МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ШКОЛА № 20»

ПРИНЯТО
на педагогическом совете
МБОУ «Средняя школа №20»
Протокол №1 от 31.08.2015г.

УТВЕРЖДЕНО
ДИРЕКТОР ШКОЛЫ
(Т.И. Захарова)
подпись расшифровка подписи
«31» августа 2015 г.
приказ от 31.08.2015г. №73§ 6

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Общие положения

1.1. Настоящее положение является локальным нормативным актом, устанавливающим основные принципы, порядок и правила обеспечения информационной безопасности в информационно-телекоммуникационных системах МБОУ «Средняя школа № 20», и является основным документом, регламентирующим деятельность Учреждения в области обеспечения безопасности информационных технологий и информационных ресурсов Учреждения.

1.2. Положение разработано на основании требований действующего законодательства Российской Федерации, в целях установления общих норм и правил защиты информационных ресурсов от внешних и внутренних угроз безопасности, информирования пользователей об обязательных требованиях по защите информационных технологий и информационных ресурсов.

1.3. Требования Положения распространяются на работников Учреждения.

2. Объекты обеспечения информационной безопасности

2.1. Основными объектами обеспечения информационной безопасности Учреждения являются:

2.1.1. Информационные ресурсы, содержащие персональные данные работников школы, учащихся и их родителей;

2.1.2. Средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), с использованием которых осуществляются обработка, передача и хранение информации;

2.1.3. программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), с использованием которых осуществляется обработка информации;

2.2. Защите подлежат следующие категории информационные ресурсы Учреждения (защищаемая информация или защищаемые информационные ресурсы):

2.2.1. **Конфиденциальные сведения** — информация, определенная Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

2.2.2. **Персональные данные** — информация, попадающая под действие Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

2.2.3. **Публичная информация** — информация о деятельности Учреждения, предназначенная для представления в публичный доступ и размещения на внешних публичных ресурсах Учреждения (сайт, блог).

2.2.4. **Открытая информация** — информация, сформированная в результате операционной деятельности Учреждения.

3. Угроза информационной безопасности

3.1. Под угрозами информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию. К основным угрозам информационной безопасности Учреждения относятся:

3.1.1. **утечка защищаемой информации** — несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, разглашение, копирование, хищение и т.д.), утечка информации по каналам связи и за счет побочных электромагнитных излучений;

3.1.2. **недоступность защищаемой информации** — блокирование информационных ресурсов, сбои в работе технических средств или программного обеспечения, дезорганизация функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления базами данных, распределенных информационных сетей, воздействие вредоносного программного обеспечения, стихийных бедствий и иных форс-мажорных обстоятельств;

3.1.3. **потеря защищаемой информации** — уничтожение, искажение (несанкционированная модификация, подделка) информационных ресурсов.

3.2. В результате воздействия угроз информационной безопасности существует вероятность возникновения следующих негативных последствий:

3.2.1. физических (причинение вреда здоровью и жизни работников, учащихся и их родителей; причинение вреда имущественному комплексу);

3.2.2. репутационных (ущерб репутации Учреждения, работников, руководителей, учащихся и их родителей).

4. Защита информационной безопасности

4.1. В целях обеспечения информационной безопасности в Учреждении принимаются административно-правовые, организационные, технические и режимные меры.

4.2. Административно-правовые и организационные меры:

- определение правового статуса субъектов отношений в сфере информационных технологий, установление их ответственности за соблюдение требований нормативных правовых актов Учреждения в этой сфере;
- разработка локальных нормативных актов, определяющих порядок защиты информационных ресурсов, периодическое уточнение и оценка эффективности принимаемых мер;
- проведение вводных инструктажей при приеме на работу;
- разработка правил (регламентов, инструкций) эксплуатации технических и программных средств с учетом требований информационной безопасности;
- разработка регламентов работы с документами, содержащими конфиденциальные сведения;
- разработка и совершенствование нормативно-правовой базы, регламентирующей порядок обмена информационными ресурсами между Учреждением и сторонними организациями;
- обеспечение принципа разграничения доступа к защищаемым информационным ресурсам с учетом минимально достаточных прав по доступу к информации, необходимой для выполнения работниками своих должностных обязанностей;
- использование информационных ресурсов, в том числе сети «Интернет» и электронной почты, только в служебных целях.

4.3. Технические меры:

- использование лицензионного программного обеспечения;
- обеспечение безотказной работы аппаратных средств;
- проведение комплексной защиты от вредоносного программного обеспечения;
- своевременная установка обновлений для средств защиты информации, операционных систем и прикладного программного обеспечения;

4.4. Режимные меры:

- ограничение круга лиц, имеющих право работы со сведениями конфиденциального характера;

- установление специальных режимных мер, применяемых в целях информационной безопасности Учреждения (ведение специального делопроизводства, выделение и контроль состояния безопасности специально оборудованных помещений, поддержание необходимого уровня пропускного и внутриобъектового режимов, подбор кадров, проведение комплексных защитнопоисковых мероприятий и т.п.);
- разграничение и контроль доступа в защищаемые помещения;
- создание эффективной системы контроля выполнения работниками Учреждения требований локальных нормативных актов по обеспечению информационной безопасности.

5. Ответственность

5.1. Лица, допущенные к автоматизированной обработке защищаемой информации, несут ответственность за соблюдение ими установленного законодательством Российской Федерации, а также локальными нормативными актами Учреждения порядка обеспечения ее защиты.

5.2. Электронные документы представляются в формате, позволяющем указывать дополнительные идентифицирующие атрибуты, в том числе автора, дату создания и последнего изменения, права доступа и т. д.

При хранении электронных документов в системе электронного документооборота или файловых архивах локальной сети доступ к ним разграничивается и предоставляется только пользователям, имеющим соответствующие права.

При хранении электронных документов локально на компьютере пользователя или на сменных носителях принимаются соответствующие меры по защите документов от несанкционированного доступа, утери или повреждения.

5.3. Предоставление сторонним организациям информации должно быть согласовано с руководителем Учреждения. Согласование производится с учетом рассмотрения всех действующих требований по безопасности.

5.4. Доступ работника к сети «Интернет» в рабочее время разрешается только для выполнения служебных обязанностей и не может использоваться в других, в том числе, в личных, целях. Запрещается посещение сайтов, не связанных с выполнением должностных обязанностей.

Информация, полученная из сети «Интернет», должна использоваться с учетом прав на интеллектуальную собственность, а также прав на использование программных продуктов, являющихся предметом собственности третьих лиц.

5.5. Во всех информационных системах Учреждения разрешается использовать только лицензионное программное обеспечение в соответствии с требованиями действующего законодательства и соответствующих лицензионных соглашений.

Установка, настройка и администрирование программного обеспечения осуществляются инженером ИКТ или заместителем директора по УВР, отвечающего за информатизацию образовательного процесса.

Пользователям запрещается самостоятельная установка и распространение любого готового прикладного программного обеспечения, в том числе общего применения (текстовых и графических редакторов, табличных процессоров, специальных программ преобразований графической информации, голосовых сообщений и т.д.) без согласования с заместителем директора по УВР, отвечающего за информатизацию образовательного процесса.

5.6. Запрещается обсуждать защищаемую информацию с использованием средств связи в общественных местах, а также передавать такую информацию по открытым каналам связи, не приняв достаточных мер по ее технической защите.

5.7. При утилизации (списании) оборудования все его компоненты, содержащие носители данных, должны быть проверены с целью безопасного сохранения или удаления данных и лицензионного ПО.

5.8. Все работники Учреждения и третьи лица, использующие информационные ресурсы Учреждения, должны незамедлительно сообщать руководителю о любых обнаруженных недостатках в обеспечении информационной безопасности.

5.9. При увольнении работник обязан сдать все технические средства и съемные носители информации, принадлежащие Учреждению и находящиеся в его пользовании.

5.10. Ответственность за соблюдения правил возлагается на всех работников Учреждения, использующих средства обработки информации.
5.11. Ответственность за организацию работы с третьими лицами возлагается на руководителя Учреждения.
5.12 . Ответственность за организацию процессов управления данными возлагается на заместителя директора по УВР, отвечающего за информатизацию образовательного процесса.
5.13. Контроль выполнения и пересмотр правил возлагаются на руководителя и заместителя директора по УВР, отвечающего за информатизацию образовательного процесса.

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "
СРЕДНЯЯ ШКОЛА № 20"
ПЕТРОПАВЛОВСК-КАМЧАТСКОГО
ГОРОДСКОГО ОКРУГА
Сахарова Татьяна Ивановна, Директор, 7a 93 ed
d6 85 b6 90 75 1b 3f 97 9d ec f7 01 8b 64 fc 30 ed
2021.03.30 15:49:53+12'00'