УТВЕРЖДЕНО

приказом МБУК ЦКС УГО

от «19» 07 2019 г. № 125

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МУНИЦИПАЛЬНОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ КУЛЬТУРЫ «ЦЕНТРАЛИЗОВАННАЯ КЛУБНАЯ СИСТЕМА» УССУРИЙСКОГО ОКРУГА

Уссурийск

2019 год

1. Общие положения

1.1. Настоящая Политика информационной безопасности муниципального бюджетного учреждения культуры «Централизованная клубная система» Уссурийского городского округа (далее – Политика), (Далее - МБУК ЦКС УГО), разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», на основании: - «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Заместителем директора ФСТЭК России от 15.02.2008 г., «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662, является официальным документом и обязательным для исполнения всеми структурными подразделениями и должностными лицами Учреждения.

1.2. В Политике определены степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.3. Обработка персональных данных работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

1.4. Для целей настоящей Политики используются следующие основные понятия:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных работника - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение

персональных данных;

распространение персональных данных - действия, направленные на раскрытие персональных данных работников неопределенному кругу лиц;

предоставление персональных данных - действия, направленные на раскрытие персональных данных работников определенному лицу или определенному кругу лиц;

блокирование персональных данных - временное прекращение обработки персональных данных работников (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников;

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному работнику.

2. Цель

2.1. Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков информационной безопасности (далее – ИБ).

2.2. Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

1. своевременное выявление, оценка и прогнозирование источников угроз ИБ;
2. создание механизма оперативного реагирования на угрозы ИБ;
3. предотвращение и/или снижение ущерба от реализации угроз ИБ;
4. защита от вмешательства в процесс функционирования ИС посторонних лиц;
5. соответствие требованиям Федерального законодательства, нормативно-методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ;
6. достижение адекватности мер по защите от угроз ИБ;
7. недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
8. выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;
9. повышение деловой репутации и корпоративной культуры.

3. Область действия

Требования настоящей Политики распространяются на всех сотрудников учреждения (штатных, временных, работающих по контракту, договору и т.п.), а также всех прочих лиц (участники клубных формирований и т.п.).

4. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются следующие:

1. постоянный и всесторонний анализ информационного пространства МБУК ЦКС УГО с целью выявления уязвимостей информационных активов;
2. своевременное обнаружение проблем, потенциально способных повлиять на МБУК ЦКС УГО, корректировка моделей угроз и нарушителя;
3. разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей МБУК ЦКС УГО, а также повышать трудоемкость технологических процессов обработки информации;
4. контроль эффективности принимаемых защитных мер;
5. персонификация и адекватное разделение ролей и ответственности между сотрудниками МБУК ЦКС УГО, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

5.1. Организация просвещения сотрудников МБУК ЦКС УГО в области информационной безопасности возлагается на администратора информационной безопасности. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности». Обучение сотрудников МБУК ЦКС УГО правилам обращения с конфиденциальной информацией, проводится путем:

5.1.1. проведения ответственным за защиту информации в ИСПДн «МБУК ЦКС УГО» инструктивных занятий с сотрудниками, принимаемыми на работу в МБУК ЦКС УГО;

5.1.2. самостоятельного изучения сотрудниками внутренних нормативных документов МБУК ЦКС УГО.

5.2. Допуск персонала к работе с защищаемыми информационными ресурсами МБУК ЦКС УГО осуществляется только после его ознакомления с настоящими политиками, а также после ознакомления пользователей с «Инструкцией по работе пользователей в ИСПДн МБУК ЦКС УГО». Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

6. Защищаемые информационные ресурсы МБУК ЦКС УГО

6.1.Конфиденциальная – информация, определенная в соответствии с Федеральным Законом от 27.07.2006г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", ФЗ от 27.07.2006г. № 152-ФЗ "О персональных данных", указом президента РФ от 06.03.1997г. № 188 "Об утверждении перечня сведений конфиденциального характера", постановлением правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» , предусмотренная Перечнем сведений конфиденциального характера.

6.2.Публичная – информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах;

6.3.Открытая – информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная в результате деятельности МБУК ЦКС УГО, которую запрещено относить конфиденциальной на основании законодательства России. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности МБУК ЦКС УГО или имеющая принципиальное значение для имиджа МБУК ЦКС УГО.

6.4.Ограниченного доступа – информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

6.5.Конфиденциальная информация представляет собой сведения ограниченного доступа, 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.

Для этого в МБУК ЦКС УГО выполняются следующие мероприятия:

- определяется порядок работы с документами, образцами изделиями и др., содержащими конфиденциальные сведения;
- устанавливается круг лиц и порядок доступа к подобной информации;
- вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;
- включаются в трудовые договоры с сотрудниками обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Форма расписки о неразглашении конфиденциальной информации подписывается при заключении трудового договора, который подписывается всеми сотрудниками учреждения при приеме на работу в МБУК ЦКС УГО.

7. Пользователи ИСПДн

В ИСПДн предприятия можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратор ;
- Операторы;

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положение о разграничении прав доступа к обрабатываемым персональным данным.

Администратор

Администратор - сотрудник учреждения ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя к элементам, хранящим персональные данные.

Администратор обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Оператор

Оператор, сотрудник предприятия, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

8. Политики информационной безопасности

8.1. Политика предоставления доступа к информационному ресурсу

8.1.1.Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым МБУК ЦКС УГО.

8.1.2. Положение Политики

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей политикой.

Каждому сотруднику МБУК ЦКС УГО, допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

8.2. Политика использования паролей

8.2.1.Назначение

Настоящая Политика определяет основные правила парольной защиты в МБУК ЦКС УГО.

8.2.2. Положение Политики

При выборе паролей необходимо исключить повторное использование или циклическое повторение старых паролей, избегать паролей из перечня доступных для автоматического подбора по словарю, не выбирать одиночные слова, набранные русскими буквами при латинской раскладке. Рекомендуется усиливать пароль использованием специальных символов или знаков препинания и увеличением длины до 9 символов и более.

8.3. Политика реализации антивирусной защиты.

8.3.1.Назначение

Настоящая Политика определяет основные правила для реализации антивирусной защиты в МБУК ЦКС УГО.

8.3.2. Положение

Настоящая Политика определяет единые требования по организации антивирусной защиты в МБУК ЦКС УГО.

К использованию в МБУК ЦКС УГО допускаются только лицензированные антивирусные средства, разрешённые для применения.

Актуализация всех версий используемых антивирусных средств и антивирусных баз проводится на регулярной основе.

Загрузка программного обеспечения и рабочих файлов на АРМ и прочие носители информации осуществляется с проведением предварительной их проверки антивирусными средствами.

8.4. Политика защиты автоматизированного рабочего места

8.4.1.Назначение

Настоящая Политика определяет основные правила и требования по защите информации МБУК ЦКС УГО от неавторизованного доступа, утраты или модификации.

8.4.2.Положения политики

Положения данной политики определяются в соответствии с используемым техническим решением.

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.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

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.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками МБУК ЦКС УГО. Запрещается использование указанных АРМ другими пользователями без согласования с директором. При передаче указанного АРМ другому пользователю, должна производится гарантированная очистка диска (форматирование).

9. Требования к персоналу по обеспечению защиты ПДн

9.1. Все сотрудники предприятия, являющиеся пользователями ИСПДн,

должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

9.2.При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

9.3.Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

9.4.Сотрудники предприятия, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированных действий к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

9.5.Сотрудники предприятия должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

9.6.Сотрудники предприятия должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

9.7.Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать носители информации, а так же записывать на них защищаемую информацию.

9.8.Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами предприятия, третьим лицам.

При работе с ПДн в ИСПДн сотрудники предприятия обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

9.9.Сотрудники предприятия должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

10. Ответственность сотрудников ИСПДн предприятия

10.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

10.2.Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

10.3. Ответственный за защиту информации несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

10.4.При нарушениях сотрудниками предприятия – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

11. Требований по обеспечению ИБ при использовании СКЗИ

11.1. Шифрование – это криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной или критичной информации.

СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения.

11.2. Порядок применения СКЗИ определяется руководством Учреждения и должен включать:

11.2.1. порядок ввода в действие, включая процедуры встраивания СКЗИ в ИС;

11.2.2. порядок эксплуатации;

11.2.3. порядок восстановления работоспособности в аварийных случаях;

11.2.4. порядок внесения изменений;

11.2.5. порядок снятия с эксплуатации;

11.2.6. порядок управления ключевой информацией;

11.2.7. порядок обращения с ключевой информацией, включая действия при смене и компрометации ключей.

При использовании шифрования в ИС Учреждения должны применяться только утверждённые стандартные алгоритмы и сертифицированные ФСБ России продукты, их реализующие.

11.3. Электронные цифровые подписи (далее ЭЦП).

ЭЦП обеспечивают защиту аутентификации и целостности электронных документов.

ЭЦП могут применяться для любой формы документа, обрабатываемого электронным способом. ЭЦП должны быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой – для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой, имеющий к нему доступ, может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Защиты целостности открытого ключа должна обеспечиваться при использовании сертификата открытого ключа.

При использовании ЭЦП, необходимо учитывать требования действующего законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

12. Управление инцидентами информационной безопасности

12.1. В Учреждении должна быть разработана и утверждена формальная процедура уведомления о происшествиях в области ИБ, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии.

12.2. Все сотрудники должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях.

12.3.В дополнение к уведомлению о происшествиях ИБ и недостатках безопасности должен использоваться мониторинг систем, сообщений и уязвимостей для обнаружения инцидентов ИБ.

Цели управления инцидентами ИБ должны быть согласованы с руководством для учёта приоритетов Учреждения при обращении с инцидентами.

13. Регулирующие законодательные нормативные документы

При организации и обеспечении работ по ИБ сотрудники МБУК ЦКС УГО должны руководствоваться следующими законодательными нормативными документами:

13.1. Основополагающие нормативные документы

К основополагающим нормативным документам относятся:

- конституция Российской Федерации;
- концепция национальной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 17.12.1997 N 1300, в редакции Указа Президента Российской Федерации N 24 от 10.01.2000);

13.2. Законы Российской Федерации

- Гражданский кодекс Российской Федерации.
- Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи";
- Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";
- Федеральный закон от 07.07.2003 N 126-ФЗ "О связи";
- Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ от 13.06.1996;

13.3. Указы и распоряжения президента Российской Федерации

- указ Президента Российской Федерации от 06.03.1997 N 188 "Об утверждении перечня сведений конфиденциального характера";

13.4. Нормативные и руководящие документы Федеральных служб Российской Федерации

- Приказ ФСБ Российской Федерации от 09.02.2005 N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение

ПКЗ-2005)";

14. Ответственность

14.1.Директор МБУК ЦКС УГО определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите, а также осуществляет общее руководство обеспечением ИБ МБУК ЦКС УГО.

14.2.Все руководители несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях.

14.3.Работники МБУК ЦКС УГО несут персональную ответственность за соблюдение требований документов и обязаны сообщать обо всех выявленных нарушениях ответственному за защиту информации в ИСПДн «МБУК ЦКС УГО».

14.4.Руководство МБУК ЦКС УГО регулярно проводит совещания, посвящённые проблемам обеспечения информационной безопасности с целью формирования чётких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ.

Нарушение требований нормативных актов МБУК ЦКС УГО по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

15. Контроль и пересмотр

15.1.Общий контроль состояния ИБ МБУК ЦКС УГО осуществляется Директором.

15.2.Текущий контроль соблюдения настоящей Политики осуществляет ответственный за защиту информации в ИСПДн «МБУК ЦКС УГО». Контроль осуществляется путем проведения мониторинга инцидентов ИБ МБУК ЦКС УГО, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

15.4.Все изменения, внесённые в настоящую Политику ИБ должны учитываться в листе «История изменений».