


УТВЕРЖДАЮ
Министр культуры Республики Крым
Т.А. Манежина
« » 2023 г.

АКТ

**проверки выполнения организационных и технических мер
по обеспечению безопасности персональных данных при обработке
персональных данных в информационных системах персональных
данных ГБУК РК «Крымская республиканская библиотека для
молодежи»**

В соответствии с Приказом Министерства культуры Республики Крым (далее - Министерство) от 13 марта 2023 года № 60 *«О проведении плановой выездной проверки условий обработки персональных данных в ГБУК РК «Крымская республиканская библиотека для молодежи»* заведующим отдела защиты информации, гражданской обороны и антитеррористической безопасности управления имущественных отношений, защиты информации и гражданской обороны Министерства культуры Республики Крым Калашниковым С.В. проведена плановая проверка организации и состояния работ по обеспечению безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн) ГБУК РК «Крымская республиканская библиотека для молодежи» (далее – Библиотека).

Проверка проводилась с целью контроля выполнения требований следующих нормативно - правовых документов:

- федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон № 152-ФЗ);
- постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» (далее - Постановление № 211);
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований их обработке в ИСПДн» (далее - Постановление № 1119);
- приказ Федеральной службы по техническому и экспортному контролю Российской Федерации (далее - 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» (далее - Приказ № 21);

- приказ Федеральной службы безопасности Российской Федерации (далее - ФСБ России) от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке ИСПДн с использованием средств криптографической защиты информации (далее - СКЗИ), необходимых для выполнения установленных Правительством Российской Федерации требований к защите ПДн для каждого из уровней защищенности» (далее — Приказ № 378);

- приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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» (далее - Приказ № 152), а также оказания методической помощи Библиотеке в организации обработке и защиты ПДн, как оператора ПДн.

Контроль проводился по адресу фактического осуществления деятельности: 295022, Республика Крым, г. Симферополь, ул. Кечкеметская, д. 94^а.

В соответствии с требованиями Закона №152-ФЗ контроль за обеспечением безопасности ПДн осуществлялся без ознакомления с ПДн, обрабатываемыми в ИСПДн.

Проверка выполнения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием средств криптографической защиты информации в Библиотеки ФСБ России не проводилась.

Контроль по вопросам технической защиты конфиденциальной информации и персональных данных в информационных системах Библиотеки представителями ФСТЭК России не проводился.

1. Общие сведения об объекте контроля

Библиотека расположена в жилом пятиэтажном здании на первом этаже. Пропускной режим в здании, где расположена Библиотека, осуществляется сотрудниками ООО ЧОО «БОКС».

Пропускной режим организован в соответствии с «Правила пропускного и внутриобъектового режима ГБУК РК «Крымская республиканская библиотека для молодежи»» разработанными сотрудниками ООО ЧОО «БОКС» в согласовании и утвержденные руководством Библиотеки.

В организационном плане систему защиты информации Библиотеки организуют:

1. Директор Библиотеки;
2. Должностное лицо, ответственное за организацию обработки персональных данных;
3. Должностное лицо, ответственное за информационную безопасность;
4. Должностное лицо, ответственное за обеспечение безопасности информации - администратор локальной вычислительной сети, развернутой в Библиотеке;
5. Комиссия по контролю защищенности информационных систем;
6. Объекты информатизации, в которых функционируют ИСПДн.

В соответствии с приказом от 22.02.2023 № 40 должностным лицом, ответственным за организацию обработки персональных данных в учреждении назначена заместитель директора Библиотеки Павлова Елена Михайловна.

22.10.2022 г. утверждена инструкция ответственного за организацию обработки ПДн в Библиотеке.

В соответствии с приказом от 21.10. 2022 № 81 создана комиссия по контролю защищенности информационных систем.

Приказом от 06.07.2018 № 80 Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации Учреждение включено в реестр операторов ПДн (номер в реестре: 91-18-008029).

Приказом от 21.10.2022 № 83 утверждены следующие документы:

- политика Библиотеки в отношении обработки ПДн;
- правила рассмотрения запросов субъектов ПДн или их представителей;
- типовое обязательство сотрудника Оператора, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;
- типовая форма согласия на обработку персональных данных сотрудников Оператора, иных субъектов персональных данных;
- типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
- порядок восстановления персональных данных модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- должностная инструкция органа (ответственного) криптозащиты (отдельная инструкция).

Приказом от 09.01.2023 № 11 утверждён перечень ИСПДн.

Приказом от 22.10.2022 № 40 утверждён перечень должностей сотрудников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, **однако сам перечень выполнен некорректно.**

Приказом от 10.01.2020 № 26 утверждён порядок уничтожения

персональных данных при достижении целей обработки.

Приказом от 09.01.2023 № 12 назначен ответственный за организацию защиты информации с помощью криптосредств.

Приказом от 28.02.2023 № 41 утверждён список лиц, непосредственно допущенных к работе с СКЗИ.

Отдельно утверждены следующие документы:

- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Законом №152-ФЗ (21.10.2022);
- правила работы с обезличенными данными в случае обезличивания персональных данных (21.10.2022);

В соответствии с п. 2 ст. 19 Закона 152-ФЗ, пп. «д», п.1 Постановления № 211 внутренний контроль соответствия обработки персональных данных требованиям действующего законодательства в Библиотеке проводится, о чем свидетельствует наличие:

- журнала контроля;
- протоколов (3 шт.) и актов (2 шт.) внутреннего контроля (проверки).

Имеющиеся в распоряжении Библиотеки нормативные правовые акты, нормативные и методические документы позволяют в полном объеме организовать работы по защите персональных данных в ИСПДн Библиотеки.

Согласно перечню ИСПДн ПДн обрабатываются в следующих информационных системах (далее - ИС):

1. ИС «1С: Предприятие БГУ»;
2. ИС «1С: Зарплата и кадры государственного учреждения»;
3. ИС САБ «ИРБИС» АРМ «База данных читателей».

2. Выполнение требований по защите персональных данных при их обработке в информационных системах персональных данных.

В процессе проверки проверялось применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн Библиотеки, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн.

Проверкой выявлено следующее:

а) в части организации режима обеспечения безопасности помещений, в которых размещена ИС (далее - Помещения), препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения:

- все помещения Библиотеки оборудованы прочными входными дверьми с замками. Двери постоянно находятся в закрытом положении, но не на замок, а отсутствие в помещении преграждающего барьера позволяет осуществлять санкционированный проход в помещения Библиотеки лиц незапущенных к обработке ПДн и использованию СКЗИ. По окончании рабочего дня Помещения закрываются на замок, но не опечатываются под охрану с записью в «Журнале приема под охрану защищаемых помещений»

не сдаются (**нарушение** пп. «а» п. 6 Приказа №378 и п 57 Приказа ФАПСИ 152);

- правила доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях в Правилах внутриобъектового и пропускного режимов **не определены**;

- перечни лиц, имеющих право доступа в Помещения не утверждены (**нарушение** абз.6, ст.88 ТК; п.8.10, ч.2 Пр21; пп. «в» п. 6 Приказа № 378), утвержденные списки с указанием лиц имеющих право доступа в конкретные помещения **отсутствуют**.

б) в части обеспечения сохранности носителей персональных данных:

- жесткие диски компьютеров (HDD), как съемные носители информации ПДн в Библиотеке **не учтены**;

в) в ИСПДн Библиотеке применяются средства защиты информации, (СКЗИ) **не прошедшие в установленном порядке процедуру оценки соответствия** (демонстрационная версия СКЗИ КристоПро).

Мероприятия по технической защите информации, предусмотренные приказом №21 не реализованы.

В ИСПДн Библиотеки применяется нелицензионное программное обеспечение.

3. Учет, эксплуатация и порядок обращения со средствами криптографической защиты информации.

В соответствии с Уставом, Библиотека не является оператором связи, предоставляющим услуги конфиденциальной связи с использованием СКЗИ и не оказывает возмездные услуги по организации и обеспечению безопасности хранения и обработки с использованием СКЗИ конфиденциальной информации, передаваемой вне сетей конфиденциальной связи на основании лицензий ФСБ России на деятельность по предоставлению услуг в области шифрования информации.

При проведении контрольной проверки выявлены следующие нарушения требований Приказа №152:

- инструкции, регламентирующие процессы подготовки, ввода, обработки, хранения и передачи защищаемой с использованием СКЗИ конфиденциальной информации не разработаны (**нарушение п. 10 Приказа №152**);

- пользователи СКЗИ не имеют соответствующих заключений, подтверждающих должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ (**нарушение п. 21 Приказа №152**);

- журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведется, но в нем отсутствует запись о аппаратных средствах, на которых установлены СКЗИ, а также отсутствуют росписи (**нарушение п. 26 Приказа №152**);

- аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ не оборудованы средствами контроля за их вскрытием (опечатывание,

опломбирование) (нарушение п. 31 Приказа №152).

СКЗИ, применяемые в Учреждении, эксплуатационно-технической документацией **не обеспечены**.

4. Вывод по результатам работы проверки выполнения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

В ГБУК РК «Крымская республиканская библиотека для молодежи» система защиты персональных данных в информационных системах персональных данных создана с нарушениями действующего законодательства, меры по обеспечению безопасности персональных данных, при их обработке в ИСПДн Библиотеки, предусмотренные ст. 19 Закона № 152-ФЗ, выполнены не в полном объеме.

Эксплуатация средств криптографической защиты информации, используемых для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, обращение СКЗИ и ключевыми документами в Библиотеки, осуществляется с нарушениями требований действующих нормативных документов в области защиты информации.

Рекомендации:

ГБУК РК «Крымская республиканская библиотека для молодежи», с целью обеспечения защиты ПДн, обрабатываемых в ИСПДн, рекомендуется обеспечить выполнение следующих мероприятий:

1. Организовать обучение специалистов в области защиты ПДн.
2. Комплект документов по обработке и защите ПДн Привести в строгое соответствие с пп б), п.1 Постановления № 211.
3. Обеспечить принятие дополнительных мер по защите информации, не содержащей сведений, составляющих государственную тайну, (ПДн) в ИС Библиотеки, обратив особое внимание на:
 - необходимость проведения аттестации информационных систем по требованиям безопасности информации в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденным приказом ФСТЭК России от 29 апреля 2021 г. №77;
 - обеспечение защищенности информации, обрабатываемой в ИС, включая периодический анализ уязвимостей программного обеспечения с учетом сведений об уязвимостях, содержащихся в банках данных угроз безопасности информации (bdu.fstec.ru);
 - своевременность обновления применяемого в информационных системах программного обеспечения, особенно средств защиты периметра информационных систем с целью устранения уязвимостей;
 - своевременное выявление инцидентов безопасности информации в информационных системах и реагирование на них;
 - принятие мер по переходу на использование отечественного

офисного программного обеспечения.

4. Провести работы по определению угроз безопасности ПДн, актуальных при обработке ПДн в ИСПДн, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания ПДн, характера и способов их обработки.

5. Обеспечить применение организационных и технических мер по обеспечению безопасности ПДн в соответствии Постановлением № 211.

6. Обеспечить применение организационных и технических мер по обеспечению безопасности ПДн в соответствии с установленным уровнем защищенности ПДн на основании требований Постановления № 1119.

7. Обеспечить применение организационных и технических мер по обеспечению безопасности ПДн в соответствии с Приказом № 21 ФСТЭК.

8. Обеспечить эксплуатацию средств криптографической защиты информации, используемых для обеспечения безопасности ПДн при их обработке в ИСПДн, обращение с СКЗИ и ключевыми документами к ним в соответствии требованиями действующих нормативных документов в области защиты информации.

9. На постоянной основе осуществлять внутренний контроль соответствия обработки ПДн установленным требованиям безопасности, в соответствии с действующим законодательством Российской Федерации.

10. Организовать работу по изучению вопроса о создании и развитию подразделений по защите информации (отдельных штатных специалистов по защите информации) в Библиотеке

11. Организовать устранение выявленных недостатков, для чего, в месячный срок с момента получения настоящего акта, составить план устранения недостатков с определением конкретных сроков и конкретных исполнителей за выполнение намеченных мероприятий.

Второй экземпляр плана устранения недостатков направить установленным порядком в Управление имущественных отношений, защиты информации и гражданской обороны Министерство культуры Республики Крым.

Доклад об устранении недостатков осуществлять ежеквартально в срок до 20 числа последнего месяца квартала в Управление имущественных отношений, защиты информации и гражданской обороны Министерство культуры Республики Крым.

**Заведующий отделом отдела защиты
информации, гражданской обороны
и антитеррористической безопасности**


/Калашников С.В.
(подпись) (Ф.И.О.)