УТВЕРЖДАЮ
Директор МБУК
«Жигулевский ДК»
Ометова Л.В.
_____
«____»_____2019 г.

ПОЛИТИКА
информационной безопасности
МБУК «Жигулевский ДК»

Введение

Настоящая Политика информационной безопасности (далее – Политика) является официальным документом МБУК «Жигулевский ДК» (далее – учреждение), в котором определена система взглядов на обеспечение информационной безопасности для информационных систем персональных данных (далее – ИСПДн) учреждения.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), обрабатываемой в ИСПДн.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и приказа ФСТЭК № 17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищённости ИСПДн, статус и должностные обязанности работников, ответственных за обеспечение безопасности информации ИСПДн.

1. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты ИСПДн от всех видов угроз, внешних и внутренних, умышленных и не преднамеренных, минимизация ущерба от возможной реализации угроз безопасности информации (далее – УБИ).

Безопасность информации достигается путём исключения несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБИ.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций, или уничтожений данных.

2. Область действия

Требования настоящей Политики распространяются на всех работников учреждения (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3. Система защиты информации

Система защиты персональных данных (далее – СЗПДн) строится на основании:

- Перечня информационных систем персональных данных учреждения;
- Положения о разграничении прав доступа к обрабатываемой информации ограниченного доступа;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень значимости информации, обрабатываемой в ИСПДн. На основании анализа актуальных угроз безопасности информации, принимается решение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности информации.

Для ИСПДн составляется перечень используемых технических средств, а также программного обеспечения участвующего в обработке информации, на всех элементах ИСПДн.

В зависимости от класса защищённости ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства защиты информации:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации при передаче защищаемой информации по каналам связи и т.д.

В перечень должны быть включены функции защиты, обеспечиваемые штатными средствами обработки защищаемой информации ОС, прикладным ПО и специальными комплексами, реализующими средства защиты.

Список функций защиты может включать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- целостность информационной системы и информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

4. Требования к подсистемам СЗПДн

СЗПДн может включать в себя следующие подсистемы:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- - защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

5. Пользователи ИСПДн

В зависимости от категорий пользователей производится типизация пользователей ИСПДн, определяется их уровень доступа и возможности.

В ИСПДн можно выделить следующие группы пользователей, участвующих в обработке и хранении защищаемой Информации:

- Администратор безопасности;
- Оператор АРМ;
- Программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности должны быть отражены в «Положении о разграничении прав доступа к обрабатываемой информации ограниченного доступа».

5.1 Администратор безопасности

Администратор

_____ –

_____,

ответственный за настройку, внедрение и сопровождение ИСПДн, функционирование СЗПДн включая обслуживание и настройку административной, серверной и клиентской компонент. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим информацию.

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 ИСПДн;

- обладает правами конфигурирования и административной настройки технических средств ИСПДн в части касающейся;

- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.

Администратор безопасности уполномочен:

- реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;

- осуществлять аудит средств защиты.

5.2 Оператор АРМ

Оператор АРМ - работник, осуществляющий обработку информации. Обработка информации включает: просмотр, ручной ввод в систему, формирование справок и отчётов по информации, полученной из ИСПДн. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации;

- располагает конфиденциальными данными, к которым имеет доступ.

6. Требования к персоналу по обеспечению защиты информации

Все работники, являющиеся пользователями ИСПДн, должны чётко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ИСПДн.

При вступлении в должность нового работника ответственный по защите информации, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите информации, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

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

Работники, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Работники должны следовать установленным процедурам поддержания режима безопасности информации при выборе и использовании паролей (если не используются технические средства аутентификации).

Работники 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 информации и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

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

При работе с защищаемой информацией в ИСПДн работники обязаны обеспечить отсутствие возможности просмотра информации третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн работники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Работники должны быть проинформированы об угрозах нарушения режима безопасности информации 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 информации.

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

7. Должностные обязанности пользователей ИСПДн

Для исполнения должностных обязанностей пользователей ИСПДн разрабатываются следующие документы:

- Руководство администратора безопасности;
- Руководство пользователя ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций.

8. Ответственность

В соответствии со ст. 17 Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» лица, виновные в нарушении требований данного Федерального закона, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

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).

Администратор безопасности несет ответственность за все действия, совершенные от имени его учётных записей или системных учётных записей, если не доказан факт несанкционированного использования учётных записей.

При нарушениях работниками правил, связанных с безопасностью информации, они несут ответственность, установленную действующим законодательством Российской Федерации (ст. 5.39, 13.11, 13.12, 13.14, 13.31, 19.4, 19.5, 19.7.10, 23.44 КоАП, ст. 81, 90 ТК, ст. 137, 140, 183, 187 УК).

Список использованных источников

1. ФЗ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. ФЗ от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
3. ФЗ от 27.07.2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
4. Постановление Правительства РФ от 0.11.2012 г. № 1119 «Об утверждении требований к защите ПДн их обработке в ИСПДн»
5. Постановление Правительства РФ от 21.03.2 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных», операторами, являющимися государственными или муниципальными органами»;
6. Постановление Правительства РФ от 27.09.2011 г. № 797 «О взаимодействии между МФЦ предоставления государственных и муниципальных услуг и федеральными ОИВ, органами государственных внебюджетных фондов, органами государственной власти субъектов Российской Федерации, ОМСУ»;
7. Приказ ФСТЭК от 11.02.2013 г. № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в ГИС»;
8. Приказ ФСТЭК от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн»;
9. Методический документ «Меры защиты информации в ГИС» утвержденный ФСТЭК 11.02.2014 г.;
10. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая Зам. директора ФСТЭК 15 февраля 2008 г.;
11. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая Зам. директора ФСТЭК 15 февраля 2008 г.