Муниципальное образование г. Тулы
(УО администрации г. Тулы)
муниципальное бюджетное общеобразовательное учреждение –
« Центр образования № 10 » имени А.В. Чернова

«Согласовано»
На педагогическом совете

Протокол № 4 от 26.12. 2016г.

«Утверждаю»
Директор МБОУ «ЦО № 10»

_____ О.Н. Чернышева
«27» 12 2016г.

Политика информационной безопасности Муниципального бюджетного общеобразовательного учреждения «Центр образования № 10» имени А.В. Чернова

2016г.

1. Общие положения

1.1. Политика информационной безопасности Муниципального бюджетного общеобразовательного учреждения «Центр образования № 10» имени А.В. Чернова определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности (далее - ИБ), которыми руководствуются работники МБОУ «ЦО № 10» при осуществлении своей деятельности.

1.2. Основной целью Политики информационной безопасности МБОУ «ЦО № 10» является защита информации 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 информации, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных.

1.3. Политика информационной безопасности разработана в соответствии с Федеральным законом РФ от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом РФ от 27 июля 2006г. № 152-ФЗ «О персональных данных», Федеральным законом РФ от 10 января 2002г. № 1-ФЗ «Об электронной цифровой записи», Указом Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

1.4. Выполнение требований Политики информационной безопасности является обязательным для всех структурных подразделений МБОУ «ЦО № 10».

1.5. 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 в образовательном учреждении;

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

-предотвращение и/или снижение ущерба от инцидентов в информационной безопасности.

2.2.Основными задачами политики ИБ являются:

-разработка требований по обеспечению ИБ;

-контроль выполнения установленных требований по обеспечению ИБ;

-повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;

-разработка нормативных документов для обеспечения ИБ образовательного учреждения;

-выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ образовательного учреждения;

-организация антивирусной защиты информационных ресурсов образовательного учреждения;

-защита информации образовательного учреждения от несанкционированного доступа (далее- НСД) и утечки по техническим каналам связи.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика ИБ 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 Центра образования, 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 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.

3.3. Стратегия обеспечения ИБ 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 Центра образования.

4. Основные принципы обеспечения информационной безопасности

4.1.Основными принципами обеспечения ИБ являются:

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

-своевременное обнаружение проблем, потенциально способных повлиять на ИБ 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 Центра образования за обеспечение ИБ образовательного учреждения исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5.Объекты защиты

5.1.Объектами защиты с точки зрения ИБ в образовательном учреждении 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.

6. Требования по информационной 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, должна быть определена ответственность соответствующего сотрудника Центра образования.
Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами образовательного учреждения, должна доводиться до сведения директора Центра образования.

6.2. Все работы в пределах образовательного учреждения, должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в образовательном учреждении.

6.3. Внос в здание и помещения образовательного учреждения личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы образовательного учреждения, производится только при согласовании с директором Центра образования.

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

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

6.6. Сотрудникам, использующим в работе портативные компьютеры образовательного учреждения, может быть предоставлен удаленный доступ к сетевым ресурсам Центра образования в соответствии с правами в информационной системе.

6.7. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети образовательного учреждения, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

6.8. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила:

- сотрудникам Центра образования 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;

- сотрудники Центра образования перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов.

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

6.10. 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". Компьютерное оборудование, является собственностью образовательного учреждения и предназначено для использования исключительно в производственных целях.

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

7. Управление информационной безопасностью

7.1. Управление ИБ образовательного учреждения включает в себя:

-разработку и поддержание в актуальном состоянии Политики ИБ;

-разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению ИБ;

-обеспечение бесперебойного функционирования комплекса средств ИБ;

-осуществление контроля (мониторинга) функционирования системы ИБ.

8. Контроль соблюдения политики информационной безопасности

8.1. Директор Центра образования на регулярной основе рассматривает реализацию и соблюдение Политики информационной безопасности, а также осуществляет контроль соблюдения ее требований.