ПРОЕКТ

РЕСПУБЛИКА КРЫМ
МИНИСТЕРСТВО КУЛЬТУРЫ

П Р И К А З

от _____ 2017 г. № _____

г. Симферополь

О защите персональных данных

В соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных», Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 №646, Постановлением Правительства Российской Федерации от 21 марта 2012 г. №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»,

ПРИКАЗЫВАЮ:

1 . Назначить ответственным:

за организацию обработки персональных данных в информационной системе персональных данных в Министерстве культуры Республики Крым Заатова Исмета Аблятифовича, заместителя министра культуры Республики Крым;

за обеспечение безопасности персональных данных в информационной системе персональных данных в Министерстве культуры Республики Крым Ходича Сергея Валерьевича – ведущего специалиста отдела целевых программ управления целевых программ и государственных закупок;

за обработку персональных данных в информационной системе персональных данных в Министерстве культуры Республики Крым Бокова Петра Васильевича, главного специалиста по мобилизационной работе и режиму секретности; Томатову Екатерину Александровну – ведущего специалиста отдела государственной гражданской службы, кадровой и правовой работы.

2. Утвердить прилагаемые:

ПРОЕКТ

2.1. Политику в отношении обработки персональных данных в информационной системе персональных данных в Министерстве культуры Республики Крым (Приложение 1).

2.2. Перечень должностных лиц, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных в Министерстве культуры Республики Крым, необходим для выполнения ими служебных (трудовых) обязанностей (Приложение 2).

2.3. Перечень разрешенных персональных данных для обработки в информационной системе персональных данных в Министерстве культуры Республики Крым (Приложение 3).

2.4. Перечень угроз безопасности персональных данных при обработке в информационной системе персональных данных в Министерстве культуры Республики Крым (Приложение 4).

3. Ведущему специалисту отдела целевых программ управления целевых программ и государственных закупок Ходичу С.В.: обеспечить ведение журнала учета машинных носителей информации, предназначенных для хранения информации и ведение журнала событий безопасности.

4. Ведущему специалисту отдела государственной гражданской службы, кадровой и правовой работы Томатовой Е.А.: ознакомить должностных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Министерства культуры Республики Крым в отношении обработки персональных данных.

5. Признать утратившими силу приказы Министерства культуры Республики Крым от 08.06.2015 г. №181 «О назначении ответственных за организацию обработки персональных данных», от 21.03.2016 г. №171-л «О назначении ответственных за организацию обработки персональных данных» и от 08.06.2015 г. №215-л «О внесении изменений в приказ от 08.06.2015 г. №181».

6. Контроль за исполнением настоящего приказа возложить на заместителя министра культуры Республики Крым Заатова И.А.

Министр **В. Новосельская**

ПРОЕКТ

Приложение 1
к приказу Министерства культуры
Республики Крым
от _____2017 г. № ___

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ КУЛЬТУРЫ РЕСПУБЛИКИ КРЫМ

1. Общие положения

1.1. Настоящий документ определяет политику (далее – Политика) Министерства культуры Республики Крым (далее – Министерство) в отношении обработки персональных данных.

1.2. Настоящая Политика разработана и утверждена в соответствии с требованиями Конституции Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», и действует в отношении всех персональных данных, обрабатываемых в Министерстве.

1.3. Целью настоящей Политики является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, а также интересов Министерства.

1.4. Настоящая Политика определяет цели, принципы, порядок и условия обработки персональных данных работников и иных лиц, чьи персональные данные обрабатываются в Министерстве, а также включает перечень мер, применяемых в целях обеспечения безопасности персональных данных при их обработке.

1.5. Политика является общедоступным документом, декларирующим концептуальные основы деятельности Министерства при обработке персональных данных.

2. Правовые основания обработки персональных данных

2.1. Правовой основой настоящей Политики в области обработки персональных данных является Федеральный закон № 152-ФЗ «О персональных данных» от 27 июля 2006 года, постановления Правительства РФ, нормативные акты ФСБ России, ФСТЭК России, иные нормативно-правовые и локальные акты Республики Крым и Министерства.

2.2. Во исполнение настоящей Политики в Министерстве разрабатываются и утверждаются локальные акты, регламентирующие

порядок организации обработки и обеспечения безопасности персональных данных.

3. Основные категории, цели и принципы обработки персональных данных

3.1. Министерство осуществляет обработку персональных данных в следующих целях:

реализации прав и обязанностей Министерства, установленных действующим законодательством, для решения следующих задач:

организации системы кадрового учета, анализ качественного состава кадров и мониторинг персонала, формирование резерва кадров;

осуществления функции учета и отчетности по расходам, связанным с оплатой труда;

обеспечения воинского учета;

выполнения задач возложенных в соответствии с Положением о Министерстве.

3.2. Содержание и объем обрабатываемых категорий персональных данных субъектов персональных данных, перечисленных в разделе 3 настоящей Политики, определяются в соответствии с целями обработки персональных данных. Министерство не обрабатывает персональные данные, которые являются избыточными по отношению к указанным целям обработки или несовместимы с такими целями.

Обрабатываемые Министерством персональные данные содержатся как в подлинниках, так и копиях документов.

В подлинниках хранятся следующие документы:

- письменное заявление о приеме на работу;
- документы о прохождении конкурса на замещение вакантной должности (если гражданин назначен на должность по результатам конкурса);
- экземпляр трудового договора, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в трудовой договор;
- аттестационный лист, и отзыв об исполнении им должностных обязанностей за аттестационный период;
- медицинское заключение установленной формы об отсутствии у гражданина заболевания, препятствующего выполнению им служебных обязанностей;
- личные карточки формы Т-2ГС;
- списки замещения штатных должностей работников Министерства;
- списки работников Министерства, подлежащих обязательному медицинскому страхованию;
- журнал учета движения трудовых книжек и вкладышей к ним;
- журнал учета принятых и уволенных работников Министерства;
- журнал учета кадровых перемещений по Министерства;
- журнал учета личных дел;

- журнал учета трудовых договоров;

- журнал учета листков нетрудоспособности;

- книга учета и выдачи служебных удостоверений;

- табели учета рабочего времени;

- документы по индивидуальному (персонифицированному) учету в системе обязательного пенсионного страхования (в соответствии с Постановлением Правления Пенсионного фонда Российской Федерации от 31.07.2006 № 192п «О формах документов индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования и инструкции по их заполнению»;

- расчетно-платежная ведомость (форма по ОКУД 0504401);

- платежная ведомость (форма по ОКУД 0504403);

- расчетный листок;

- карточка-справка (форма по ОКУД 0504417);

- налоговая карточка по учету доходов и налога на доходы физических лиц (форма 1-НДФЛ);

- справка о доходах физического лица в инспекцию Федеральной налоговой службы (форма 2-НДФЛ);

- индивидуальные сведения о страховом стаже и начисленных страховых взносах на обязательное пенсионное страхование застрахованного лица (форма СЗВ-4-2);

- реестр застрахованных лиц, за которых перечислены дополнительные страховые взносы на накопительную часть трудовой пенсии и уплачены взносы работодателя (форма ДСВ-3);

- индивидуальная карточка учета сумм начисленных выплат и иных вознаграждений, сумм начисленного единого социального налога, страховых вносов на пенсионное страхование (налогового вычета) (приложение 1 к приказу МНС РФ от 27.07.2004 № САЭ-3-05/443);

- справка о заработной плате работников, выдаваемая для предъявления работником по месту требования;

В копиях и подлинниках хранятся следующие документы:

- паспорт;

- свидетельства о государственной регистрации актов гражданского состояния;

- документы, подтверждающие прохождение военной или иной службы;

- документы о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);

- документы воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

- страховые свидетельства обязательного пенсионного страхования;

- свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации;

- страховые медицинские полисы обязательного медицинского страхования граждан;

- трудовые книжки;

- собственноручно заполненные и подписанные анкеты работников, а также лиц, претендующих на замещение вакантных должностей или на включение в кадровый резерв, установленной формы с фотографией;

- приказы по кадровым вопросам (в том числе о назначении на должность, переводе на иную должность, освобождении от замещаемой должности), приказы Министерства о награждении ведомственными наградами Министерства, документы о награждении государственными наградами, присвоении почетных званий, присуждении государственных премий (если таковые имеются), а также проекты указанных правовых актов;

- документы о включении работника в кадровый резерв, а также об исключении его из кадрового резерва;

- решения о поощрении работника, а также о наложении на него дисциплинарного взыскания до его снятия или отмены;

- документы о начале служебной проверки, ее результатах, об отстранении работника от замещаемой должности;

- справки-объективки;

- иные документы, установленные федеральными законами, иными нормативными актами Российской Федерации, представляемые при поступлении на работу и в процессе осуществления трудовой деятельности.

3.3. Министерство в своей деятельности обеспечивает соблюдение принципов и условий обработки персональных данных, указанных в статьях 5 и 6 Федерального закона 152-ФЗ «О персональных данных».

Обработка персональных данных в Министерстве осуществляется на основе принципов:

законности и справедливости целей и способов обработки персональных данных;

соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Министерства;

соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

3.4. Министерство осуществляет обработку персональных данных только при условиях, определенных действующим законодательством Российской Федерации в области персональных данных.

3.5. Министерство не выполняет обработку специальных категорий персональных данных.

3.6. Министерство не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

3.7. В Министерстве могут быть созданы общедоступные источники персональных данных (справочники, адресные книги). Персональные данные, сообщаемые субъектом (фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и др.), включаются в такие источники только с письменного согласия субъекта персональных данных.

4. Порядок, условия и сроки обработки персональных данных

4.1. Министерство обрабатывает персональные данные своих работников, а также иных лиц, давших согласие на обработку персональных данных, во исполнение заключенных договоров или с целью их заключения, во исполнение обязательств, предусмотренных федеральным законодательством и иными нормативными правовыми актами, а также в иных целях в соответствии с требованиями Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных».

4.2. Обработка персональных данных прекращается по истечении срока, предусмотренного законом, иным нормативным правовым актом Российской Федерации, договором, или согласием субъекта персональных данных на обработку его персональных данных. При отзыве субъектом персональных данных согласия на обработку его персональных данных такая обработка осуществляется только в пределах, необходимых для исполнения заключенных с ним договоров и в целях, предусмотренных законодательством Российской Федерации.

4.3. В Министерстве обеспечивается защита персональных данных в рамках единого комплекса организационно-технических и правовых мероприятий по защите информации, составляющей персональные данные. При обеспечении защиты персональных данных учитываются требования Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных», принятых в соответствии с ним нормативных правовых актов и Трудового кодекса Российской Федерации. Система защиты информации Министерства

непрерывно развивается и совершенствуется на базе требований национальных стандартов информационной безопасности.

4.4. В предусмотренных нормативными актами и локальными актами случаях в Министерстве проводится аттестация информационных систем на соответствие требованиям по безопасности информации.

4.5. Сроки обработки и архивного хранения персональных данных определяются в соответствии с требованиями действующего законодательством РФ (Гражданским кодексом РФ, Трудовым кодексом РФ, Налоговым кодексом РФ, Федеральным законом РФ №152-ФЗ от 27.07.2006 г. «О персональных данных», Федеральным законом 125-ФЗ от 22.10.2004 г. «Об архивном деле», Приказом Минкультуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», а также иными требованиями действующего законодательства РФ), нормативными актами и локальными актами Министерства.

4.6. Министерство прекращает обработку персональных данных в следующих случаях:

при достижении цели обработки персональных данных;

при изменении, признании утратившими силу нормативных правовых актов, устанавливающих правовые основания обработки персональных данных;

при выявлении неправомерной обработки персональных данных, осуществляемой Министерством;

при отзыве субъектом персональных данных согласия на обработку его персональных данных, если в соответствии с Федеральным законом обработка персональных данных допускается только с согласия субъекта персональных данных.

4.7. Уничтожение Министерством персональных данных осуществляется в порядке и сроки, предусмотренные законодательством Российской Федерации.

5. Категории субъектов персональных данных

5.1. Министерство обрабатывает персональные данные следующих категорий субъектов персональных данных:

- работников Министерства (далее – работники);
- лиц, претендующих на замещение вакантных должностей в Министерстве при прохождении процедуры согласования назначения на должность в установленном порядке;
- лиц, претендующих на включение в кадровый резерв;
- исполнителей по гражданско-правовым договорам;
- руководителей предприятий, учреждений, отнесенных к ведению Министерства;

-заместителей руководителей и главных бухгалтеров предприятий, учреждений, отнесенных к ведению Министерства;

- физических лиц, проходящих процедуры в соответствии целями и задачами Министерства.

6. Передача персональных данных

6.1. Министерство не предоставляет и не раскрывает сведения, содержащие персональные данные субъектов персональных данных, третьей стороне без согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральными законами.

6.2. Министерство передает обрабатываемые персональные данные в уполномоченные организации, государственные органы, государственные внебюджетные фонды только на основаниях и в случаях, предусмотренных законодательством Российской Федерации,

6.3. По мотивированному запросу, исключительно для выполнения возложенных законодательством функций и полномочий, персональные данные субъекта персональных данных без его согласия могут быть переданы в судебные органы, в органы государственной безопасности, прокуратуры, полиции, следственные органы – в случаях, установленных нормативными правовыми актами, обязательными для исполнения.

7. Обеспечение безопасности персональных данных

7.1. Министерство при обработке персональных данных принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

7.2. Во исполнение норм действующего законодательства, а также в соответствии с настоящей Политикой в Министерстве принимаются следующие меры:

назначаются ответственные за организацию обработки персональных данных, за информационную безопасность, администратор информационной безопасности;

разрабатываются и внедряются локальные акты, определяющие правила обработки персональных данных, а также процедуры, направленные на выявление и предотвращение нарушения таких правил;

применяются правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона РФ №152-ФЗ от 27.07.2006 г. «О персональных данных»;

осуществляется внутренний контроль соответствия обработки персональных данных требованиям нормативных актов с целью выявления нарушений установленных процедур по обработке персональных данных и устранение последствий таких нарушений;

с работниками Министерства, непосредственно осуществляющими обработку персональных данных, связанными с вопросами защиты информации проводится обучение правилам обработки и защиты персональных данных (в том числе мероприятия по ознакомлению с положениями законодательства Российской Федерации в области персональных данных, с требованиями к защите персональных данных, документами, определяющими политику Министерства в отношении обработки персональных данных, локальными актами Министерства по вопросам обработки персональных данных);

осуществляется оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона РФ №152-ФЗ от 27.07.2006 г. «О персональных данных»;

7.3. В целях обеспечения безопасности персональных данных проводятся следующие мероприятия:

определяются угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных,

определяются уровни защищенности персональных данных;

применяются средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия;

проводится оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

осуществляется учет машинных носителей персональных данных;

принимаются процедуры, направленные на выявление фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;

производится восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

устанавливаются правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивается регистрация и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных;

осуществляется постоянный контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

7.4. Обязанности должностных лиц, осуществляющих обработку и защиту персональных данных, а также их ответственность,

определяются локальными актами Министерства по вопросам обработки и обеспечения безопасности персональных данных.

8. Права субъектов персональных данных

В соответствии с Федеральным Законом № 152-ФЗ «О персональных данных» субъект персональных данных имеет право:

8.1. Требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.2.Требовать перечень своих персональных данных, обрабатываемых Министерством и источник их получения.

8.3. Получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения.

8.4. Требовать извещения Министерством всех лиц, которым в рамках действующего законодательства РФ ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

8.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

8.6. На защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;

8.7. Отозвать свое согласие на обработку своих персональных данных.

9. Обязанности управления и конфиденциальность персональных данных

9.1. Министерство обязано осуществить самостоятельно или обеспечить (если обработка персональных данных осуществляется другим лицом) конфиденциальность, блокирование, уточнение, прекращение обработки, уничтожение персональных данных субъекта персональных данных в соответствии с требованиями статьи 21 Федерального закона № 152-ФЗ «О персональных данных».

9.2. Персональные данные работников Министерства, обрабатываемые в Министерстве и подающие справку о доходах в контролирующие органы, относятся к информации конфиденциального характера.

9.3. Работники Министерства, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими служебных (трудовых) обязанностей**,** обязаны соблюдать конфиденциальность обрабатываемых персональных данных и информируются о том, что в соответствии со ст.24 ФЗ-152 «О персональных

данных» лица, виновные в нарушении требований закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

9.4. Работники Министерства подписывают обязательство о неразглашении персональных данных.

10. Заключительные положения

10.1. Настоящая Политика является общедоступным документом и подлежит размещению на официальном сайте Министерства.

10.2. Настоящая Политика подлежит пересмотру в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

10.3. Контроль за исполнением требований настоящей Политики осуществляется ответственным лицом Министерства, назначаемым в установленном порядке локальным актом.

10.4. Ответственность должностных лиц Министерства, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с действующим законодательством Российской Федерации в области персональных данных и локальными актами Министерства.

ПРОЕКТ

Приложение 2
к приказу Министерства культуры
Республики Крым
от _____2017 г. №___

ПЕРЕЧЕНЬ
ДОЛЖНОСТНЫХ ЛИЦ, ДОСТУП КОТОРЫХ К ПЕРСОНАЛЬНЫМ ДАННЫМ, ОБРАБАТЫВАЕМЫМ В ИНФОРМАЦИОННОЙ СИСТЕМЕ В МИНИСТЕРСТВЕ КУЛЬТУРЫ, НЕОБХОДИМ ДЛЯ ВЫПОЛНЕНИЯ ИМИ СЛУЖЕБНЫХ (ТРУДОВЫХ) ОБЯЗАННОСТЕЙ

1. Заатов И.А. заместитель министра
2. Управление планирования и финансов
Меметова Л.Э. – начальник – управления – главный бухгалтер

1.1. Отдел бухгалтерского учета и отчетности управление планирования и финансов

Зорина О.В. – заведующий отделом – заместитель главного бухгалтера
Поцелуйко А.С. – главный специалист
Дорошенко О.Л. - ведущий специалист

3. Отдел государственной гражданской службы, кадровой и правовой работы

Минкина Е.С. – заведующий отделом
Коновалов А.А. – заместитель заведующего отделом
Рассказова О.В. – консультант
Грибакова Е.В. – главный специалист
Томатова Е.А. – ведущий специалист

4. Отдел целевых программ управления целевых программ и государственных закупок

Ходич С.В. – ведущий специалист

5. Задорожная М.В. – консультант внутреннего финансового контроля и внутреннего финансового аудита.

6. Боков П.В. – главный специалист по мобилизационной работе и режиму секретности

ПРОЕКТ

Приложение 3
к приказу Министерства культуры
Республики Крым
от _____2017 г. № ___

ПЕРЕЧЕНЬ
РАЗРЕШЕННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ ОБРАБОТКИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ КУЛЬТУРЫ РЕСПУБЛИКИ КРЫМ

1. В соответствии с целями, указанными в пункте 7 раздела 2 Правил обработки персональных данных в Министерстве культуры Республики Крым (далее – Правила, Министерство), утвержденного приказом Министерства от 25.08.2016 № 326-л обрабатываются следующие категории персональных данных гражданских служащих Министерства, руководителей подведомственных организаций, граждан претендующих на замещение вакантных должностей гражданской службы, а также граждан, претендующих на замещение должностей руководителей подведомственных организаций:

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

2) число, месяц, год рождения;

3) место рождения;

4) сведения о гражданстве (в том числе предыдущие гражданства, иные гражданства);

5) вид, серия, номер документа удостоверяющего личность (дата выдачи, наименование органа, выдавшего его);

6) адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;

7) номер контактного телефона или сведения о других способах связи;

8) реквизиты страхового свидетельства обязательного пенсионного страхования;

9) идентификационный номер налогоплательщика;

10) реквизиты страхового медицинского полиса обязательного медицинского страхования;

11) реквизиты свидетельства государственной регистрации актов гражданского состояния;

12) сведения о семейном положении, составе семьи и о близких родственниках (в том числе бывших);

13) сведения о трудовой деятельности;

14) сведения о воинском учете и реквизиты документов воинского учета;

15) сведения об образовании (когда и какие образовательные, научные и иные организации окончил, номера документов об образовании,

направление подготовки или специальность по документу об образовании, квалификация);

16) сведения об ученой степени;

17) сведения о владении иностранными языками, уровень владения;

18) сведения об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению;

19) фотография;

20) сведения о прохождении гражданской службы (работы), в том числе: дата, основания поступления на гражданскую службу (работу) и назначения на должность гражданской службы, дата, основания назначения, перевода, перемещения на иную должность гражданской службы (работы), наименование замещаемых должностей гражданской службы с указанием структурных подразделений, размера денежного содержания (заработной платы), результатов аттестации на соответствие замещаемой должности гражданской службы, а так же сведения о прежнем месте работы;

21) сведения, содержащие в служебном контракте, дополнительных соглашениях к служебному контракту;

22) сведения о пребывании заграницей;

23) сведения о классном чине;

24) сведения о наличии или отсутствии судимости;

25) сведения об оформленных допусках к государственной тайне;

26) сведения о государственных наградах, иных наградах и знаков отличия;

27) сведения о профессиональной переподготовке и (или) повышении квалификации;

28) сведения об ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

29) сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;

30) номер расчетного счета;

31) номер банковской карты;

32) иные персональные данные, необходимые для достижения целей, предусмотренные пунктом 7 Правил.

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

1) фамилия, имя, отчество (последнее при наличии);

2) почтовый адрес;

3) адрес электронной почты;

4) указанный в обращении контактный телефон;

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

3. При аккредитации организаций (индивидуальных предпринимателей), оказывающих услуги в области охраны труда, осуществляется обработка

следующих персональных данных представителей организаций (индивидуальных предпринимателей), обратившихся в Министерство:

1) фамилия, имя, отчество (последнее при наличии);

2) вид, серия, номер документа, удостоверяющего личность, дата выдачи, наименование органа, выдавшего его;

3) адрес места жительства;

4) номер контактного телефона и, при наличии, адрес электронной почты;

5) идентификационный номер налогоплательщика;

6) сведения об образовании (когда и какие образовательные, научные и иные организации окончил, номера документов об образовании, направление подготовки или специальность по документу об образовании, квалификация).

ПРОЕКТ

Приложение 4
к приказу Министерства культуры
Республики Крым
от _____2017 г. № ___

ПЕРЕЧЕНЬ
УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛНЫХ ДАННЫХ В МИНИСТЕРСТВЕ КУЛЬТУРЫ РЕСПУБЛИКИ КРЫМ

1. Угрозы безопасности персональных данных определяемые согласно требованиям Федеральной службы по техническому и экспортному контролю для информационных систем персональных данных обеспечения типовой и специальной деятельности Министерства:

1.1. Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

1.2. Угрозы разглашения пользовательских имен и паролей;

1.3. Угрозы, связанные с расширением привилегий пользователей;

1.4. Угрозы, связанные с возможностью внедрения операторов SQL;

1.5. Угрозы несанкционированного копирования защищаемой информации;

1.6. Угрозы внедрения вредоносных программ;

1.7. Угрозы наличия механизмов разработчика;

1.8. Угрозы "Анализ сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;

1.9. Угрозы сканирования, направленные на выявление типа операционной системы, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и другого;

1.10. Угрозы выявления паролей;

1.11. Угрозы получения несанкционированного доступа путем подмены доверенного объекта;

1.12. Угрозы удаленного запуска приложений;

1.13. Угрозы несанкционированного отключения средств защиты информации;

1.14. Угрозы, связанные с недостаточной квалификацией обслуживающего информационные системы персональных данных (далее - ИСПДн) персонала;

1.15. Угрозы непреднамеренного или преднамеренного вывода из строя технических средств;

1.16. Угрозы надежности технических средств и коммуникационного оборудования;

1.17. Угрозы утраты носителей информации;

1.18. Угрозы легитимности использования программного обеспечения;

1.19. Угрозы достаточности и качества применяемых средств защиты информации и средств антивирусной защиты;

1.20. Угрозы использования информации идентификации (аутентификаци) заданной по умолчанию;

1.21. Угрозы, связанные с анализом сетевого трафика между компонентами информационной системы с целью получения аутентификационной информации;

1.22. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

1.23. Угрозы подмены доверенного объекта;

1.24. Угрозы заражения DNS-кеша;

1.25. Угрозы неправомерных действий в каналах связи;

1.26. Угрозы совершения атак на монитор виртуальных машин из физической сети;

1.27. Угрозы совершения атаки с виртуальной машины на другую виртуальную машину;

1.28. Угрозы совершения атаки на систему управления виртуальной инфраструктурой;

1.29. Угрозы выхода процесса за пределы виртуальной машины;

1.30. Угрозы неконтролируемого копирования данных внутри хранилища больших данных;

1.31. Угрозы неконтролируемого уничтожения информации хранилищем больших данных;

2. Угрозы безопасности персональных данных для информационных систем персональных данных обеспечения типовой и специальной деятельности, установленные дополнительно согласно требованиям Федеральной службы безопасности Российской Федерации:

2.1. Угрозы внесения несанкционированных изменений в средства криптографической защиты информации (далее - СКЗИ) и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ, в совокупности представляющие среду функционирования СКЗИ (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований;

2.2. Угрозы внесения несанкционированных изменений в документацию на СКЗИ и компоненты СФ;

2.3. Угрозы атаки на персональные и все возможные данные, передаваемые в открытом виде по каналам связи;

2.4. Угрозы получения из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть Интернет) информации об информационной системе, в которой используются СКЗИ;

2.5. Угрозы получения из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-

телекоммуникационную сеть Интернет) информации об информационной системе, в которой используются СКЗИ;

2.6. Угрозы применения находящихся в свободном доступе или используемых за пределами контролируемой зоны автоматизированных систем (далее - АС) и программного обеспечения (далее - ПО), включая аппаратные и программные компоненты АС и ПО, а также специально разработанных АС и ПО;

2.7. Угрозы применения находящихся в свободном доступе или используемых за пределами контролируемой зоны автоматизированных систем (далее - АС) и программного обеспечения (далее - ПО), включая аппаратные и программные компоненты АС и ПО, а также специально разработанных АС и ПО;

2.8. Угрозы использования на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки: каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами; каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

2.9. Угрозы проведения на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

2.10. Угрозы использования на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ.