

УТВЕРЖДАЮ

Директор

ООО Центр защиты информации

«Эгида»

И.У. Кулдыбаева

2015 г.



ЗАКЛЮЧЕНИЕ

по результатам аттестационных испытаний

Информационной системы персональных данных
«Находка-ЗАГС»

отдела ЗАГС администрации Добрянского муниципального района Пермского
края

г. Добрянка, ул. Советская, 66, отдел ЗАГС

2015 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Аттестационная комиссия ООО ЦЗИ «Эгида», Лицензия ФСТЭК России № 2712 (от 30.09.2015) в составе:

Кулдыбаева И.У. – директор ООО ЦЗИ «Эгида», ответственная за проведение аттестационных испытаний на соответствие организационно-техническим требованиям по защите информации, председатель аттестационной комиссии;

Волков Н.В. – ответственный за проведение аттестационных испытаний на соответствие требованиям по защите информации от НСД, требованиям по защите информации от утечки по каналам ПЭМИН, инженер по защите информации ООО ЦЗИ «Эгида».

провела аттестационные испытания объекта информатизации – информационная система персональных данных «Находка-ЗАГС» отдела ЗАГС администрации Добрянского муниципального района Пермского края, расположенной по адресу: Пермский край, г. Добрянка, ул. Советская, 66 (далее ИСПДн) в соответствии с «Программой и методикой проведения аттестационных испытаний» (Уч.№ 60 К от 02.12.2015 г.).

Результаты аттестационных испытаний приведены в протоколе по направлению:

– Испытания объекта на соответствие требованиям по защите информации от несанкционированного доступа (уч. № уч. № 61 К от 04.12.2015 г.).

1.2 Аттестационные испытания проведены в рамках добровольной аттестации информационных систем персональных данных в соответствии с «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации» (СТР-К), а также других действующих нормативно-методических документов ФСТЭК (Гостехкомиссии России).

1.3 Заявитель аттестационных испытаний объекта – администрация Добрянского муниципального района.

2. ЦЕЛЬ, ОБЪЕКТЫ И УСЛОВИЯ ИСПЫТАНИЙ

Целью аттестации является определение соответствия уровня защищенности объекта информатизации требованиям нормативных документов Российской Федерации по защите информации.

Объект аттестационных испытаний – Информационная система персональных данных «Находка-ЗАГС».

Состав основных технических средств и систем (ОТСС) объекта приведен в таблице 1. Полное описание объекта, состав вспомогательных технических средств и систем (ВТСС), приведены в «Техническом паспорте» (от 02.12.2015 г.).

Таблица 1 – Состав ОТСС

№ п/п	Тип ОТСС	Заводской номер	Сведения по сертификации, специследованиям и специпроверкам
1	ПЭВМ №1 – АРМ начальника Отдела ЗАГС в составе:		
1.1	Системный блок	S/N: 636190002	-
1.2	Монитор ACER AL1916WD	S/N: ETL8608130802021074 2D0	-
1.3	Клавиатура Microsoft	0200704681932	-
1.4	Манипулятор Genius	X76089902674	-
1.5	Телефон Panasonic PNLC1042	S/N: 4EAQA013459	-
1.6	Принтер HP LaserJet P1102	S/N: VNC6B52675	-
1.7	МФУ CANON F159502	S/N: HBY65447	-
1.8	Принтер EPSON B251A	S/N: GSET031156	-
1.9	ИБП APC BE525-RS	S/N: BB0644003902	-
1.10	Rutoken	0821580387	-
2	ПЭВМ №2 – АРМ консультанта Отдела ЗАГС (PC-1) в составе:		
2.1	Системный блок	S/N: 636190001	-
2.2	Монитор ЛЮС 919Sa2	S/N: Q1099JA001382	-
2.3	Клавиатура Genius K639	S/N: ZM4C39063701	-
2.4	Манипулятор Logitech	S/N: LZE30450290	-
2.5	Телефон Panasonic PNLC1042	S/N: 4DAQA001598	-
2.6	Принтер EPSON LQ-690	S/N: LKWH011192	-
2.7	Принтер CANON L11121E	S/N: LPKA759066	-
2.8	Rutoken	0821580050	-
3	ПЭВМ №3 – АРМ ведущего специалиста Отдела ЗАГС (comp 02) в составе:		
3.1	Системный блок	Инв. № 011010410245	-
3.2	Монитор PHILIPS 170S6FS/00	S/N: BZ000536315957	-
3.3	Клавиатура AQUARIUS SK-1689	S/N: C0306098870	-
3.4	Манипулятор Genius GM-080025	S/N: X4K89455102186	-
3.5	Принтер HP LaserJet 1020	S/N: CNCK674682	-
3.6	Телефон Panasonic PNLC1042	S/N: 4EAQA013459	-
3.7	ИБП APC SUA750I	Инв. № 016161630773	-
3.8	Rutoken	0821582181	-
4	ПЭВМ №4 – АРМ ведущего специалиста Отдела ЗАГС (PC-02) в составе:		
4.1	Монитор LG Flatron L1919S-BF	S/N: 609NTPC2Z240	-
4.2	Принтер HP LaserJet P2035	Инв. № 01010411304	-
4.3	Системный блок	Инв. № 0116161631232	-

4.4	Телефон Panasonic PNLC1042	S/N: 4FCQA002562	-
4.5	Телефон/факс Panasonic KX-FT908RU	S/N: 51AQA050945	-
4.6	Манипулятор OKLICK	S/N: 50621509005	-
4.7	Клавиатура OKLICK	S/N: 39217070900509	-
4.8	ИБП APC BK475-RS	S/N: BB0329016086	-
4.9	Rutoken	0821581378	
5	Системный блок (сервер БДн)	S/N: GB874417JN	
6	ИБП UPC-Back UPS ES525	S/N: 8B0748R44585	
7	Коммутатор D-LINK	S/N: QB3A1B1015608	

В ходе аттестационных испытаний проводились следующие мероприятия:

- анализ полноты исходных данных, проверка их соответствия реальным условиям размещения, монтажа и эксплуатации технических средств ИСПДн;
- исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки информации средств;
- проверка состояния организации работ и выполнения организационно – технических требований по защите информации, оценка правильности определения уровня защищенности, оценка полноты разработки организационно – распорядительной, проектной и эксплуатационной документации, оценка уровня подготовки кадров и распределения ответственности за выполнение требований по обеспечению безопасности информации;
- проверка ИСПДн на соответствие требованиям по защите информации от НСД;
- подготовка отчетной документации.

При проведении аттестационных испытаний применялись следующие методы проверок и испытаний:

- экспертно-документальный метод;
- проверка функций или комплекса функций защиты информации от НСД путем пробного запуска средств защиты информации от НСД и наблюдение за их выполнением;
- проверка соответствия применяемых параметров настройки элементов системы защиты информации требованиям безопасности информации;
- проверка подсистем защиты информации от НСД, целостности применяемых СЗИ от НСД, в том числе с использованием специальных средств контроля эффективности защиты информации.

В ходе проведения аттестационных испытаний использовались следующие руководящие и нормативно-технические документы:

- Постановление Правительства №1119 от 01 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие положения.
- ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методика аттестационных испытаний.
- Руководящий документ. Защита от НСД к информации. Термины и определения. Гостехкомиссии России, 1992 г.
- Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации. Гостехкомиссии России, 1992 г.

– Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992;

– Руководящий документ РД 50-34.698-90. Автоматизированные системы. Требования к содержанию документов.. Гостехкомиссия России, от 1 января 1992 г.

– Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1992 г

– Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30.08.2002 г., № 282.

– Приказ ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

При проведении аттестационных испытаний использовались следующие средства контроля защищенности от НСД к информации:

Таблица 2

Используемые средства	Сведения о сертификате, знаке соответствия
Программа фиксации и контроля исходного программного комплекса «ФИКС 2.0.2»	Сертификат ФСТЭК России № 1548, действителен до 15.01.2017 г., СЗЗ № А 270541

3. ПОРЯДОК ПРОВЕДЕНИЯ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

Для проведения испытаний аттестационной комиссии предъявлены следующие исходные данные и документация (см. Таблица 3):

Таблица 3

№ п.п.	Предоставлено Заявителем	Рег. номер
1.	Распоряжение о назначении комиссии по классификации ИСПДн	№ от 02.12.2015
2.	Положение по организации и порядку проведения работ по обеспечению безопасности персональных данных субъектов персональных данных	от 02.12.2015
3.	Распоряжение О назначении сотрудников, ответственных за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных	от 02.12.2015
4.	Порядок доступа в помещения, в которых ведется обработка персональных данных	от 02.12.2015
5.	Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами	от 02.12.2015
6.	Правила рассмотрения запросов субъектов персональных данных или их представителей	от 02.12.2015
7.	Перечень персональных данных, обрабатываемых в отделе ЗАГС администрации Добрянского муниципального района Пермского края, в связи с осуществлением государственных функций и предоставлением государственных услуг	от 02.12.2015
8.	Перечень информационных систем персональных данных отдела ЗАГС администрации Добрянского муниципального района Пермского края	от 02.12.2015
9.	Перечень должностей работников отдела ЗАГС администрации Добрянского муниципального района Пермского края, осуществляющих обработку персональных данных либо имеющих доступ к персональным данным	от 02.12.2015
10.	Должностная инструкция ответственного за организацию обработки персональных данных	от 02.12.2015
11.	Инструкция по организации антивирусной защиты информационных систем персональных данных	от 02.12.2015
12.	Инструкция по организации парольной защиты информационных систем персональных данных	от 02.12.2015
13.	Инструкция по организации учета, использования и уничтожения машинных носителей персональных данных отдела ЗАГС администрации Добрянского муниципального района Пермского края	от 02.12.2015
14.	Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных	от 02.12.2015

№ п.п.	Предоставлено Заявителем	Рег. номер
15.	Инструкция по организации учета, использования и уничтожения машинных носителей персональных данных	от 02.12.2015
16.	Инструкция администратора информационной безопасности ИСПДн «Находка-ЗАГС»	от 02.12.2015
17.	Инструкция пользователя ИСПДн «Находка-ЗАГС»	от 02.12.2015
18.	Матрица доступа пользователей к информационным и программным ресурсам ИСПДн «Находка-ЗАГС»	от 02.12.2015
19.	Акт определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных «Находка-ЗАГС»	от 02.12.2015
20.	Акт определения класса защищенности информационной системы «Находка-ЗАГС»	от 02.12.2015
21.	Модель нарушителя (модель угроз верхнего уровня) для информационной системы персональных данных Отдела ЗАГС администрации Добрянского муниципального района Пермского края «Находка-ЗАГС»	Уч. № 56 К от 2.12.2015
22.	Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Находка-ЗАГС»	Уч. № 57 К от 2.12.2015
23.	Требования к системе защиты персональных данных в информационной системе персональных данных «Находка-ЗАГС»	Уч. № 58 К от 2.12.2015
24.	Технический паспорт ИСПДн «Находка-ЗАГС»	Уч. № 59 К от 2.12.2015
25.	Описание технологического процесса обработки конфиденциальной информации в ИСПДн	от 02.12.2015
26.	Акты установки СЗИ от НСД	от 01.12.2015 г.
27.	Типовое обязательство о неразглашении сведений конфиденциального характера	-
28.	Журнал учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных	-
29.	Журнал периодического тестирования средств защиты информации	-
30.	Журнал учета машинных носителей информации в ИСПДн	-
31.	Журнал учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн	-
32.	Журнал учета процедуры резервного копирования	-
33.	Журнал учета средств защиты информации, эксплуатационной и технической документации к ним	-

Аттестационные испытания были проведены в следующем порядке:

- проанализированы и оценены представленные исходные данные и документация по защите информации на объекте информатизации;
- осуществлена проверка соответствия представленных исходных данных реальным условиям размещения, монтажа средств вычислительной техники и эксплуатации средств

защиты информации, рассмотрен технологический процесс обработки и хранения информации, составляющей конфиденциальную информацию, проанализированы информационные потоки, определен состав и структура использованных для обработки конфиденциальной информации технических и программных средств вычислительной техники;

– проверено состояние организации работ и выполнения организационно-технических требований по защите информации, наличие организационно-распорядительной, проектной и эксплуатационной документации, ее соответствие требованиям государственной и отраслевой нормативной документации по безопасности информации, подготовки кадров и распределения ответственности за выполнение требований по обеспечению безопасности информации;

– проведены комплексные испытания ИСПДн на соответствие требованиям по защите информации от НСД;

– подготовлена отчетная документация и настоящее заключение по результатам аттестационных испытаний.

4. РЕЗУЛЬТАТЫ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

В результате проверки организации работ и готовности к функционированию объекта информатизации на соответствие требованиям безопасности информации установлено:

1. В соответствии с разделом Постановлением Правительства Российской Федерации №1119 от 1 ноября 2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» аттестуемому объекту информатизации присвоен 2 уровень защищенности.

2. В соответствии с Приказом ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» аттестуемому объекту информатизации присвоен 3 класс защищенности.

3. В соответствии с п. 27 Приказа ФСТЭК России №17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для обеспечения требуемого уровня защищенности персональных данных необходимо обеспечить выполнение требований по 2 классу защищенности.

4. Объект информатизации размещен на первом этаже административного здания-пристройка к жилому зданию. Границей контролируемой зоны являются ограждающие конструкции помещения Отдела ЗАГС. Минимальное расстояние от ОТСС до границы контролируемой зоны, в которой расположен объект, соответствует указанному в плане границы контролируемой зоны и составляет не менее 1,5 м.

5. Визуальный просмотр обрабатываемой на объекте информатизации посторонними лицами невозможен.

6. На объект информатизации разработан технический паспорт, соответствующий требованиям СТР-К. Состав ОТСС и ВТСС, установленных на объекте, соответствует указанному в техническом паспорте.

7. Определен технологический процесс обработки персональных данных.

8. Требования по защите информации от несанкционированного доступа по 2 классу защищенности выполнены.

9. Помещение, в котором установлены ОТСС и хранятся машинные носители информации, удовлетворяет требованиям СТР-К и признано годным для работы с

документами и машинными носителями информации в рабочее время и хранения документов и машинных носителей информации в нерабочее время.

10. Доступ посторонних лиц в помещение ограничен и без контроля невозможен. В нерабочее время помещение запирается на ключ, здание находится под охраной.

11. ИСПДн не имеет выхода в международные телекоммуникационные сети передачи данных.

12. Лица, ответственные за эксплуатацию и выполнение требований по защите информации, обрабатываемой на объекте, определены распоряжением главы администрации.


13. На объекте имеются инструкции, на основании которых осуществляется работа пользователей, администратора безопасности ИСПДн.

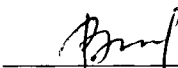
5. ЗАКЛЮЧЕНИЕ

Учитывая вышеизложенное, комиссия считает, что реализованные средства и меры защиты на объекте информатизации Информационная система персональных данных «Находка-ЗАГС» отдела ЗАГС администрации Добрянского муниципального района Пермского края, расположенной по адресу: Пермский край, г. Добрянка, ул. Советская, 66, достаточны и соответствуют требованиям действующих нормативных документов по безопасности информации, предъявляемых к информационным системам персональных данных 2 класса защищенности. На аттестуемый объект информатизации возможна выдача «Аттестата соответствия» на право обработки конфиденциальной информации сроком на 3 года.

Периодический контроль эффективности защиты должен осуществляться не менее одного раза в год.

Члены комиссии

 И.У. Кулдыбаева

 Н.В. Волков