к сети Интернет одноточечный, предоставляется на основании постановления Правительства Магаданской области от 09.01.2014 года №4-пп "Об утверждении Положения о министерстве дорожного хозяйств, транспорта и связи Магаданской области".

Беспроводные технологии в ЛВС ОИ не используются. Подробная схема ЛВС ОИ представлена на рисунке 2.



Рисунок 2 – Схема ЛВС ОИ

# Технология обработки ЗИ на ОИ

Защищаемая информация, хранимая, обрабатываемая и передаваемая на ОИ существует как в электронном виде, так и на бумажных носителях.

В своей деятельности ОИ хранит, обрабатывает и передает данные, относящиеся к прямо или косвенно определенному, или определяемому физическому лицу, что попадает под действие документа [2].

Основанием для отнесения сведений, обрабатываемых на ОИ, к информации ограниченного распространения является документ [3].

Объект информатизации взаимодействует с организациями и учреждениями разных форм собственности. К примеру, ОИ взаимодействует с органами государственной власти МО, органами местного самоуправления, с правоохранительными органами МО, с природоохранной прокуратурой и др.

Обмен ЗИ осуществляется как в электронном виде, так и на бумажных носителях. В электронном виде информация передается по открытым или защищенным каналам связи. На бумажных носителях ЗИ передается нарочным или с привлечением специализированных организаций.

## Технология обработки защищаемой информации без использования средств вычислительной техники

Защищаемая информация может содержаться на бумажных носителях в текущей документации работника, служебной переписке и другой документации.

Документы, предназначенные для служебного пользования (с пометкой ДСП), отрабатываются исключительно на местах, допущенных к обработке настоящей информации работников.

Хранение документов, обработка которых завершена и (или) приостановлена, осуществляется в архивном помещении.

Таблица 3 – Места хранения носителей информации

| № п/п | Тип и наименование ЗИ | Наименование документов (носителей) | Места хранения | № кабинета |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
|  | ПДн "Нарушителей" | Согласно номенклатуре дел | Шкаф, рабочий стол работника (на момент обработки) | 401 |
|  | ПДн "Граждан" | Согласно номенклатуре дел | Шкаф, рабочий стол работника (на момент обработки) | 402 |
|  | ПДн "Граждан" | Согласно номенклатуре дел | Шкаф, рабочий стол работника (на момент обработки) | 404 |
| ПДн "Нарушителей" |
| Документы с пометкой ДСП | Служебная переписка |
|  | Документы с пометкой ДСП | Служебная переписка | Шкаф, рабочий стол работника (на момент обработки) | 405 |
|  | Документы с пометкой ДСП | Служебная переписка | Шкаф, рабочий стол работника (на момент обработки) | 406 |
|  | ПДн "Работников" | Согласно номенклатуре дел | Шкаф, рабочий стол работника (на момент обработки) | 409 |
|  | ПДн "Граждан" | Согласно номенклатуре дел | Шкаф, рабочий стол работника (на момент обработки) | 417 |
| ПДн "Заявителей на обладание охотничьего билета" |
|  | ПДн "Работников" | Согласно номенклатуре дел | Шкаф, рабочий стол работника (на момент обработки) | 419 |
| ПДн "Кандидатов" |
|  | ПДн "Заявителей на обладание охотничьего билета" | Согласно номенклатуре дел | Шкаф, рабочий стол работника (на момент обработки) | 430 |
| ПДн "Заявителей на разрешение на добычу охотничьих ресурсов" | Согласно номенклатуре дел | Шкаф, рабочий стол работника (на момент обработки) |
|  | ПДн "Охотпользователей" | Согласно номенклатуре дел | Шкаф, рабочий стол работника (на момент обработки) | 435 |
| ПДн "Нарушителей" |
| ПДн "Кандидатов" |
|  | ПДн "Охотпользователей" | Согласно номенклатуре дел | Шкаф, рабочий стол работника (на момент обработки) | 436 |
| ПДн "Нарушителей" |

## Технология обработки защищаемой информации с использованием средств вычислительной техники

Обработка ЗИ в информационных системах ОИ с использованием средств вычислительной техники осуществляется в системном и прикладном программном обеспечении.

Обмен информацией в электронном виде между пользователями ИС осуществляется через общие сетевые ресурсы ЛВС, а также на съемных машинных носителях информации.

Таблица 4 – Автоматизированная обработка защищаемой информации

| № п/п | Тип защищаемой информации (ЗИ) | Пользователи, обрабатывающие ЗИ | Технологические процессы обработки информации | УО ТС | Программные комплексы |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  | ПДн "Работников" (иные, общедоступные категории) | Главный бухгалтер | Осуществляет контроль за выданными в подотчет денежными средствами, правомерностью их расходования, внесением остатков в кассу и сроками предоставления отчетов подотчетными лицами.Осуществляет контроль за использованием выданных доверенностей на получение имущественно-материальных и других ценностей.Составляет и предоставляет в установленные законодательством Российской Федерации органы, а также порядке и сроки бухгалтерской, бюджетной и налоговой отчетности. | HD-010-03 | Бухгалтерский комплекс СЛВ "Бухгалтерия", КС-Хранилище, Свод-Смарт, Microsoft Office |
| Главный специалист отдела правового, информационного и кадрового обеспечения | Осуществляет подготовку документов, необходимых при приеме, переводе, прохождении государственной гражданской службы и освобождении от государственной гражданской службы в соответствии с Федеральным законом от 07.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации", законом Магаданской области от 09.02.2005 №553-ОЗ "О государственной гражданской службе Магаданской области", а также постановлениями и распоряжениями Правительства и губернатора МО.Осуществляет:-ведение реестра государственных гражданских служащих ОИ;-ведение трудовых книжек, книги учета движения трудовых книжек и вкладышей к ним;-ведение личных дел государственных гражданских служащих ОИ. | HD-010-23 | Microsoft Office, Портал государственной службы, АИС "Дело" |
| Главный специалист отдела учета финансов | Осуществляет начисление и выплату заработной платы служащим ОИ.Составляет и предоставляет в установленные законодательством Российской Федерации органы, а также порядке и сроки бухгалтерской, бюджетной и налоговой отчетности. | HD-010-06 | Бухгалтерский комплекс СЛВ "Бухгалтерия", Бухгалтерский комплекс СЛВ "Зарплата", Банк-клиент Сбербанк, Банк-клиент ВТБ24, Microsoft Office |
|  | ПДн "Кандидатов" (иные, общедоступные категории) | Специалист – государственный инспектор по охране окружающей среды | Занимается размещением информации о вакансиях, мониторингом соискателей на работу на федеральном портале управленческих кадров  | HD-010-18 | Microsoft Office, Федеральный портал управленческих кадров |
| Главный специалист отдела правового, информационного и кадрового обеспечения | Мониторинг соискателей на работу на портале государственной службы. | HD-010-23 | Microsoft Office, Портал государственной службы, АИС "Дело" |
|  | ПДн "Нарушителей" (иные категории) | Первый заместитель руководителя департамента – заместитель главного государственного инспектора по охране окружающей среды | Рассмотрение дел об административных правонарушениях в сфере надзора и охраны объектов животного мира. | HD-010-07 | Microsoft Office |
| Ведущий специалист территориальной группы по г. Магадану и Ольскому району – государственный инспектор по охране окружающей среды | HD-010-12 | Microsoft Office |
| Охотовед 2 категории – государственный инспектор по охране окружающей среды | HD-010-13 | Microsoft Office |
| Специалист 1 категории отдела воспроизводства объектов животного мира – государственный инспектор по охране окружающей среды | HD-010-16 | Microsoft Office |
| Заместитель начальника отдела надзора, охраны и использования объектов животного мира и среды их обитания – руководитель территориальной группы по г. Магадану и Ольскому району – старший государственный инспектор по охране окружающей среды | HD-010-17 | Microsoft Office |
| Специалист – государственный инспектор по охране окружающей среды | HD-010-22 | Microsoft Office |
|  | ПДн "Охотпользователей" (иные категории) | Начальник отдела воспроизводства объектов животного мира – старший государственный инспектор по охране окружающей среды | Оказание государственных услуг: - Заключение охотхозяйственных соглашений без проведения аукциона;- Организация и проведение аукционов на право заключения охотхозяйственных соглашений | HD-010-14 | Microsoft Office |
|  | ПДн "Заявителей на обладание охотничьим билетом" (иные категории) | Начальник отдела надзора, охраны и использования объектов животного мира и среды их обитания – старший государственный инспектор по охране окружающей среды | Осуществление федерального государственного охотничьего надзора на территории Магаданской области, просмотр списков заявителей на обладание охотничьего билета. | HD-010-19 | Microsoft Office |
| Ведущий специалист отдела воспроизводства объектов животного мира – государственный инспектор по охране окружающей среды | Оказание государственной услуги: "Выдача и аннулирование охотничьего билета единого федерального образца на территории Магаданской области" | HD-010-21 | Microsoft Office, СМЭВ (ViPNet 2542) |
| Специалист – государственный инспектор по охране окружающей среды | HD-010-22 | Microsoft Office, СМЭВ (ViPNet 2542) |
|  | ПДн "Заявителей на разрешение на добычу охотничьих ресурсов" (иные категории) | Специалист – государственный инспектор по охране окружающей среды | Оказание государственной услуги: "Выдача разрешений на добычу охотничьих ресурсов, за исключением охотничьих ресурсов, находящихся на особо охраняемых природных территориях федерального значения, а также занесенных в Красную книгу Российской Федерации" | HD-010-22 | Microsoft Office, СМЭВ (ViPNet 2542) |
| Ведущий специалист отдела воспроизводства объектов животного мира – государственный инспектор по охране окружающей среды | HD-010-21 | Microsoft Office, СМЭВ (ViPNet 2542) |
|  | ПДн "Граждан" (иные, общедоступные категории) | Секретарь | Прием и регистрация обращений граждан | HD-010-02 | АИС "Дело", Microsoft Office (Word, Excel) |
| Первый заместитель руководителя департамента – заместитель главного государственного инспектора по охране окружающей среды | Осуществляют прием и рассмотрение обращений граждан, поступающих через ПО для ССТУ. На каждое обращение заводится дело (в том числе в электронном виде), в которое заносится информация по обращению, в том числе ПДн обратившегося. По поступившим обращениям готовятся проекты ответов, которые в дальнейшем после подписи ответственных лиц направляются обратившимся | HD-010-07 | Microsoft Office,УАРМ ОДПГ |
| Специалист – государственный инспектор по охране окружающей среды | HD-010-18 | Microsoft Office,УАРМ ОДПГ |
| Заместитель руководителя департамента – заместитель главного государственного инспектора по охране окружающей среды | HD-010-20 | Microsoft Office |
|  | Служебная информация | Специалист – государственный инспектор по охране окружающей среды | Администрирование информационных систем ОИ, наполнение и сопровождения портала ОИ | HD-010-18 | 49gov.ru |
| Главный специалист отдела правового, информационного и кадрового обеспечения | Наполнение и сопровождения портала ОИ | HD-010-23 |
|  | Информация ограниченного доступа | Секретарь | Организует делопроизводство в ОИ, осуществляет экспедиционную обработку, прием, регистрацию, учет, хранение, доставку и рассылку корреспонденции (входящей, исходящей, внутренней), в том числе переданной по специальным средствам связи, ведет справочную работу по ней. | HD-010-02 | АИС "Дело" |
| Первый заместитель руководителя департамента – заместитель главного государственного инспектора по охране окружающей среды | Электронный документооборот | HD-010-07 | АИС "Дело" |
| Заместитель руководителя департамента – заместитель главного государственного инспектора по охране окружающей среды | HD-010-20 | АИС "Дело" |

# Технология функционирования информационных систем

В рамках выполнения аудита информационной безопасности на ОИ, были выделены следующие информационные системы:

* ИС "Бухгалтерия и кадры";
* ИС "Охрана объектов животного мира";
* ИС "Охотпользователи";
* ИС "Администраторы";
* ИС "Дело" (пользовательский сегмент).

Принадлежность каждого пользователя и ТС ОИ к той или иной ИС представлена в таблице 5.

Таблица 5 – Информационные системы, функционирующие на объекте информатизации

| № п/п | УО ТС | Должность | Роль пользователя | Роль ТС | Кабинет | Тип информации | Подключение к сторонним ИС | ИС |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|  | HD-010-01 | И.о. руководителя департамента – главный государственный инспектор по охране окружающей среды | Пользователь | АРМ пользователя | 406 | Общедоступная и служебная информация | - | - |
|  | HD-010-02 | Секретарь | Пользователь | АРМ пользователя | 405 | Информация ограниченного доступаОбщедоступная и служебная информация | АИС "Дело" | ИС "Дело" (пользовательский сегмент) |
|  | HD-010-03 | Главный бухгалтер | Пользователь | АРМ пользователя | 409 | ПДн "Работников" | - | ИС "Бухгалтерия и кадры" |
|  | HS-010-04 | Специалист – государственный инспектор по охране окружающей среды | Локальный администратор | АРМ, выполняющий серверную роль | 409 | ПДн "Работников"ПДн "Кандидатов" | - | ИС "Бухгалтерия и кадры" |
|  | HD-010-05 | Должность сокращена | Пользователь | АРМ пользователя | 409 | - | - | - |
|  | HD-010-06 | Главный специалист отдела учета финансов | Пользователь | АРМ пользователя | 409 | ПДн "Работников" |  | ИС "Бухгалтерия и кадры" |
|  | HD-010-07 | Первый заместитель руководителя департамента – заместитель главного государственного инспектора по охране окружающей среды | Пользователь | АРМ пользователя | 404 | ПДн "Нарушителей"Информация ограниченного доступа | ССТУ | ИС "Охрана объектов животного мира"ИС "Дело" (пользовательский сегмент) |
|  | HD-010-08 | Механик | Пользователь | АРМ пользователя | 402 | Общедоступная и служебная информация | - | - |
|  | HD-010-09 | Охотовед 1 категории – государственный инспектор по охране окружающей среды | Пользователь, модератор портала | АРМ пользователя | 402 | Общедоступная и служебная информация | - | Требования по защите АРМ выдвигаются оператором ИС "49gov.ru" |
|  | HD-010-10 | Консультант по государственным закупкам отдела воспроизводства объектов животного мира | Пользователь, представитель организации | АРМ пользователя | 402 | Общедоступная и служебная информация | zakupki.gov.ru | - |
|  | HD-010-11 | Ведущий специалист отдела воспроизводства объектов животного мира – государственный инспектор по охране окружающей среды | Пользователь, представитель организации | АРМ пользователя | 402 | Общедоступная и служебная информация | - | - |
|  | HD-010-12 | Ведущий специалист территориальной группы по г. Магадану и Ольскому району – государственный инспектор по охране окружающей среды | Пользователь | АРМ пользователя | 401 | ПДн "Нарушителей" | - | ИС "Охрана объектов животного мира" |
|  | HD-010-13 | Охотовед 2 категории – государственный инспектор по охране окружающей среды | Пользователь | АРМ пользователя | 401 | ПДн "Нарушителей" | - | ИС "Охрана объектов животного мира" |
|  | HD-010-14 | Начальник отдела воспроизводства объектов животного мира – старший государственный инспектор по охране окружающей среды | Пользователь | АРМ пользователя | 436 | ПДн "Охотпользователи" | - | ИС "Охотпользователи" |
|  | HD-010-15 | Государственный инспектор отдела воспроизводства объектов животного мира | Локальный администратор, пользователь, представитель организации | АРМ пользователя | 436 | Общедоступная и служебная информация | - | - |
|  | HD-010-16 | Специалист 1 категории отдела воспроизводства объектов животного мира – государственный инспектор по охране окружающей среды | Локальный администратор, пользователь | АРМ пользователя | 436 | ПДн "Нарушителей" | - | ИС "Охрана объектов животного мира" |
|  | HD-010-17 | Заместитель начальника отдела надзора, охраны и использования объектов животного мира и среды их обитания – руководитель территориальной группы по г. Магадану и Ольскому району – старший государственный инспектор по охране окружающей среды | Пользователь | АРМ пользователя | 435 | ПДн "Нарушителей" |  | ИС "Охрана объектов животного мира" |
|  | HD-010-18 | Специалист – государственный инспектор по охране окружающей среды | Модератор портала, пользователь, локальный администратор. | АРМ пользователя | 435 | Информация ограниченного доступа ПДн "Граждан"ПДн "Кандидатов" | 49gov.ruССТУГАС "Управление"torgi.gov.ru | ИС "Администраторы"Требования по защите АРМ выдвигаются оператором ИС "49gov.ru" |
|  | HD-010-19 | Начальник отдела надзора, охраны и использования объектов животного мира и среды их обитания – старший государственный инспектор по охране окружающей среды | Пользователь | АРМ пользователя | 417 | ПДн "Заявителей на обладание охотничьим билетом" | 49gov.ru | ИС "Охотпользователи" |
|  | HD-010-20 | Заместитель руководителя департамента – заместитель главного государственного инспектора по охране окружающей среды | Пользователь | АРМ пользователя | 417 | Информация ограниченного доступа | 49gov.ru | ИС "Дело" (пользовательский сегмент) |
|  | HD-010-21 | Ведущий специалист отдела воспроизводства объектов животного мира – государственный инспектор по охране окружающей среды | Пользователь, представитель организации | АРМ пользователя | 430 | ПДн "Заявителей на разрешение на добычу охотничьих ресурсов"ПДн "Заявителей на обладание охотничьим билетом" | СМЭВ | ИС "Охотпользователи" |
|  | HD-010-22 | Специалист – государственный инспектор по охране окружающей среды | Пользователь | АРМ пользователя | 430 | ПДн "Заявителей на разрешение на добычу охотничьих ресурсов"ПДн "Заявителей на обладание охотничьим билетом"ПДн "Нарушителей" | СМЭВ49gov.ru | ИС "Охотпользователи"ИС "Охрана объектов животного мира" |
|  | HD-010-23 | Главный специалист отдела правового, информационного и кадрового обеспечения | Модератор портала, пользователь | АРМ пользователя | 419 | ПДн "Кандидатов"ПДн "Работников" | АИС "Дело"СМЭВ49gov.ru | ИС "Бухгалтерия и кадры"Требования по защите АРМ выдвигаются оператором ИС "49gov.ru" |
| 1.
 | VS-010-01 | Специалист – государственный инспектор по охране окружающей среды | Оператор портала, пользователь, локальный администратор | Виртуальный сервер | ЦОД Миндор | Экземпляр АИС "ДЕЛО" | - | ИС "Дело" (пользовательский сегмент) |

# Выполнение требований к защите информации на момент обследования

Помещения, в которых расположены ТС ОИ, оборудованы пожарной сигнализацией. Ответственность за физическую охрану помещений возлагается на Арендодателя в лице ОГБУ "МОЭЦ". Здание не оборудовано системой контроля управления доступом. Пропускной режим отсутствует. Контроль доступа посторонних лиц в кабинеты ОИ в рабочие часы осуществляется работниками ОИ.

Расположение устройств отображения информации значительно затрудняет несанкционированный визуальный съем информации с экранов мониторов.

Работы по разработке, модернизации, монтажу, установке, наладке, ремонту и обслуживанию ИС ОИ и их элементов осуществляются сотрудником ОИ с привлечением (при необходимости) сторонней организации (далее – Обслуживающая организация) в соответствии с Федеральным законом №44-ФЗ от 05.04.2013.

Для передачи защищаемой информации по открытым каналам связи используются средства криптографической защиты информации – ViPNet Client, КриптоПро CSP, Континент-АП.

В качестве средства антивирусной защиты (далее - САЗ) информации применяется ПК "ESET NOD32 Antivirus". Антивирусные средства защиты установлены не на всех АРМ ОИ. Базы сигнатур САЗ обновляются регулярно с серверов компании разработчика.

Доступ к серверному сегменту ИС "Дело" предоставляется Министерством. ИС "Дело" не проходила процедуру оценки соответствия требованиям нормативно-правовых документов РФ.

На ОИ не разработаны организационно-распорядительные документы, регламентирующие защиту ПДн.

# Классификация информационных систем

Для всех выявленных ИС, которые являются негосударственными информационными системами, по решению оператора могут быть применены требования в соответствии с [7].

1. ИС "Бухгалтерия и кадры":
* в ИС обрабатываются иные и общедоступные категории персональных данных менее чем 100 000 субъектов персональных данных;
* все ОТСС ИС находятся в пределах РФ.
1. ИС "Охрана объектов животного мира":
* ИС создана в целях реализации полномочий органа исполнительной власти МО;
* ИС имеет объектовый масштаб, так как функционирует на базе государственного органа исполнительной власти МО;
* в ИС возможна обработка иных и общедоступных категорий персональных данных менее чем 100 000 субъектов персональных данных;
* в ИС возможна обработка служебной информации и информации ограниченного доступа;
* ОТСС ИС находятся в пределах РФ.

1. ИС "Охотпользователи":
* ИС создана в целях реализации полномочий органа исполнительной власти МО;
* ИС имеет объектовый масштаб, так как функционирует на базе государственного органа исполнительной власти МО;
* в ИС возможна обработка иных и общедоступных категорий персональных данных менее чем 100 000 субъектов персональных данных;
* в ИС возможна обработка служебной информации и информации ограниченного доступа;
* ОТСС ИС находятся в пределах РФ.
1. ИС "Администраторы":
* ИС создана в целях реализации полномочий сотрудников органа исполнительной власти МО;
* ИС имеет объектовый масштаб, так как функционирует на базе государственного органа исполнительной власти МО;
* в ИС возможна обработка служебной информации и информации ограниченного доступа;
* ОТСС ИС находятся в пределах РФ.
1. ИС "Дело" (пользовательский сегмент):
* ИС создана в целях реализации полномочий органа исполнительной власти МО;
* ИС создана в целях обеспечения обмена информацией ОИ, органов исполнительной власти МО, органов местного самоуправления МО, а также иных организаций, предприятий и учреждений разных форм собственности;
* ИС имеет региональный масштаб, так как она функционирует на территории МО и имеет сегменты в нескольких муниципальных образованиях, подведомственных и иных организациях;
* ИС является пользовательским сегментом региональной информационной системы "Дело";
* в ИС возможна обработка специальных, иных и общедоступных категорий персональных данных менее чем 100 000 субъектов персональных данных;
* в ИС возможна обработка служебной информации и информации ограниченного доступа;
* ОТСС ИС находятся в пределах РФ.

## Определение требуемого уровня защищенности персональных данных

### ИС "Бухгалтерия и кадры", ИС "Охрана объектов животного мира", ИС "Охотпользователи":

ИС предназначены для обработки иных и общедоступных категорий персональных данных.

В соответствии с документом [5] определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда. В настоящем документе приведены рекомендации по определению типа угроз безопасности персональных данных.

В соответствии с моделью угроз безопасности информации для ИС актуальны угрозы 3-го типа, так как для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

В соответствии с документом [5] для ИС необходимо обеспечить четвертые уровни защищенности (УЗ 4) персональных данных.

### ИС "Дело" (пользовательский сегмент)

В ИС возможна обработка специальных, иных и общедоступных категорий персональных данных.

В соответствии с документом [5] определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда. В настоящем документе приведены рекомендации по определению типа угроз безопасности персональных данных.

В соответствии с частной моделью угроз безопасности информации для ИС актуальны угрозы 3-го типа, так как для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

В соответствии с документом [5] для ИС необходимо обеспечить третий уровень защищенности (УЗ 3) персональных данных.

## Определение класса защищенности информационной системы

### ИС "Дело" (пользовательский сегмент), ИС "Охотпользователи", ИС "Охрана объектов животного мира"

ИС не являются государственными информационными системами, однако по решению оператора, а также для выполнения требований сторонних информационных систем, к которым осуществляется подключение, к ней могут быть применены требования в соответствии с [7].

В соответствии с [7], класс защищенности государственной информационной системы определяется в зависимости от уровня значимости информации, обрабатываемой в этой информационной системе, и масштаба информационной системы. Уровень значимости информации определяется степенью возможного ущерба для обладателя информации и (или) оператора от нарушения конфиденциальности, целостности или доступности информации.

Учитывая, что степень возможного ущерба определяется обладателем информации и (или) оператором самостоятельно экспертным или иными методами, в настоящем документе приведены рекомендации по определению степени возможного ущерба.

Классификационные признаки ИС представлены в таблице 6.

Таблица 6 – Классификационные признаки ИС "Дело", ИС "Охрана объектов животного мира", ИС "Охотпользователи"

| № п/п | Характеристика, необходимая для определения уровня значимости | Возможность нанесения ущерба при нарушении заданных характеристик безопасности |
| --- | --- | --- |
| Целостность | Доступность | Конфиденциальность |
| 1 | 2 | 3 | 4 | 5 |
|  | Последствия в социальной области деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Низкая |
|  | Последствия в политической области деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Нет |
|  | Последствия в международной области деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Нет |
|  | Последствия в экономической области деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Нет |
|  | Последствия в финансовой области деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Нет |
|  | Последствия в иных областях деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Низкая |
|  | Невозможность выполнения оператором (владельцем информации) своих функций  | Нет | Нет | Нет |
|  | Невозможность выполнения оператором (владельцем информации) хотя бы одной из возложенных функций | Нет | Нет | Нет |
|  | Выполнение возложенных на оператора (владельца информации) функций с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств | Да (Низкая) | Да (Низкая) | Нет |
| Итог: | Низкая | Низкая | Низкая |

Таким образом, в соответствии с [7], при нарушении заданных характеристик безопасности, обрабатываемых в ИС:

Уровень значимости = [(конфиденциальность, низкая) (целостность, низкая) (доступность, низкая)] = 3.

ИС "Охрана объектов животного мира", ИС "Охотпользователи" имеют объектовый масштаб.

ИС "Дело" имеет региональный масштаб.

В соответствии с приложением 1 документа [7], для ИС необходимо установить третий класс защищенности информационной системы – К 3.

### ИС "Администраторы"

ИС не является государственной информационной системой. В ИС осуществляется обработка информации ограниченного доступа (конфигурационные файлы СрЗИ, объектов поддерживающей инфраструктуры; аутентификационная информация и др.). Для ИС необходимо обеспечить требования в соответствии с [7].

В соответствии с [7] класс защищенности государственной информационной системы определяется в зависимости от уровня значимости информации, обрабатываемой в этой информационной системе, и масштаба информационной системы. Уровень значимости информации определяется степенью возможного ущерба для обладателя информации и (или) оператора от нарушения конфиденциальности, целостности или доступности информации.

Учитывая, что степень возможного ущерба определяется обладателем информации и (или) оператором самостоятельно экспертным или иными методами, в настоящем документе приведены рекомендации по определению степени возможного ущерба.

Классификационные признаки ИС представлены в таблице 7.

Таблица 7 – Классификационные признаки ИС "Администраторы"

| № п/п | Характеристика, необходимая для определения уровня значимости | Возможность нанесения ущерба при нарушении заданных характеристик безопасности |
| --- | --- | --- |
| Целостность | Доступность | Конфиденциальность |
| 1 | 2 | 3 | 4 | 5 |
|  | Последствия в социальной области деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Нет |
|  | Последствия в политической области деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Нет |
|  | Последствия в международной области деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Нет |
|  | Последствия в экономической области деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Нет |
|  | Последствия в финансовой области деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Нет |
|  | Последствия в иных областях деятельности оператора (владельца информации) |
|  | существенные негативные | Нет | Нет | Нет |
|  | умеренные негативные | Нет | Нет | Нет |
|  | незначительные негативные | Нет | Нет | Нет |
|  | Невозможность выполнения оператором (владельцем информации) своих функций  | Нет | Нет | Нет |
|  | Невозможность выполнения оператором (владельцем информации) хотя бы одной из возложенных функций | Нет | Нет | Нет |
|  | Выполнение возложенных на оператора (владельца информации) функций с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств | Да (Низкая) | Да (Низкая) | Да (Низкая) |
| Итог: | Низкая | Низкая | Низкая |

Таким образом, в соответствии с [7], при нарушении заданных характеристик безопасности, обрабатываемых в ИС:

Уровень значимости = [(конфиденциальность, низкая) (целостность, низкая) (доступность, низкая)] = 3.

ИС имеет объектовый масштаб.

В соответствии с приложением 1 документа [7], для ИС необходимо установить третий класс защищенности информационной системы – К 3.

# Состав мер защиты информации

Для ИС третьего, четвертого уровня защищённости персональных данных и третьего класса защищенности государственных информационных систем базовый набор мер защиты информации установлен в таблице 8.

Таблица 8 – Базовый набор мер

| УО меры | Меры защиты информации в информационных системах | УЗ 4 | УЗ 3 | К 3 |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| ИАФ | I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ): |  |  |  |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора  | + | + | + |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов  | + | + | + |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации  | + | + | + |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации  | + | + | + |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)  | + | + | + |
| УПД | II. Управление доступом субъектов доступа к объектам доступа (УПД): |  |  |  |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей  | + | + | + |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа  | + | + | + |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | + | + | - |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы  | + | + | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы  | + | + | + |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | + | + |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу  | - | + | + |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | - | + | + |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | + | + | + |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + | + | + |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + | + | + |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + | + | + |
| ОПС | III. Ограничение программной среды (ОПС): |  |  |  |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | - | - | + |
| ЗНИ | IV. Защита машинных носителей персональных данных (ЗНИ): |  |  |  |
| ЗНИ.1 | Учет машинных носителей персональных данных | - | - | + |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных | - | - | + |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания | - | + | + |
| РСБ | V. Регистрация событий безопасности (РСБ): |  |  |  |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | + | + |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | + | + |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | + | + |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти | - | - | + |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | - | - | + |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе | - | - | + |
| РСБ.7 | Защита информации о событиях безопасности | + | + | + |
| АВЗ | VI. Антивирусная защита (АВЗ): |  |  |  |
| АВЗ.1 | Реализация антивирусной защиты | + | + | + |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов)  | + | + | + |
| АНЗ | VIII. Контроль (анализ) защищенности персональных данных (АНЗ): |  |  |  |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | - | + | + |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | + | + |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | - | + | + |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | - | + | + |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе | - | + | + |
| ОЦЛ | IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ): |  |  |  |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | - | - | + |
| ЗСВ | XI. Защита среды виртуализации (ЗСВ): |  |  |  |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | + | + | + |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | + | + |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре | - | + | + |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре | - | - | + |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей  | - | + | - |
| ЗТС | XII. Защита технических средств (ЗТС): |  |  |  |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования | - | - | + |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены | + | + | + |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр  | + | + | + |
| ЗИС | XIII. Защита информационной системы, ее средств, систем связи и передачи данных (3ИС): |  |  |  |
| ЗИС.3 | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | + | + | + |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств | - | - | + |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе | - | + | + |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе | - | - | + |
|  | XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)  |  |  |  |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных  |  | + |  |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных  |  | + |  |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных  |  | + |  |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных  |  | + |  |

Выводы и рекомендации

Проведенный аудит показал:

1. Во всех выделенных ИС ОИ ведется обработка иных и общедоступных категорий персональных данных.
2. В некоторых ИС ОИ ведется обработка специальных категорий персональных данных.
3. ИС "Бухгалтерия и кадры":

Для ИС необходимо обеспечить четвертый уровень защищенности персональных данных (УЗ 4).

1. ИС "Охрана объектов животного мира":

Для ИС необходимо обеспечить четвертый уровень защищенности персональных данных (УЗ 4).

ИС должна соответствовать требованиям, предъявляемым к государственным информационным системам третьего класса защищенности (К 3).

1. ИС "Охотпользователи":

Для ИС необходимо обеспечить четвертый уровень защищенности персональных данных (УЗ 4).

ИС должна соответствовать требованиям, предъявляемым к государственным информационным системам третьего класса защищенности (К 3).

1. ИС "Администраторы":

ИС должна соответствовать требованиям, предъявляемым к государственным информационным системам третьего класса защищенности (К 3).

1. ИС "Дело" (пользовательский сегмент):

ИС является пользовательским сегментом информационной системы "Дело" министерства дорожного хозяйства, транспорта и связи МО.

Для ИС необходимо обеспечить третий уровень защищенности персональных данных (УЗ 3).

В связи с перспективой развития и возможность обработки в ИС информации конфиденциального характера, ИС должна соответствовать требованиям, предъявляемым к государственным информационным системам третьего класса защищенности (К 3).

1. Меры защиты информации, применяемые в ИС ОИ, недостаточны для обеспечения защиты информации.
2. Для обеспечения защиты информации необходимо разработать технический проект системы защиты информации в информационных системах ОИ.
3. В ИС ОИ необходимо произвести внедрение системы защиты информации, с учетом технического проекта системы защиты информации в информационных системах ОИ.
4. Рекомендуется вывести АРМ HD-010-05 из эксплуатации, в связи с прекращением обработки информации на нем и сокращения штатной единицы ОИ.
5. Информация по общему количеству ИС, АРМ и серверов на ОИ, требующих защиты, представлена в таблице 9.

Таблица 9 – Суммарные результаты аудита

| № п/п | Наименование ИС | Тип ИС (ИС[[1]](#footnote-1)/ГИС/ИСПДн) | Классификация ИС | Количество ОТСС |
| --- | --- | --- | --- | --- |
| В соответствии с [7] | В соответствии с [8] | АРМ | Серверы |
| 1 | 2 | 3 | 5 | 4 | 6 | 7 |
|  | ИС "Бухгалтерия и кадры" | ИСПДн |  | УЗ 4 | 4 | - |
|  | ИС "Охрана объектов животного мира" | ИС | К 3 | УЗ 4 | 6 | - |
|  | ИС "Охотпользователи" | ИС | К 3 | УЗ 4 | 4 | - |
|  | ИС "Администраторы" | ИС | К 3 | - | 1 | - |
|  | ИС "Дело" | ИС | К 3 | УЗ 3 | 3 | 1 |
| Итого защищаемых ТС: | 16 | 1 |

|  |  |  |
| --- | --- | --- |
| Заместитель начальника ОП ООО "МАСКОМ-Техлайн" |  | К. В. Котов |
|  |  |  |
| Ведущий инженер-проектировщик ОПООО "МАСКОМ-Техлайн" |  | И. Д. Клименко |

1. информационная система, которая не является государственной информационной системой, но по решению оператора к ней предъявляются требования в соответствии с [7] [↑](#footnote-ref-1)