МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 5 ГОРОДА ЗЕИ АМУРСКОЙ ОБЛАСТИ

ПРИНЯТО
Управляющим советом
МОАУ СОШ № 5
протокол от 10.11.2020 № 2

УТВЕРЖДЕНО
приказом директора
МОАУ СОШ № 5
от 11.11.2020 № 240/од

Положение
об информационной безопасности МОАУ СОШ № 5

1. Общие положения

1.1. Положение об информационной безопасности (далее - Положение) МОБУ СОШ № 5 (далее - Учреждение) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и принципов в области информационной безопасности, которыми руководствуются работники Учреждения.

1.2. Основной целью информационной безопасности Учреждения является защита информации Учреждения при осуществлении уставной деятельности, 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 в Учреждении.

1.3. Положение разработано 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 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»;
- Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановлением Правительства РФ от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.4. Выполнение требований Положения является обязательным для всех работников Учреждения.

2. Цельи задачи и информационной безопасности

2.1. Основными целями информационной безопасности являются:

- сохранение конфиденциальности информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам Учреждения;
- защита целостности информации с целью поддержания возможности Учреждения по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Учреждения;
- определение степени ответственности и обязанностей работников Учреждения по обеспечению информационной безопасности в Учреждении;
- 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 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 Учреждения;
- выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности;
- организация антивирусной защиты информационных ресурсов Учреждения;
- защита информации Учреждения от несанкционированного доступа;
- организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору Учреждения.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Информационная безопасность 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 работников 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.

3.2. Наибольшими возможностями для нанесения ущерба обладает собственный персонал Учреждения. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного

обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией работников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

3.3. Обеспечение информационной безопасности Учреждения заключается в использовании мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий работников Учреждения.

4. Основные принципы обеспечения информационной безопасности

4.1. Основными принципами обеспечения информационной безопасности являются:

- постоянный и всесторонний анализ автоматизированных систем с целью выявления уязвимости информационных активов Учреждения;
- своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность Учреждения, корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер;
- контроль эффективности принимаемых защитных мер.

5. Объекты информационной защиты

5.1. Объектами информационной защиты с точки зрения информационной безопасности в Учреждении являются:

- информационный процесс профессиональной деятельности;
- информационные активы Учреждения.

5.2. Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности 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.

6. Требования по информационной безопасности

6.1. Все работы в пределах Учреждения должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Учреждении.

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

6.3. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования.

Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

6.4. В процессе своей деятельности работники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.

6.5. Каждый работник обязан уведомить администратора ЛВС обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети. Доступ третьих лиц к информационным системам Учреждения должен быть обусловлен производственной необходимостью. В связи с этим порядок доступа к информационным ресурсам Учреждения четко определен, контролируем и защищен.

6.6. Работникам Учреждения, использующим в работе портативные компьютеры, может быть предоставлен удаленный доступ к сетевым ресурсам Учреждения в соответствии с правами в корпоративной информационной системе.

6.7. Работникам, находящимся за пределами Учреждения с использованием компьютера, не принадлежащего Учреждению, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

6.8. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Учреждения, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

6.9. Правила использования сети Интернет:

- работникам Учреждения разрешается использовать сеть Интернет только в служебных целях;

- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

- работники Учреждения не должны использовать сеть Интернет для хранения корпоративных данных;

- работа с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Учреждения в сеть Интернет;

- работникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Учреждению;

- работники Учреждения перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

- запрещен доступ в Интернет через сеть Учреждения для всех лиц, не являющихся работниками Учреждения, включая членов семьи работников Учреждения.

6.10. Администратор ЛВС имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.11. Работники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация Учреждения.

6.12. Работникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор ЛВС.

6.13. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы), коммуникационное оборудование (факс-модемы, сетевые адаптеры и концентраторы), предоставленное Учреждением, является его собственностью и предназначено для использования исключительно в служебных целях.

6.14. Каждый работник, получивший в пользование компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

6.15. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавише и после выхода из режима «Экранной заставки». Для установки режимов защиты пользователь должен обратиться к администратору ЛВС. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

6.16. Работникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их служебной деятельности.

6.17. На всех компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;
- антивирусное программное обеспечение.

6.18. Все компьютеры, подключенные к ЛВС, должны быть оснащены системой антивирусной защиты, утвержденной администратором ЛВС.

6.19. Работники Учреждения не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

6.20. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается.

6.21. Работники Учреждения для обмена документами должны использовать только свой официальный адрес электронной почты.

6.22. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма, и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций. В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать администратора ЛВС. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

6.23. Не допускается при использовании электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- рассылка рекламных материалов;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

6.24. Объем пересылаемого сообщения по электронной почте не должен превышать 5 Мбайт.

6.25. 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.

6.26. В случае кражи компьютера следует незамедлительно сообщить администрации Учреждения.

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

- проинформировать администратора ЛВС;
- не пользоваться и не выключать зараженный компьютер;

6.28. Работникам Учреждения запрещается:

- нарушать информационную безопасность и работу сети Учреждения;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- передавать информацию о работниках или списки работников Учреждения посторонним лицам;

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

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

Только администратор ЛВС может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

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

6.30. Все заявки на проведение технического обслуживания компьютеров должны направляться администратору ЛВС.

7. Управление информационной безопасностью

7.1. Управление информационной безопасностью Учреждения включает в себя:

- 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. Порядок внесения изменений и дополнений в Положение

8.1. Внесение изменений и дополнений в Положение производится не реже одного раза в три года с целью приведения в соответствие определенных Положением защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

9. Контроль соблюдения информационной безопасности

9.1. Текущий контроль соблюдения выполнения требований Положения возлагается на заместителя директора Учреждения, курирующего вопросы ИКТ.

9.2. Директор Учреждения осуществляет контроль соблюдения требований Положения.