Приложение
к приказу от 30.09.2024 № 48

ПОЛОЖЕНИЕ О КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ КУЛЬТУРЫ «ОДИНЦОВСКИЙ ЦЕНТР КУЛЬТУРНОГО РАЗВИТИЯ»

1. Общие положения

1.1 Положение о конфиденциальной информации в Муниципальном бюджетном учреждении культуры «Одинцовский Центр культурного развития» (далее – Положение) разработано в соответствии с Гражданским кодексом Российской Федерации, Федеральными законами: от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении сведений конфиденциального характера», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Гостехкомиссии России от 30.08.2002 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации» государственная техническая комиссия», приказом 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», иными федеральными законами и нормативными правовыми актами Российской Федерации (далее – законодательство РФ).

1.2 Настоящее Положение регулирует отношения, связанные с обработкой, использованием и защитой конфиденциальной информации в Муниципальном бюджетном учреждении культуры «Одинцовский Центр культурного развития» (далее – Учреждение).

1.3 Положение определяет политику Учреждения по безопасности информационных и коммуникационных ресурсов и технологий и общий порядок обращения с документами, содержащими служебную информацию ограниченного распространения, и устанавливает:

1) объекты защиты информации и субъекты доступа к информации информационных систем и ресурсов;

2) основные угрозы информационной безопасности (далее – информационная безопасность);

3) основные принципы построения системы защиты информации Учреждения;

4) меры, методы и средства обеспечения информационной безопасности в Учреждении.

1.4 Настоящее Положение разработано с целью установления надлежащего порядка работы и создания безопасных условий для обучающихся, родителей (законных представителей) обучающихся, работников, посетителей, контрагентов Учреждения, иных обладателей конфиденциальной информации, связанных с Учреждением договорными отношениями, а так же исключения возможности доступа посторонних лиц к конфиденциальной безопасности, выноса носителей информации, иных нарушений обработки, использования и защиты конфиденциальной информации.

1.5 В настоящем Положении используются следующие термины и определения:

1) информация – сведения (сообщения, данные) независимо от формы их представления;

2) конфиденциальная информация – любые сведения, которые не подлежат без согласия их обладателя предоставлению и/или распространению, разглашению лицом, получившим к ней доступ;

3) обладатель конфиденциальной информации - лицо, самостоятельно создавшее конфиденциальную информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к такой информации;

4) персональные данные – любая информация, относящаяся к работнику, обучающемуся, родителю (законному представителю) несовершеннолетнего обучающегося, пользователю услугами Учреждения, контрагенту, посетителю либо иному третьему лицу как субъекту персональных данных, позволяющая идентифицировать его личность;

5) доступ к конфиденциальной информации - возможность получения конфиденциальной информации и ее использования, ознакомление определенных лиц с конфиденциальной информацией с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

6) предоставление конфиденциальной информации – передача конфиденциальной информации ее обладателем определенному кругу лиц в соответствии с законодательством РФ, осуществляемая в порядке, установленном соглашением лиц, участвующих в обмене информацией;

7) распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц. В отношении конфиденциальной информации свободно не осуществляется;

8) разглашение конфиденциальной информации - действие или бездействие, в результате которых конфиденциальная информация, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств), становится известной третьим лицам без согласия обладателя такой информации и без законных на это оснований;

9) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

10) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

11) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

12) информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

1.6 Учреждение является обладателем конфиденциальной информации.

1.7 Перечень сведений конфиденциального характера определяется Приложением 1 к настоящему Положению.

1.8 Общее управление обеспечением режима безопасности сведений, содержащих конфиденциальную информацию, осуществляет директор Учреждения.

1.9 Настоящее Положение, все изменения и дополнения к нему утверждаются приказом директора Учреждения. Все остальное, что не предусмотрено настоящим Положением, регулируется нормами действующего законодательства Российской Федерации.

1.10 Все работники Учреждения в обязательном порядке должны быть ознакомлены под роспись с настоящим Положением и всеми изменениями к нему.

1.11 Данное Положение размещается на официальном сайте Учреждения информационно - телекоммуникационной сети «Интернет».

2. Защита конфиденциальной информации

2.1 Защита конфиденциальной информации Учреждения состоит в принятии комплекса мер, направленных на ограничение доступа к конфиденциальной информации третьих лиц, не являющихся обладателями данной информации, на предотвращение несанкционированного разглашения конфиденциальной информации, выявление попыток разглашения конфиденциальной информации, пресечение нарушений использования и хранения конфиденциальной информации, в том числе путем установления технических средств защиты от несанкционированного доступа к информации (видеонаблюдение, сейфы и металлические контейнеры (ящики) для хранения документов и пр.).

2.2 Для защиты персональных данных принимаются организационные и технические меры в соответствии с требованиями законодательства и локальными нормативными правовыми актами Учреждения, определяющими политику обработки и защиты персональных данных.

3. Объекты, подлежащие защите

3.1. В Учреждении обрабатывается конфиденциальная информация, содержащая сведения ограниченного распространения (служебная информация, персональные данные), и открытые сведения. Защите подлежат все информационные системы Учреждения, независимо от их местонахождения, числящиеся на бухгалтерском учете Учреждения.

3.2. Основные объекты, подлежащие защите в Учреждении:

1) информационные системы персональных данных (в традиционном и электронном виде);

2) имеющие коммерческое значение данные об уставной деятельности Учреждения, в том числе о контрагентах, сделках, размерах прибыли от приносящей доход деятельности Учреждения (объекты, подпадающие под понятие «коммерческая тайна»);

3) открытая (общедоступная) информация, необходимая для бесперебойной и эффективной работы Учреждения, независимо от формы и вида ее представления;

4) процессы обработки конфиденциальной информации в информационных системах Учреждения, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи конфиденциальной информации;

5) информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

3.3. Особенности объектов, подлежащих защите:

1) объединение в единую систему большого количества технических средств обработки и передачи информации;

2) необходимость обеспечения непрерывности функционирования Учреждения;

3) высокая интенсивность информационных потоков;

4) разнообразие категорий пользователей.

4. Цели и задачи системы обеспечения информационной безопасности

4.1. Субъектами доступа к конфиденциальной информации при обеспечении информационной безопасности Учреждения являются:

1) работники Учреждения, участвующие в информационном обмене в соответствии с возложенными на них должностными обязанностями;

2) обучающиеся, родители (законные представители) обучающихся, иные физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах Учреждения (в соответствии со ст.14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

3) сотрудники внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием электронно-цифрового оборудования и/или информационных систем;

4) физические и юридические лица, являющиеся пользователями услуг, оказываемых Учреждением или контрагентами Учреждения (сторонами сделок) в процессе осуществления уставной деятельности.

4.2. Перечисленным субъектам доступа к информации необходимо обеспечить:

1) своевременность доступа к необходимой им информации (ее доступность);

2) достоверность (полноту, точность, актуальность, целостность) информации;

3) конфиденциальность (сохранение в тайне) определенной части информации, защиту от навязывания ложной (недостоверной, искаженной) информации;

4) возможность осуществления контроля и управления процессами обработки и передачи информации;

5) защиту информации от незаконного распространения.

4.3 Цель защиты информации достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

1) доступности информации для авторизованных субъектов доступа (устойчивого функционирования системы, при котором авторизованные субъекты доступа имеют возможность получения необходимой информации);

2) целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в системах Учреждения и передаваемой по каналам связи;

3) конфиденциальности – сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи.

4.4 Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается методами и средствами, соответствующими множеству значимых угроз.

4.5 Для достижения основной цели защиты и обеспечения указанных свойств информации система информационной безопасности должна обеспечивать решение следующих основных задач:

1) своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем;

2) создание механизма оперативного реагирования на угрозы безопасности информации;

3) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

4) защиту от вмешательства в процесс функционирования систем Учреждения посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

5) разграничение доступа субъектов доступа и иных пользователей к информационным, аппаратным, программным и иным ресурсам – обеспечение доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей;

6) обеспечение аутентификации субъектов доступа и иных пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

7) защиту от несанкционированной модификации используемых в системах программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;

8) защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

4.6 Основные цели обеспечения информационной безопасности и решение перечисленных выше задач достигаются:

1) учётом всех подлежащих защите информационных систем Учреждения;

2) учётом действий персонала, в том числе сторонних организаций, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы (внутренней сети Учреждения);

3) полнотой, реальной выполнимостью и непротиворечивостью требований локальных нормативных актов Учреждения по вопросам обеспечения информационной безопасности;

4) подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности;

5) наделением каждого работника (субъекта доступа или иного пользователя) Учреждения минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Учреждения;

6) четким знанием и строгим соблюдением всеми субъектами доступа и иными пользователями информационных систем Учреждения требований локальных нормативных актов Учреждения по вопросам обеспечения информационной безопасности;

7) персональной ответственностью за свои действия каждого работника, имеющего доступ к информационным ресурсам Учреждения в рамках своих должностных обязанностей;

8) непрерывным поддержанием необходимого уровня защищенности элементов информационных систем Учреждения;

9) применением программно-аппаратных средств защиты информации и непрерывной административной поддержкой их использования;

10) эффективным контролем над соблюдением субъектами доступа и иными пользователями информационных ресурсов Учреждения требований по обеспечению информационной безопасности.

5. Основные угрозы информационной безопасности Учреждения

5.1 Существует два вида угроз информационной безопасности:

1) искусственные – угрозы, вызванные деятельностью человека;

2) естественные – угрозы, вызванные воздействиями на информационную систему и ее элементы объективных физических процессов техногенного характера или стихийных природных явлений, не зависящих от человека.

5.2 Наиболее значимыми угрозами информационной безопасности Учреждения (способами нанесения ущерба субъектам информационных отношений) являются:

1) нарушение функциональности компонентов информационных систем Учреждения, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;

2) нарушение целостности (искажение, подмена, уничтожение) информационных ресурсов Учреждения, а также фальсификация (подделка) документов;

3) нарушение конфиденциальности (разглашение, утечка) конфиденциальной информации, в том числе персональных данных.

5.3. Основные источники угроз информационной безопасности Учреждения:

1) непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи конфиденциальной информации, а также требований безопасности информации и другие действия субъектов доступа и иных пользователей информационных систем Учреждения (в том числе работников, отвечающих за обслуживание и администрирование элементов информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем;

2) преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам Учреждения субъектов доступа (в том числе работников, отвечающих за обработку конфиденциальной информации, обслуживание и администрирование элементов информационных систем), которые приводят к непроизводительным затратам времени и ресурсов, разглашению информации и сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем Учреждения;

3) удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (прежде всего через сеть «Интернет»), через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к информационным ресурсам;

4) ошибки, допущенные при разработке элементов информационных систем Учреждения и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации);

5) технические сбои элементов информационных систем.

5.4 Пути реализации угроз информационной безопасности Учреждения.

5.4.1 Пути реализации непреднамеренных искусственных угроз информационной безопасности Учреждения. Работники Учреждения, являющиеся авторизованными субъектами доступа информационных систем (субъектами доступа к конфиденциальной информации), а также работники, обслуживающие отдельные элементы информационных систем, являются внутренними источниками случайных воздействий. Основные пути реализации непреднамеренных искусственных (субъективных) угроз информационной безопасности Учреждения (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

1) неосторожные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем Учреждения;

2) неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие ее общедоступной;

3) разглашение, передача или утрата атрибутов разграничения доступа (ключей (логинов), паролей, ключевых носителей и т. п.);

4) игнорирование установленных правил при работе с информационными ресурсами, в том числе халатное отношение к носителям информации;

5) проектирование алгоритмов обработки данных, разработка программного обеспечения с возможностями, представляющими опасность для функционирования информационных систем и информационной безопасности Учреждения;

6) пересылка информации по ошибочному электронному адресу (устройства);

7) ввод ошибочных данных;

8) неосторожная порча носителей информации;

9) неосторожное повреждение каналов связи;

10) неправомерное отключение оборудования или изменение режимов работы элементов информационных систем;

11) заражение компьютеров вирусами;

12) несанкционированный запуск технологических программ, способных вызвать потерю работоспособности элементов информационных

систем или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных);

13) некомпетентное использование, настройка или неправомерное отключение средств защиты.

5.4.2 Пути реализации преднамеренных искусственных (субъективных) угроз информационной безопасности.

Основные возможные пути умышленной дезорганизации работы, вывода элементов информационных систем из строя, несанкционированного доступа к конфиденциальной информации (с корыстными целями, по принуждению, из желания отомстить):

1) умышленные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем Учреждения;

2) действия по дезорганизации функционирования информационных систем Учреждения, хищение электронных документов и носителей информации;

3) умышленное оставление документов и других носителей информации без присмотра, в неположенных местах, нарушение правил хранения;

4) несанкционированное копирование электронных документов и носителей информации;

5) умышленное искажение информации, ввод неверных данных;

6) отключение или вывод из строя подсистем обеспечения функционирования элементов информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи);

7) перехват данных, передаваемых по каналам связи и их анализ;

8) незаконное получение атрибутов разграничения доступа (используя халатность пользователей, путем подделки, подбора пароля);

9) несанкционированный доступ к ресурсам информационных систем с рабочих станций авторизованных субъектов доступа;

10) хищение или вскрытие шифров криптозащиты информации;

11) внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования элементов информационных систем Учреждения;

12) незаконное использование элементов информационных систем, нарушающее права обладателей конфиденциальной информации и третьих лиц;

13) применение подслушивающих устройств, фото и видео съемка для несанкционированного съема информации.

5.5 Пути реализации основных естественных угроз информационной безопасности:

1) выход из строя оборудования информационных систем и оборудования обеспечения его функционирования;

2) выход из строя или невозможность использования линий связи;

3) пожары, стихийные бедствия и иные форс-мажорные ситуации.

5.6. Модель возможных нарушителей защиты конфиденциальной информации.

5.6.1. Типы нарушителей:

1) с учетом категории лиц, мотивации, квалификации, наличия специальных средств:

- некомпетентный (невнимательный) пользователь – работник Учреждения (или подразделения внешней организации, занимающейся обслуживанием информационных систем Учреждения), предпринимающий попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационных систем с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией, действуя по ошибке, некомпетентности или халатности без умысла и использующий при этом только штатные средства;

- делитант – работник Учреждения (или подразделения внешней организации, занимающейся обслуживанием информационных систем Учреждения), пытающийся нарушить систему защиты без корыстных целей, умысла или для самоутверждения.

При этом используются различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств), нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства;

- внутренний (внешний) злоумышленник - авторизованный субъект доступа (постороннее лицо) действующий целенаправленно (в том числе в сговоре с лицами, не являющимися работниками Учреждения). При этом используются методы и средства взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Учреждения;

5.6.2 Внутренние нарушители:

Внутренним нарушителем может быть лицо из следующих категорий работников Учреждения:

1) работники Учреждения, имеющие легальный доступ к конфиденциальной информации, зарегистрированные пользователи и персонал, обслуживающий технические средства информационных систем Учреждения;

2) работники, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам Учреждения, но имеющие доступ в здания и помещения;

3) работники, задействованные в разработке и сопровождении программного обеспечения.

5.6.3 Внешние нарушители:

Внешним нарушителем может быть лицо из следующих категорий:

1) работники Учреждения, с которыми прекращен (расторгнут) трудовой договор, ранее имевшие доступ к конфиденциальной информации;

2) представители внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием элементов информационных систем;

3) члены преступных организаций или лица, действующие по их заданию;

4) лица, случайно или умышленно проникшие в локальную электронноцифровую сеть Учреждения из внешних телекоммуникационных сетей (хакеры);

5) администраторы автоматизированных систем Учреждения, имеющие неограниченный доступ к информационным ресурсам компонентов корпоративной информационной системы.

Администраторы автоматизированных систем могут относиться как к внешним, так и к внутренним нарушителям.

5.7 Утечка информации по техническим каналам.

При проведении мероприятий и эксплуатации технических средств устанавливаются следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

1) побочные электромагнитные излучения информативного сигнала от технических средств Учреждения и линий передачи информации;

2) наводки информативного сигнала, обрабатываемого техническими средствами локальной вычислительной сети Учреждения, на провода и линии, выходящие за пределы контролируемой зоны Учреждения, в том числе на цепи заземления и электропитания;

3) электрические сигналы или радиоизлучения, обусловленные воздействием на средства передачи информации высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.);

4) информативные сигналы;

5) акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;

6) электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;

7) вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации выделенных помещений;

8) воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе электромагнитное, через специально внедренные электронные и программные средства («закладки»);

9) перехват информации или воздействие на нее с использованием технических средств может вестись непосредственно из зданий, расположенных в непосредственной близости от объекта, мест временного пребывания, заинтересованных в перехвате информации или воздействии на нее лиц при посещении ими Учреждения, а также с помощью скрытно устанавливаемой автономной автоматической аппаратуры.

6. Основные принципы построения системы защиты конфиденциальной информации

Построение системы защиты конфиденциальной информации Учреждения и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

6.1 Законность.

Предполагает осуществление защитных мероприятий и разработку системы защиты конфиденциальной информации Учреждения в соответствии с законодательством РФ в области информации, информатизации и защиты информации.

Принятые меры информационной безопасности не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством РФ случаях к ресурсам конкретных информационных систем. Все субъекты доступа к конфиденциальной информации и пользователи информационных систем Учреждения должны иметь представление об ответственности за правонарушения в области информации.

6.2 Системность.

Системный подход к построению системы защиты конфиденциальной информации в Учреждении предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности Учреждения. При создании системы защиты учитываются все слабые и наиболее уязвимые места информационных систем Учреждения, а также характер, возможные объекты и направления атак на неё со стороны нарушителей, пути несанкционированного доступа к информации. Система защиты должна строиться с учетом возможности появления принципиально новых путей реализации угроз безопасности.

6.3 Комплексность.

Комплексное использование методов и средств защиты информационных систем предполагает согласованное применение программных и технических

средств при построении целостной системы защиты, перекрывающей все значимые каналы реализации угроз. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

6.4. Непрерывность защиты.

Для обеспечения этого принципа необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, перераспределение полномочий). Для информации, находящейся в документации традиционного вида, важно её хранение в строго отведённых местах, сейфах (ящиках), запертых на ключ либо запертых с помощью цифровой и иной кодификации. Порядок получения доступа к информационным ресурсам и ответственность за обработку и защиту конфиденциальной информации регламентируется в локальных нормативных актах Учреждения.

6.5 Своевременность.

Предполагается упреждающий характер мер обеспечения информационной безопасности, то есть постановка задач по комплексной защите информации и реализация мер обеспечения безопасности информации на ранних стадиях разработки информационных систем. Разработка системы защиты ведется параллельно с разработкой и развитием самой подлежащей защите информационной системы.

6.6 Преемственность и совершенствование.

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем Учреждения и систем информационной защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

6.7 Персональная ответственность.

Предполагает возложение ответственности за обеспечение информационной безопасности на каждого работника, имеющего доступ к конфиденциальной информации, в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

6.8 Минимизация полномочий.

Предполагает предоставление субъектам доступа и пользователям минимальных прав доступа к конфиденциальной информации в соответствии со служебной необходимостью. Доступ к конфиденциальной информации должен предоставляться только в том случае и объёме, если это необходимо работнику для выполнения его должностных обязанностей.

6.9. Гибкость системы информационной безопасности.

Предполагает способность системы информационной безопасности реагировать на изменения внешней среды и условий осуществления Учреждением своей деятельности.

В число таких изменений входят:

1) изменения организационной и штатной структуры Учреждения;

2) изменение существующих или внедрение принципиально новых информационных систем;

3) ввод в эксплуатацию новых технических средств;

4) изменение направлений деятельности Учреждения;

5) изменение правил делопроизводства в Учреждении.

6.10. Простота применения средств защиты.

Механизмы и методы системы защиты конфиденциальной информации должны быть понятны и просты в использовании. Применение средств и методов защиты не связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе субъектов доступа и зарегистрированных пользователей, а также не требует от них выполнения малопонятных им операций.

6.11 Обоснованность и техническая реализуемость.

Информационные технологии, технические и программные средства, средства и меры защиты конфиденциальной информации реализуются на современном техническом уровне и обоснованы для достижения заданного уровня безопасности конфиденциальной информации и экономической целесообразности, а также соответствуют установленным нормам и требованиям по безопасности информации.

6.12 Специализация и профессионализм.

Привлекаться к разработке средств и реализации мер защиты информации должны специализированные организации, наиболее подготовленные к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты осуществляется профессионально подготовленными специалистами защиты информации Учреждения в соответствии с должностными инструкциями.

6.13 Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных локальными нормативными актами правил обеспечения безопасности конфиденциальной информации в Учреждении.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты осуществляется на основе применения средств оперативного контроля и регистрации и охватывает санкционированные и несанкционированные действия пользователей. Выявленные работниками Учреждения недостатки системы защиты

информации доводятся до сведения непосредственного руководителя. О существенных недостатках сообщается руководителю Учреждения.

7. Меры, методы и средства обеспечения информационной безопасности

7.1 Меры обеспечения информационной безопасности.

7.1.1 К законодательным (правовым) мерам обеспечения информационной безопасности относятся действующие в Российской Федерации законодательные и иные нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры обеспечения информационной безопасности носят упреждающий, профилактический характер и требуют постоянной разъяснительной работы с работниками (пользователями) и обслуживающим персоналом информационных систем Учреждения.

7.1.2. К технологическим мерам обеспечения информационной безопасности относятся технологические решения и приемы, направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

7.1.3. Организационные (административные) меры обеспечения информационной безопасности – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. Организационными (административными) мерами обеспечения информационной безопасности являются:

1) регламентация доступа в здание (помещения) Учреждения;

2) регламентация допуска работников к использованию информационных ресурсов;

3) анализ требований к элементам системы на основе заявок пользователей на обслуживание и модификацию аппаратных и программных ресурсов;

4) обеспечение и контроль физической целостности (неизменности конфигурации) средств электронно-цифровой техники;

5) регламентация хранения и работы с документацией, содержащей конфиденциальную информацию;

6) обучение работников, имеющих в силу должностной компетенции к конфиденциальной информации, пользователей внутренней сети и иных электронно-цифровых систем в Учреждении;

7) деятельность по обеспечению информационной безопасности;

8) условия обработки информационных ресурсов конфиденциального

характера, ответственность за нарушения установленного порядка пользования информационными ресурсами Учреждения.

7.1.4. Физические меры обеспечения информационной безопасности основаны на применении механических, электронных или электронноцифровых устройств, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к элементам информационных систем и защищаемой информации.

7.1.5. Технические (аппаратно-программные) меры обеспечения информационной безопасности основаны на использовании электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации).

8. Обязанности и права должностных лиц Учреждения

8.1. Директор Учреждения организует работу по построению системы защиты информационной системы, в том числе приказом:

1) назначает ответственного за организацию защиты конфиденциальной информации из числа работников Учреждения. Данные полномочия обязательно отражаются в должностной инструкции работника;

2) утверждает круг лиц, имеющих доступ к защищаемой конфиденциальной информации, перечень и объём конфиденциальной информации, к которой имеет допуск работник, занимающий определённую должность, порядок их работы с такой информацией. Все перечисленные в приказе работники должны быть под роспись ознакомлены с приказом;

3) утверждает комплект документов, определяющих политику в отношении защиты конфиденциальной информации в Учреждении, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ.

8.2. Лицо, ответственное за защиту конфиденциальной информации:

1) разрабатывает локальные нормативные акты и организационно-распорядительные документы по вопросам защиты конфиденциальной информации при её обработке с помощью информационной системы;

2) контролирует исполнение законодательных и иных нормативных правовых актов, приказов и распоряжений вышестоящих органов и Учреждения по вопросам обеспечения безопасности информации;

3) обеспечивает защиту конфиденциальной информации, циркулирующей на объектах информатизации;

4) проводит систематический контроль работы систем защиты информации, применяемых в информационной системе, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности конфиденциальной информации;

5) проводит инструктаж работников, имеющих доступ к конфиденциальной информации и/или пользователей информационной системы Учреждения;

6) контролирует выполнение администратором информационной системы обязанностей по обеспечению функционирования систем защиты конфиденциальной информации (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам информационной системы, антивирусная защита, резервное копирование данных и т.д.);

7) контролирует порядок учёта и хранения бумажных и машинных носителей конфиденциальной информации;

8) участвует в работах по внесению изменений в аппаратно-программную конфигурацию информационной системы;

9) определяет порядок и осуществляет контроль ремонта средств электронно-цифровой техники, входящих в состав информационной системы;

10) принимает меры по оперативному изменению паролей (ключей доступа) при увольнении или перемещении сотрудников, имевших допуск к информационной системе;

11) требует устранения выявленных нарушений и недостатков, дает обязательные для исполнения указания по вопросам обеспечения положений законодательных и иных нормативных правовых и локальных актов по защите конфиденциальной информации;

12) требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;

13) в случае выявления попыток несанкционированного доступа к конфиденциальной информации или попыток хищения, копирования, изменения, незамедлительно принимает меры пресечения и докладывает директору Учреждения;

14) об имеющихся недостатках и выявленных нарушениях требований нормативных и распорядительных документов по защите конфиденциальной информации, а также в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите конфиденциальной информации.

8.3. Каждый работник, имеющий доступ к конфиденциальной информации, в том числе к персональным данным, подписывает обязательство о неразглашении конфиденциальной информации, в том числе персональных данных.

8.4 Работник, имеющий доступ к конфиденциальной информации Учреждения, обязан:

1) соблюдать установленный режим охраны такой информации;

2) не разглашать конфиденциальные сведения, ставшие ему известными из письменных, устных и иных источников и не использовать эту информацию в личных целях;

3) обеспечить невозможность утраты (целостность и сохранность, соблюдение порядка хранения) бумажных и электронных документов, содержащих указанные сведения;

4) обеспечить невозможность несанкционированного доступа к документам, информационным системам, содержащим конфиденциальную информацию и находящимся в его ведении;

5) передать ответственному лицу при прекращении трудовых, образовательных и иных гражданско-правовых отношений с Учреждением, имеющиеся в пользовании работника материальные и иные носители конфиденциальной информации;

6) работать только с теми конфиденциальными сведениями и документами, к которым он получил доступ в силу своих должностных обязанностей, знать, какие конкретно сведения подлежат защите, и строго соблюдать правила использования и защиты конфиденциальной информации;

7) незамедлительно сообщить директору Учреждения о пропаже, искажении, подделке документов, электронно-цифровых, в том числе съёмных, носителей информации, содержащих конфиденциальные сведения, а также о несанкционированном доступе не управомоченных лиц к такой информации, или о попытке подобного доступа.

8.5 По факту разглашения конфиденциальной информации, потери, искажения, фальсификации документов и иного несанкционированного доступа к конфиденциальной информации, проводится служебное расследование, по результатам которого виновные лица привлекаются к ответственности.

8.6 Предоставление конфиденциальной информации Учреждения третьим лицам возможно только с разрешения директора Учреждения, а конфиденциальной информации (персональных данных) работников, обучающихся, их родителей (законных представителей) и иных обладателей информации, возможно только с их письменного согласия (за исключением случаев, установленных законодательством РФ).

8.7 При привлечении к деятельности Учреждения третьих лиц работник Учреждения, ответственный за обработку и защиту конфиденциальной информации, может знакомить их представителей с конфиденциальной информацией только с письменного разрешения директора. Директор учреждения при этом должен определить конкретные вопросы, подлежащие рассмотрению, и указать, кому, какая и в каком объеме может быть предоставлена конфиденциальная информация, подлежащая защите.

9. Ответственность за нарушение порядка работы и защиты конфиденциальной информации

9.1 Несоответствие деятельности и мер, предпринимаемых руководителем и работниками Учреждения установленным требованиям или нормам по защите конфиденциальной информации, является нарушением и влечёт ответственность виновных лиц в соответствии с законодательством РФ.

9.2 Сотруднику, который в связи с исполнением трудовых обязанностей

на основании приказа директора Учреждения получил доступ к конфиденциальной информации, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого сотрудника состава преступления, в соответствии со статьёй 192 Трудового кодекса Российской Федерации назначается дисциплинарное взыскание.

9.3 Работник Учреждения, осуществляющий сбор конфиденциальной информации незаконными способами в целях разглашения либо незаконного использования этих сведений, а также за их разглашение или незаконное использование, совершенные из корыстной или иной личной заинтересованности и причинивший крупный ущерб Учреждению, в соответствии со статьёй 183 Уголовного кодекса Российской Федерации (далее – УК РФ) несёт уголовную ответственность.

9.4 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

9.5 За нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные с использованием своего служебного положения, виновные лица несут уголовную ответственность и могут понести наказание в виде штрафа, лишения права занимать определенные должности или заниматься определенной деятельностью, арестом в соответствии с УК РФ.

Приложение

к Положению о конфиденциальной информации
в Муниципальном бюджетном учреждении культуры
«Одинцовский Центр культурного развития»

**Перечень сведений конфиденциального характера
в Муниципальном бюджетном учреждении культуры
«Одинцовский Центр культурного развития»**

1. Персональные данные (любая информация, относящиеся прямо или косвенно к определенному или определяемому физическому лицу).
2. Сведения о личной (семейной) тайне. Сведения о частной жизни. Сведения, раскрывающие тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.
3. Сведения, предоставляемые участниками торгов в соответствии с правилами организованных торгов.
4. Сведения, содержащиеся в материалах служебных расследований (проверок) до издания соответствующих распорядительных документов.
5. Сведения о системах защиты информации (средства, методы и способы защиты информации, реквизиты доступа, матрицы доступа и процедуры доступа к информационным системам и ресурсам).
6. Сведения об информационно-телекоммуникационных сетях и каналах связи, компьютерных сетях, средствах вычислительной техники, программном обеспечении, системах и средствах охрано - тревожной, пожарной сигнализации и видеонаблюдения.
7. Сведения о деятельности конкурсных, аукционных и других подобных комиссий и об оценке предложений до момента утверждения победителя закупочной процедуры.
8. Несекретная информация, касающаяся деятельности учреждения, ограничения на распространения которой диктуются служебной необходимостью.