Государственное профессиональное образовательное
автономное учреждение Ярославской области
Ярославский педагогический колледж

150029 г. Ярославль
улица Маланова, 14

Телефон: (4852) 32-64-14
Факс: (4852) 32-64-14

УТВЕРЖДАЮ

Директор ГПОАУ ЯО
Ярославского педагогического
колледжа _____ М.Е. Лавров

приказ директора
от 20.04.2017 № 110

Политика информационной безопасности ГПОАУ ЯО Ярославского педагогического колледжа

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее – Политика) разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных и на основании Приказа 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».

1.2. Целью настоящей Политики является обеспечение безопасности объектов защиты оператора информационной системы от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (далее – УБПДн) информационной системы.

1.3. 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.

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

1.5. Состав объектов защиты определяется Перечнем персональных данных, подлежащих защите в информационных системах персональных данных.

2. Область действия

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

3. Система защиты персональных данных

3.1. Система защиты персональных данных (СЗПДн) строится на основании:

- отчётов о результатах проведения внутренних проверок;

- Перечня персональных данных, подлежащих защите в информационных системах персональных данных;

- актов классификации информационной системы персональных данных;

- Порядка доступа работников ГПОАУ ЯО Ярославского педагогического колледжа в помещения, в которых ведётся обработка персональных данных;

- руководящих документов ФСТЭК, ФСБ России;

- иных нормативно-правовых и локальных актов в сфере обработки и защиты персональных данных.

3.2. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;

- средства межсетевого экранирования;

- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

3.3. В список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты (управление и разграничение доступа пользователей, обнаружение вторжений).

4. Антивирусная защита как средство защиты ПДн

4.1. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн оператора.

4.2. Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;

- антивирусное сканирование;

- скрипт-блокирование;

- централизованная/удаленная установка/деинсталляция антивирусного продукта, настройка, администрирование, просмотр отчётов и статистической информации по работе продукта;

- автоматизированное обновление антивирусных баз;

- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

- автоматический запуск сразу после загрузки операционной системы.

5. Пользователи ИСПДн

5.1. В ИСПДн оператора можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратор ИСПДН;

- администратор по информационной безопасности;

- пользователь ИСПДн (оператор АРМ).

5.2. Данные о группах пользователей, уровне их доступа и информированности, правах и обязанностях, полномочиях отражаются в приказах директора колледжа и локальных нормативных актах.

6. Требования к персоналу по обеспечению защиты ПДн

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

6.2. При вступлении в должность нового работника специалист по кадровой работе, а также непосредственный начальник подразделения, в которое поступает работник, обязаны 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.

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

6.4. Работники оператора 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.

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

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

6.7. При работе с ПДн в ИСПДн работники оператора обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

6.8. 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.

6.9. Работники 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.

7. Ответственность сотрудников ИСПДн колледжа

7.1. При нарушениях работниками колледжа правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.