Приложение №1
к приказу от 30.09.2024 № 46

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ «ОДИНЦОВСКАЯ КОНЦЕРТНАЯ ОРГАНИЗАЦИЯ» (МБУК «ОКО»)

Положение об информационной безопасности

1. Общие положении

1.1. Положение об информационной безопасности МБУК "ОКО" (далее - Учреждение) определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Учреждение в своей деятельности. Информационная безопасность является одним из составных элементов комплексной безопасности Учреждения.

1.2. Данное положение разработано в соответствии с Постановление Правительства РФ от 11.02.2017 М 176 (фед. от 13.02.2018) "Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий)", Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.), Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных".

1.3. Под информационной безопасностью Учреждения следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

Основной целью Положения являются защита информации Учреждения. Положение об информационной безопасности направлено на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников (террористов), уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации, и обеспечение нормального функционирования технологических процессов.

Общее руководство обеспечением информационной безопасности осуществляет заместитель директора. Ответственность за организацию мероприятий по обеспечению информационной безопасности и контроль за соблюдением требований ИБ несет инженер ведущий.

Настоящее Положение распространяется на все структурные подразделения Учреждения и обязательно для исполнения всеми его сотрудниками и должностными лицами. Положение применимо для использования во внутренних нормативных и методических документах, а также в договорах. Сотрудники Учреждения обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой

информации и другой защищаемой информации, соблюдать требования настоящего Положения и других документов ИБ.

Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

Организация просвещения сотрудников Учреждения в области информационной безопасности возлагается на инженера ведущего. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности».

Обучение сотрудников Учреждения правилам обращения с конфиденциальной информацией, проводится путем:

- проведения инженером ведущим вводного инструктажа по информационной безопасности с сотрудниками, принимаемыми на работу в Учреждение;
- самостоятельного изучения сотрудниками внутренних нормативных документов Учреждения.

Допуск персонала к работе с защищаемыми информационными ресурсами Учреждения осуществляется только после его ознакомления с настоящим Положением. Согласие на соблюдение правил и требований настоящего Положения подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Защищаемые информационные ресурсы Учреждения.

Различаются следующие категории информационных ресурсов, подлежащих защите в Учреждении:

- конфиденциальная - информация, определенная в соответствии с Федеральным Законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ от 27.07.2006 г. №152-ФЗ «О персональных данных», указом президента РФ от 06.03.1997 №138 «Об утверждении перечня сведений конфиденциального характера», постановлением правительства РФ от 17.11.2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений конфиденциального характера.
- публичная - информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах;
- открытая - информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная в результате деятельности Учреждения, которую запрещено относить к конфиденциальной на основании законодательства России. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности Учреждения;
- ограниченного доступа - информация, не попадающая под остальные категории, доступ к которой должен быть ограничен для определенной категории лиц.

- конфиденциальная - информация представляет собой сведения ограниченного доступа, включая персональные данные, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

Подходы к решению проблемы защиты информации в Учреждении, в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования процессов Учреждения.

Для этого в Учреждении выполняются следующие мероприятия:

- устанавливается круг лиц и порядок доступа к подобной информации;

- вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;

- в трудовые договоры с сотрудниками включаются обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Форма подписки о неразглашении сведений конфиденциального характера подписывается при заключении трудового договора, который подписывается работником Учреждения при приеме на работу в Учреждение.

Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Учреждением с другими организациями.

Персональные данные сотрудника Учреждения - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

Согласно ст. 86 п. 7 Трудового кодекса РФ защита персональных данных сотрудника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

Согласно ст. 88 Трудового кодекса РФ при передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

- осуществлять передачу персональных данных сотрудника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым сотрудник должен быть ознакомлен под расписку;

- разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций.

Согласно ст. 90 Трудового кодекса РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

К информации ограниченного доступа в Учреждении относится Акт обследования и категорирования объектов и Паспорт безопасности объекта.

Паспорт безопасности объекта (территории) является документом, содержащим служебную информацию ограниченного распространения, и имеет пометку "Для служебного пользования".

Паспорт безопасности объекта (территории) составляется комиссией в 2 экземплярах, подписывается членами комиссии, утверждается руководителем Учреждения и согласовывается (в том числе при его актуализации) с территориальным органом безопасности, территориальным органом Федеральной службы войск национальной гвардии Российской Федерации или подразделением вневедомственной охраны войск национальной гвардии Российской Федерации по месту нахождения объекта (территории) в 30 - дневный срок со дня его составления.

Первый экземпляр Паспорта безопасности объекта (территории) хранится на объекте (территории). Второй экземпляр направляется в вышестоящую организацию в сфере культуры.

Копия (электронная копия) Паспорта безопасности объекта (территории) направляется в территориальный орган безопасности и территориальный орган Министерства внутренних дел Российской Федерации по месту нахождения объекта (территории).

1.4. К объектам информационной безопасности в учреждении относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера и ограниченного доступа;
- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. персональные данные;
- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

1.5. Система информационной безопасности (далее - СИБ) должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

1.6. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая зашита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная зашита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

2. Правовые нормы обеспечения информационной безопасности

2.1. Учреждение имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных работников, информации ограниченного доступа, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

Допуск в Учреждении имеют:

к конфиденциальной информации:

- директор;
- заместитель директора;
- главный бухгалтер;
- заместитель главного бухгалтера;
- специалист по кадрам;
- документовед.

Ответственность за сохранность документации несет индивидуально каждый сотрудник Учреждения, допущенный к конфиденциальной информации, согласно должностной инструкции и трудовому договору.

К информации ограниченного доступа, в т.ч. ограничения доступа должностных лиц (работников) к служебной информации ограниченного распространения, содержащейся в паспорте безопасности объекта (территории), иных документах и на других материальных носителях информации:

- директор;
- заместитель директора;
- инженер ведущий;
- начальник АХО.

Ответственность за сохранность документации несет индивидуально каждый сотрудник Учреждения, допущенный к информации ограниченного доступа, согласно должностной инструкции и трудовому договору.

Ответственность за хранение паспорта безопасности объекта (территории), иных документов и других материальных носителей информации, содержащих сведения о состоянии антитеррористической защищенности объекта (территории) и принимаемых мерах по се усилению несет инженер ведущий.

Ответственность за организацией и осуществлением контроля за обеспечением установленного порядка работы со служебной информацией ограниченного распространения и ее хранения в целях выявления и предупреждения возможной утечки служебной информации ограниченного распространения, в том числе содержащейся в паспорте безопасности объекта (территории), иных документах и на других материальных носителях информации несет заместитель директора.

Учреждение:

- имеет право издавать нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;

- имеет право включать требования по защите информации в договоры по всем видам деятельности;

- имеет право разрабатывать дополнительно перечень сведений конфиденциального характера;

- имеет право разрабатывать дополнительно перечень сведений ограниченного доступа;

- имеет право требовать защиты интересов Учреждения со стороны государственных и судебных инстанций.

2.2. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора о назначении ответственного за обеспечение информационной безопасности;

- должностные обязанности ответственного за обеспечение информационной безопасности;

- перечень защищаемых информационных ресурсов и баз данных.

2.3. Порядок допуска сотрудников Учреждения к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера и сведений ограниченного доступа;

- ознакомление работника с нормами законодательства РФ и Учреждения об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

- инструктаж работника специалистом по информационной безопасности;

- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера и ограниченного доступа.

3. Мероприятия по обеспечению информационной безопасности.

Для обеспечения информационной безопасности в Учреждении требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности Учреждения;

- защита компьютеров, локальных сетей и сети подключения к системе Интернета;

- организация защиты конфиденциальной информации, в т. ч. Персональных данных работников:

- учет всех носителей конфиденциальной информации.

4. Организация работы с информационными ресурсами и технологиями.

4.1. Система организации делопроизводства:

- учет всей документации Учреждения, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

- регистрация и учет всех входящих (исходящих) документов в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

- особый режим уничтожения документов.

4.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

4.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

4.2.2. Документы, дела и издания с грифом конфиденциальности и особого доступа должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

4.2.3. Передача документов исполнителю производится только через ответственного за сохранность данного документа.

4.2.4. Запрещается выносить документы с грифом " Ограниченного доступа" за пределы Учреждения.

4.2.5. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема - передачи документов.

4.3. Для организации делопроизводства приказом директора Учреждения назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором Учреждения. Контроль за порядком его ведения возлагается на заместителя директора.

5. Обеспечение безопасности АРМ.

Основные правила предоставления сотрудникам доступа к автоматизированному рабочему месту (АРМ) и защищаемым информационным ресурсам.

К работе с информационным ресурсом допускаются пользователи, назначенные ответственными за работу в информационных ресурсах и ознакомленные с правилами работы, а также ответственностью за их нарушение.

Каждому сотруднику Учреждения, допущенному к работе с конкретным информационным ресурсом, должно быть присвоено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИР.

В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей).

Порядок пользования учетной записью пользователя.

При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться.

В случае необходимости сохранения персональных документов (профайла пользователя) на АРМ сотрудника, после прекращения срока действия его полномочий, его непосредственный руководитель должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия своих полномочий) подать заявку на блокирование учетной записи пользователя с указанием срока хранения указанной информации.

Регистрационные учетные записи подразделяются на:

- пользовательские - предназначенные для идентификации/аутентификации пользователей информационных активов;

- системные - используемые для нужд операционной системы;

- служебные - предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов Учреждения назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

На каждом АРМ и системе должен быть установлен пароль пользователя.

На каждом АРМ должна быть активна система лицензионной антивирусной защиты.

Основные правила и требования по защите конфиденциальной информации, информации ограниченного доступа и персональных данных и иной информации Учреждения неавторизованного доступа, утраты или модификации.

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с документами, согласно занимаемой должности.

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратор информационной безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками Учреждения. Запрещается использование указанных АРМ другими пользователями без согласования с заместителем директора. При передаче указанного АРМ другому пользователю, должна производиться гарантированная очистка диска (форматирование).