Экз. № 1

**АКТ**
**проверки выполнения организационных и технических мер по обеспечению безопасности персональных данных при обработке персональных данных в информационных системах персональных данных казенного учреждения Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа»**

27.07.2017 г. Воронеж

Комиссией УФСБ России по Воронежской области в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон), на основании Плана государственного контроля на 2017 год и распоряжения от 12.07.2017 № 8/250нс, в период с 17 по 27 июля 2017 года проведена плановая выездная проверка выполнения организационных и технических мер по обеспечению безопасности персональных данных при обработке персональных данных в информационных системах персональных данных (далее – ИСПДн) казенного учреждения Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа» (далее – Учреждение, Управление), расположенного по адресу: г. Воронеж, ул. Никитинская, 8а.

Кроме Управления проверке были подвергнуты следующие территориально удаленные подразделения:

- отдел по предоставлению жилищных субсидий (ул. Березовая роща, 68);
- отдел социального обслуживания на дому (ул. Орджоникидзе, 3);
- отдел приема граждан (ул. 3 Интернационала, 31).

Контроль за выполнением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн Учреждения сотрудниками УФСБ России по Воронежской области ранее не проводился.

В соответствии с Законом проверка осуществлялась без ознакомления с персональными данными (ПДн), обрабатываемыми в информационных системах Учреждения.

На момент проверки информация, содержащая сведения, составляющие государственную тайну, в ИСПДн Управления не обрабатывалась.

## 1. Информационные системы персональных данных. Организация криптографической защиты информации

Уведомление об обработке ПДн в Учреждении установленным порядком было направлено в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Воронежской области в марте 2015 года (исх. № 01/1319 от 12.03.2015).

В ходе работы комиссии были уточнены сведения по используемым в Учреждении средствам криптографической защиты (СКЗИ). Для внесения необходимых изменений в реестр операторов, осуществляющих обработку персональных данных, в надзорный орган направлено информационное письмо № 1182724 от 18.07.2017.

Приказом директора Учреждения от 17.10.2016 № 183/ОД «Об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в казенном учреждении Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа» утвержден перечень ИСПДн, используемых в Управлении:

- Единая информационная система «Электронный социальный регистр населения»;

- Информационная система «1С:Предприятие».

Управление подведомственно департаменту социальной защиты населения Воронежской области (далее – Департамент). В соответствии с приказом головной организации от 12.04.2016 № 711/ОД в Департаменте и подведомственных учреждениях (органах социальной защиты Воронежской области) функционирует государственная ИСПДн «Единая информационная система персонифицированного учета граждан в органах социальной защиты Воронежской области» (далее - ЕИС). В связи с вышеизложенным считаем, что перечень ИСПДн, функционирующих в Управлении, требуется переработать, включив в него корректное наименование ЕИС.

ЕИС предназначена для автоматизации процессов принятия решений и предоставления мер социальной поддержки населения путем формирования и использования единой базы данных в масштабах Воронежской области, содержащей комплексную информацию о лицах, нуждающихся в социальном обеспечении и (или) социальном обслуживании.

В качестве средств криптографической защиты информации и межсетевого экранирования на периферийных серверных сегментах ЕИС используются программно-аппаратные комплексы VipNet Coordinator HW100C (далее – ПАК) Один из ПАК размещен в кабинете № 6 основного административного здания Управления (ул. Никитинская, 8а), второй – в отделе предоставления жилищных субсидий (ул. Березовая роща, 68). Сертификат соответствия ФСБ России комиссии представлен (СФ/124-2981, действителен до 14.11.2019).

Для размещения заказов на электронных торговых площадках используется СКЗИ «КриптоПро CSP» версии 4.0 (сертификат соответствия СФ/114-3009, действителен до 31.12.2018). При указанном взаимодействии персональные данные не обрабатываются.

В целях обеспечения целостности и авторства электронных документов при взаимодействии Учреждения с УФК по Воронежской области на момент начала проверки использовалось СКЗИ «КриптоПро CSP» версии 3.6 (сборка 6497). При указанном взаимодействии персональные данные также не обрабатываются. Вместе с тем отмечаем, что сертификат соответствия данного СКЗИ окончил свое действие 31.12.2016. В ходе работы комиссии от УФК по Воронежской области получен дистрибутив «КриптоПро CSP» версии 3.6.1, администратором

информационных систем на соответствующее АРМ произведена инсталляция сертифицированной версии программного продукта.

Лицензии на право использования средств криптозащиты комиссии предоставлены.

В ходе проверки было выявлено подключение к АРМ (инв. № 1043358) с установленным СКЗИ «КриптоПро CSP» Wi-Fi адаптера D-Link, обеспечивающего выход в сеть международного информационного обмена Интернет, что является нарушением требований эксплуатационной документации (раздел 12 ЖТЯИ.0050-02 90 02). По требованию комиссии Wi-Fi адаптер был отключен, соответствующее программное обеспечение деинсталлировано.

Правом электронной подписи (далее – ЭП) документов в Управлении наделено 9 сотрудников. Соответствующие распорядительные документы представлены. Выдача машинных носителей с ключевой информацией осуществляется под расписку должностных лиц в Журнале учета ключевых носителей электронной подписи. Хранение машинных носителей ЭП осуществляется в условиях, исключающих несанкционированный доступ.

Технические и профилактические работы на автоматизированных рабочих местах, входящих в состав ИСПДн, проводит программист общего отдела Управления.

До настоящего времени аттестация государственной информационной системы персональных данных по требованиям безопасности информации не проводилась (п. 17 приказа ФСТЭК России от 11.02.2013 № 17).

Рекомендации:

1. С сотрудниками, допущенными к работе с СКЗИ, провести инструктаж по соблюдению требований эксплуатационной документации для конкретных типов криптосредств.

2. Используемые в Учреждении СКЗИ эксплуатировать в строгом соответствии с требованиями соответствующей документации.

## 2. Организация работ по обеспечению безопасности персональных данных, функционирования СКЗИ

В целях обеспечения безопасности ПДн в Учреждении разработаны необходимые организационно-распорядительные документы по защите информации, содержащей персональные данные, в том числе:

1. Приказ директора Учреждения от 17.10.2016 № 182/ОД «О комиссии казенного учреждения Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа» по обеспечению безопасности персональных данных» (с изменениями, внесенными приказом от 01.06.2017 № 78/ОД). Данным приказом утверждены:

- Положение о комиссии казенного учреждения Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа» по обеспечению безопасности персональных данных»;
- Состав комиссии казенного учреждения Воронежской области

«Управление социальной защиты населения Центрального района г. Воронежа» по обеспечению безопасности персональных данных».

2. Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в казенном учреждении Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа» (утверждено приказом директора Учреждения от 17.10.2016 № 183/ОД).

3. Приказ директора Учреждения от 10.11.2016 № 202/ОД «О разрешительной системе доступа к информационным системам персональных данных казенного учреждения Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа».

4. Приказ директора Учреждения от 13.06.2017 № 84/ОД, на основании которого:

- утвержден список ответственных за обработку персональных данных при работе с «Единой системой персонифицированного учета граждан в органах социальной защиты населения Воронежской области» (ЕИС);
- определены границы контролируемой зоны объекта информатизации – сегмента ЕИС;
- утверждена схема границ контролируемых зон объектов информатизации.

Приказом директора Учреждения от 07.04.2016 № 78/ОД ответственным за обеспечение безопасности персональных данных при их обработке в ИСПДн назначена первый заместитель директора Фатеева Наталья Васильевна. В соответствии с приказом от 01.06.2017 № 79/ОД обязанности по организации работ по обеспечению безопасности персональных данных и поддержанию достигнутого уровня защиты персональных данных на этапах эксплуатации ИСПДн возложены на заместителя начальника отдела социальных выплат и администрирования баз данных Терещенко Ирину Анатольевну.

Работа по защите информации в Управлении регламентируется также следующими документами:

- Инструкцией по организации учета, хранения и работы с материальными носителями информации ограниченного доступа, в том числе с машинными носителями информации казенного учреждения Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа»;
- Инструкцией администратора безопасности информационных систем персональных данных казенного учреждения Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа»;
- Инструкцией пользователя информационных систем персональных данных казенного учреждения Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа».

Сотрудники, допущенные к обработке персональных данных и являющиеся пользователями СКЗИ, с перечисленными документами ознакомлены под роспись, обязательства о неразглашении персональных данных имеются.

В Учреждении разработан и 05.06.2017 утвержден директором «План проведения контроля состояния обеспечения безопасности персональных данных в КУВО «УСЗН Центрального района г. Воронежа». Мероприятия, включенные в план, носят актуальный характер. Вместе с тем отмечаем, что

отметки о выполнении мероприятий ответственным сотрудником своевременно не проставляются.

В ходе работы комиссии в Учреждении разработана частная модель угроз безопасности персональных данных, обрабатываемых в ЕИС. При подготовке указанного документа за основу были взяты положения модели угроз Департамента. Построение частной модели угроз Учреждения выполнено в соответствии с методическими документами ФСТЭК России и ФСБ России. На основании сформированной в модели угроз совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, следует, что для эксплуатируемой ЕИС актуальными являются классы угроз, не связанные с наличием НДВ в системном и прикладном ПО ИСПДн, определен минимальный класс применяемых СКЗИ – КС2. Класс используемых в ЕИС криптосредств предъявляемым требованиям соответствует.

Учет несъемных машинных носителей информации, содержащей персональные данные (далее – МНПДн), осуществляется в соответствующем журнале. Вместе с тем комиссия отмечает, что на момент начала проверки отдельные МНПДн учтены не были. В ходе работы комиссии указанный недостаток устранен, МНПДн учтены установленным порядком.

Для реализации антивирусной защиты в ИСПДн используется лицензионное программное средство «Kaspersky Endpoint Security 10 для Windows», сертифицированное ФСБ России. Обновление антивирусных баз производится регулярно. Вместе с тем в ходе работы комиссии было выяснено, что на АРМ сотрудников отдела социального обслуживания на дому (ул. Орджоникидзе, 3), используемых для обработки ПДн, средства антивирусной защиты установлены не были. Кроме того, сотрудники отдела для обработки персональных данных использовали неучтенные (личные) флэш-накопители. В ходе работы комиссии администратором информационных систем на данных АРМ установлены программные средства антивирусной защиты «Kaspersky Endpoint Security 10 для Windows», зарегистрированные служебные флэш-накопители выданы ответственным сотрудникам под расписку в соответствующем журнале.

Отмечаем, что в нарушение требований, предъявляемых к парольной защите, отдельные сотрудники Учреждения хранили значение личного пароля для доступа в ИСПДн на материальных носителях (на листе бумаги, в блокноте). В ходе работы комиссии произведена внеплановая смена скомпрометированных личных паролей с учетом предъявляемых требований.

Рекомендации:

1. С сотрудниками, допущенными к работе в ИСПДн, провести дополнительный инструктаж по соблюдению требований, предъявляемых к парольной защите.

2. Администратору безопасности ИСПДн проводить периодические проверки соблюдения требований, предъявляемых к парольной защите.

3. В «Плане проведения контроля…» своевременно проставлять отметки о выполнении мероприятий.

## 3. Учет, хранение и порядок обращения с криптосредствами, ключевой и эксплуатационной документацией

Поставка программно-аппаратных комплексов VipNet Coordinator HW100C осуществлена централизованно из Департамента. В соответствии с представленным договором комплект СКЗИ «КриптоПро CSP» версии 4.0 получен от ООО «Перемена» (бессрочная лицензия от 02.03.2016 № 1939Н выдана УФСБ России по Воронежской области). СКЗИ «КриптоПро CSP» версии 3.6 получено от УФК по Воронежской области на основании договора от 07.10.2013 № 3138/69.

Установку и настройку средств криптографической защиты информации проводили сотрудники ООО «ТЕХНОМАРКЕТ» (бессрочная лицензия от 20.03.2014 № 1683Н выдана УФСБ России по Воронежской области).

Формуляры на СКЗИ, а также их инсталляционные (дистрибутивные) пакеты ПО с электронными копиями технической документации на CD-дисках хранятся в сейфе, расположенном в служебном кабинете первого заместителя директора Учреждения.

Для осуществления поэкземплярного учета СКЗИ в Учреждении ведется специальный журнал, форма которого соответствует требованиям нормативно-методических документов ФСБ России. Вместе с тем отмечаем, что на момент начала проверки в данном журнале отсутствовали расписки пользователей СКЗИ, а также лиц, производивших их подключение.

Кроме того, в формулярах на введенные в эксплуатацию СКЗИ отсутствовали отметки об их закреплении за ответственными сотрудниками Учреждения. В ходе проведения проверки приказом № 90/ОД от 18.07.2017 назначен ответственный за эксплуатацию СКЗИ, соответствующие отметки в формуляры проставлены.

Рекомендация:

Учет СКЗИ осуществлять в строгом соответствии с требованиями «Инструкции об организации и обеспечению 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 при Президенте Российской Федерации от 13.06.2001 № 152 (далее – Инструкция № 152).

## 4. Работа с сотрудниками Учреждения, администратором безопасности информации и пользователями криптосредств

Приказом директора Учреждения от 13.06.2017 № 81/ОД администратором безопасности ИСПДн назначена заместитель начальника отдела социальных выплат и администрирования баз данных Терещенко Ирина Анатольевна.

Отмечаем, что данный сотрудник не обладает достаточными знаниями и не имеет опыта работы в области информационной безопасности, обучение на

курсах профессиональной переподготовки (повышения квалификации) по вопросам защиты информации до настоящего времени не планировалось.

В соответствии с требованиями п. 17 приказа ФСБ России от 10 июля 2014 года № 378[1] (далее – приказ № 378), выполнение которых обязательно для операторов, использующих СКЗИ для обеспечения безопасности персональных данных при их обработке в информационных системах, ответственным за обеспечение безопасности персональных данных в информационной системе необходимо назначать должностное лицо (работника), обладающего достаточными навыками.

Обучение сотрудников Учреждения, использующих СКЗИ (пользователей криптосредств), правилам работы с ними до настоящего времени не проводилось.

Рекомендации:

1. Целесообразно организовать обучение администратора безопасности ИСПДн на соответствующих курсах по изучению порядка организации и обеспечения безопасности информации, в том числе, содержащей персональные данные, обрабатываемые в информационных системах с применением средств криптографической защиты.

2. Спланировать и организовать изучение сотрудниками - пользователями криптосредств инструкций по эксплуатации и другой нормативно-методической документации на используемые средства защиты информации.

## 5. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

Специальные помещения размещены на первом и втором этажах основного административного здания Учреждения, в котором также располагаются сторонние организации. Въезд автотранспорта на прилегающую к зданию территорию оборудован автоматическим шлагбаумом. Входные двери спецпомещений деревянные, одностворчатые, оборудованы надежными механическими замками, приспособления для опечатывания имеются. От просмотра извне окна защищены с помощью жалюзи. Однако отмечаем, что окна серверного помещения с установленными в нем СКЗИ (кабинет № 6) не оборудованы средствами, препятствующими неконтролируемому проникновению в специальное помещение посторонних лиц (не выполнены требования п. 52 Инструкции 152).

По окончании рабочего дня ключи от специальных помещений в опечатанных тубусах сдаются сторожу общего отдела под расписку в Журнале приема и выдачи ключей. Должностные обязанности сторожа регламентируются служебной инструкцией, утвержденной директором Учреждения 31.07.2015.

---

[1] Приказ ФСБ России от 10 июля 2014 г. № 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».

В соответствии с контрактом от 03.02.2017 № 117 услуги по охране подразделений Учреждения, расположенных на ул. Березовая роща, 68 и ул. 3 Интернационала, 31, оказывает общество с ограниченной ответственностью частное охранное предприятие «Орлан» (лицензия ГУ МВД России по Воронежской области № 0001747 от 07.11.2013).

Отмечаем, что в отделе приема граждан обработка ПДн с использованием средств автоматизации не осуществляется.

Обработка персональных данных в ЕИС осуществляется в кабинете № 1 отдела по предоставлению жилищных субсидий. Вход в данное помещение возможен также через кабинет № 2 (архив). Отмечаем, что на момент проверки входные двери в кабинеты № 1 и № 2 в конце рабочего дня на замок не запирались (ключи от замков утеряны). Соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии, вышеуказанные кабинеты не оборудованы (не выполнены требования пп. а) п. 6 приказа № 378). В ходе работы комиссии входные двери указанных помещений оборудованы новыми механическими замками и приспособлениями для опечатывания. Ключи от замков пронумерованы и учтены в соответствующем журнале, выданы ответственным сотрудникам под расписку. Кроме того в спецпомещении имеется запасный выход, оборудованный охранной сигнализацией, выведенной на централизованный пульт ООО ЧОП «Орлан».

Комиссия отмечает, что на момент начала проверки ключи от входных дверей спецпомещений не были пронумерованы и учтены в соответствующем журнале, выданы без расписок в получении (не выполнены требования п. 55 Инструкции № 152). По рекомендации комиссии форма журнала переработана, ключи учтены и выданы под расписку ответственным сотрудникам.

Окна спецпомещений Учреждения, расположенных на первых этажах зданий, оборудованы металлическими решетками.

Правила доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств, утверждены директором Учреждения 02.06.2017.

Уборка помещений осуществляется в служебное время в присутствии сотрудников Управления.

Рекомендация:

Окна серверного помещения оборудовать средствами, препятствующими неконтролируемому проникновению посторонних лиц (металлическими решетками или охранной сигнализацией).

**Выводы:**

1. В казенном учреждении Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа» создана и функционирует система обеспечения безопасности персональных данных при их обработке в ИСПДн с использованием шифровальных (криптографических) средств.

2. Эксплуатация СКЗИ, используемых для обеспечения безопасности персональных данных при их обработке в ИСПДн, обращение с криптосредствами и ключевой информацией осуществляется с отступлениями от требований руководящих документов в области защиты информации.

Замечания, а также рекомендации по их устранению даны в соответствующих разделах акта.

О выполнении рекомендаций комиссии проинформировать УФСБ России по Воронежской области до 31 августа 2017 года.

Проверку провели:

Сотрудники УФСБ России
по Воронежской области — Д.В. Булашов

К.В. Логвинов

При проверке присутствовала:

Заместитель начальника отдела социальных выплат и администрирования баз данных казенного учреждения Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа» — И.А. Терещенко

С актом ознакомлена:

Первый заместитель директора казенного учреждения Воронежской области «Управление социальной защиты населения Центрального района г. Воронежа» — Н.В. Фатеева

Рег. от 01/5612 27.07.2017г.