МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
НАЧАЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 7
ГОРОДА ЮЖНО-САХАЛИНСКА

693007, г. Южно-Сахалинск, ул. им. Антона Буюклы, 14,
Тел.: (4242) 22-54-75, (4242) 22-54-76, факс: (4242) 22-54-76 Email: school7@yuzhno-sakh.ru

УТВЕРЖДЕНА
приказом директора
Муниципального автономного
общеобразовательного учреждения
начальная общеобразовательная
школа №7 города Южно-Сахалинска
от 14.11.2017 № 284 – ОД

Политика информационной безопасности

1. Общие положения

1.1. Политика информационной безопасности Муниципального автономного общеобразовательного учреждения начальная общеобразовательная школа №7 города Южно-Сахалинска (далее – образовательное учреждение) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности, которыми руководствуются работники ОО при осуществлении своей деятельности.

1.2. В целях настоящего документа 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 - 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;

– автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

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

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

– блокирование персональных данных - временное прекращение обработки персональных данных (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 и (или) в результате которых уничтожаются материальные носители персональных данных;

– обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

– информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

– информационные активы - информационные ресурсы или средства обработки информации организации.

1.3. В понятие информационной безопасности образовательного учреждения входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы; защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы.

1.4. Основной целью Политики информационной безопасности образовательного учреждения является защита информации образовательного учреждения, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных.

1.5. Политика информационной безопасности разработана в соответствии с:

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»;

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

– Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;

– Постановлением Правительства РФ от 01.11.2012. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства от 15.09.2008 РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– приказом ФСТЭК от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– иными нормативными правовыми актами в сфере защиты информации.

1.6. Выполнение требований Политики информационной безопасности является обязательным для всех сотрудников образовательного учреждения.

1.7. Ответственность за соблюдение информационной безопасности несет каждый сотрудник образовательного учреждения.

2. Цель и задачи политики информационной безопасности

2.1. Основными целями Политики информационной безопасности являются:

– сохранение конфиденциальности критичных информационных ресурсов;

– обеспечение непрерывности доступа к информационным ресурсам образовательного учреждения;

– защита целостности информации с целью поддержания возможности образовательного учреждения по оказанию услуг высокого качества и принятию эффективных управленческих решений;

– повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами образовательного учреждения;

– определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности;

– повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз информационной безопасности;

– предотвращение и/или снижение ущерба от инцидентов информационной безопасности.

2.2. Основными задачами политики информационной безопасности являются:

– разработка требований по обеспечению информационной безопасности;

– контроль выполнения установленных требований по обеспечению информационной безопасности;

– повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;

– разработка нормативных документов для обеспечения информационной безопасности образовательного учреждения;

– выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности образовательного учреждения;

– организация антивирусной защиты информационных ресурсов образовательного учреждения;

– защита информации образовательного учреждения от несанкционированного доступа и утечки по техническим каналам связи;

– организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору образовательного учреждения.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика информационной безопасности образовательного учреждения направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников образовательного учреждения, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

Наибольшими возможностями для нанесения ущерба обладает персонал образовательного учреждения.

Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

Стратегия обеспечения информационной безопасности образовательного учреждения заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений,

позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников образовательного учреждения.

4. Основные принципы обеспечения информационной безопасности

4.1. Основными принципами обеспечения информационной безопасности:

– постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов образовательного учреждения;

– своевременное обнаружение проблем, потенциально способных повлиять на информационной безопасности образовательного учреждения, корректировка моделей угроз и нарушителя; -

– разработка и внедрение защитных мер;

– контроль эффективности принимаемых защитных мер;

– персонификация и разделение ролей и ответственности между сотрудниками образовательного учреждения за обеспечение информационной безопасности образовательного учреждения исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5.Объекты защиты

5.1. Объектами защиты с точки зрения информационной безопасности являются:

– информационный процесс профессиональной деятельности;

– информационные активы образовательного учреждения.

5.2. Защищаемая информация делится на следующие виды:

– информация по финансово-экономической деятельности образовательного учреждения;

– персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

– другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. Меры по обеспечению безопасности

6.1. В отношении всех собственных информационных активов образовательного учреждения, активов, находящихся под контролем образовательного учреждения, а также активов, используемых для получения доступа к инфраструктуре образовательного учреждения, определена ответственность соответствующего сотрудника образовательного учреждения.

6.2. Все работы в пределах образовательного учреждения выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в управлении.

6.3. Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну образовательного учреждения и хранящиеся на жестких дисках портативных компьютеров зашифрованы.

6.4. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему осуществляется с использованием уникального имени пользователя и пароля.

6.5. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим.

6.6. В процессе своей работы сотрудники используют режим «Экранной заставки» с парольной защитой.

6.7. Работа в информационно-телекоммуникационной сети Интернет на элементах ИСПДн, проводиться только при служебной необходимости.

6.8. Администратор ЛВС контролирует содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.10. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация образовательного учреждения.

6.11. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор ЛВС.

6.12. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются «компьютерное оборудование».

6.12.1. Компьютерное оборудование, предоставленное образовательным учреждением, является ее собственностью и предназначено для использования исключительно в производственных целях.

6.12.2. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

6.13. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), проверяются, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Выполняется процедура форматирования носителей информации, исключающая возможность восстановления данных.

6.14. Все программное обеспечение, установленное на предоставленном образовательным учреждением компьютерном оборудовании, является собственностью образовательного учреждения и должно использоваться исключительно в производственных целях.

6.15. Сотрудникам запрещается самовольно вносить какие-либо изменения в конфигурацию компьютерного оборудования или устанавливать любые программные и аппаратные средства. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено директору образовательного учреждения.

6.16. Все компьютеры оснащены системой антивирусной защиты, утвержденной администратором ИСПДн.

6.17. Использование электронной почты в личных целях не допускается.

6.18. Сотрудникам запрещается направлять конфиденциальную информацию образовательного учреждения по электронной почте без использования систем шифрования. Строго конфиденциальная информация образовательного учреждения, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6.19. Все пользователи должны быть осведомлены о своей обязанности сообщать, об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

6.20. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

- проинформировать администратора ИСПДн;
- не пользоваться и не выключать зараженный компьютер.

6.21. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

6.22. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

6.23. Только администратор ЛВС на основании запроса директора образовательной организации может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

6.24. Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

6.25. Все заявки администратору ЛВС на проведение технического обслуживания компьютеров должны оформляться в журнале заявок.

7. Управление информационной безопасностью

7.1. Управление ИБ образовательного учреждения включает в себя:

- разработку и поддержание в актуальном состоянии Политики информационной безопасности;
- разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению информационной безопасности;
- обеспечение бесперебойного функционирования комплекса средств информационной безопасности;
- осуществление контроля (мониторинга) функционирования системы информационной безопасности;
- оценку рисков, связанных с нарушениями информационной безопасности

8. Реализация политики информационной безопасности

8.1. Реализация Политики информационной безопасности образовательного учреждения осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в образовательном учреждении.