Муниципальное бюджетное общеобразовательное учреждение города Юрьев-Польского
«Школа № 1»
(МБОУ «Школа № 1»)

«СОГЛАСОВАНО»
Председатель профкома
_____ / Галибина Н. Ю.
(подпись) *(Ф. И. О.)*

«УТВЕРЖДАЮ»
Директор МБОУ «Школа №1»
_____ / Цыбина И. В.
(подпись) *(Ф. И. О.)*
М. П.

Политика информационной безопасности

Г. Юрьев-Польский 2023 г.

1. Общие положения

Политика информационной безопасности Муниципального бюджетного общеобразовательного учреждения города Юрьев-Польского «Школа №1» (далее – школа) 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 школы при осуществлении своей деятельности.

Основной целью Политики информационной безопасности школы является защита информации школы 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 управлении.

Политика информационной безопасности разработана в соответствии с: Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным закон от 27 июля 2006г. № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Постановление Правительства РФ №687 от 15.09.08г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» а также рядом иных нормативных правовых актов в сфере защиты информации.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник школы. На лиц, работающих по договорам гражданско-правового характера, положения настоящей политики распространяются в случае, если это обусловлено в таком договоре.

2. Цель и задачи политики информационной безопасности

Основными целями ИБ являются:

1) сохранение конфиденциальности критичных информационных ресурсов;
2) обеспечение непрерывности доступа к информационным ресурсам школы
3) повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами школы;
4) определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности;
5) повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;
6) предотвращение и/или снижение ущерба от инцидентов ИБ.

Основными задачами политики ИБ являются:

1) разработка требований по обеспечению ИБ;
2) контроль выполнения установленных требовании по обеспечению ИБ;
3) повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;
4) Разработка нормативных документов для обеспечения ИБ школы
5) Выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ школы;
6) Организация антивирусной защиты информационных ресурсов школы; защита информации школы от несанкционированного доступа (далее-НСД) и утечки по техническим каналам связи.

3. Концептуальная схема обеспечения информационной безопасности

Политика ИБ школы 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 школы, 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 собственный персонал школы. 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 ИБ школы 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 школы.

4. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения информационной безопасности являются:

1) Постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов школы;
2) Своевременное обнаружение проблем, потенциально способных повлиять на ИБ школы, корректировка моделей угроз и нарушителя;
3) Разработка и внедрение защитных мер;
4) Контроль эффективности принимаемых защитных мер;
5) Персонификация и разделение ролей и ответственности между сотрудниками школы за обеспечение ИБ школы исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5. Объекты защиты

Объектами защиты с точки зрения ИБ в управлении являются:

1) Информационный процесс профессиональной деятельности;
2) Информационные активы школы.

Защищаемая информация делится на следующие виды:

1) Информация по финансово-экономической деятельности школы;
2) 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;
3) Другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. Требования по информационной безопасности

В отношении всех собственных информационных активов школы, активов, находящихся под контролем школы, а также активов, используемых для получения доступа к инфраструктуре школы, должна быть определена ответственность соответствующего сотрудника школы. Информация о смене владельцев активов, их

распределении, изменениях в конфигурации и использовании за пределами школы должна доводиться до сведения директора школы.

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

Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

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

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.

В процессе своей работы сотрудники обязаны постоянно использовать режим "Экранной заставки" с парольной защитой. Рекомендуется устанавливать максимальное время "простоя" компьютера до появления экранной заставки не дольше 15 минут.

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

Рекомендованные правила:

1) сотрудникам школы разрешается использовать сеть Интернет только в служебных целях;
2) запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, религиозных или политических убеждений, национального происхождения или недееспособности;
3) работа сотрудников школы с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации школы в сеть Интернет;
4) сотрудники школы перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
5) запрещен доступ в Интернет через сеть школы для всех лиц, не являющихся сотрудниками школы, включая членов семьи сотрудников.

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

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

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор безопасности информации.

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

оборудование, предоставленное школой, является ее собственностью и предназначено для использования исключительно в производственных целях.

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

Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". Для установки режимов защиты пользователь должен обратиться к администратору безопасности информации. 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.

При записи какой-либо информации на носитель для передачи субъектам, участвующим в информационном обмене, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации. Порты передачи данных, в том числе CD дисководы в стационарных компьютерах сотрудников школы блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись от администратора.

Все программное обеспечение, установленное на предоставленном школой компьютерном оборудовании, является собственностью школы и должно использоваться исключительно в производственных целях.

Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственно директору школы.

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

1) Антивирусное программное обеспечение Сотрудники школы не должны:
1) блокировать антивирусное программное обеспечение;
2) устанавливать другое антивирусное программное обеспечение;
3) изменять настройки и конфигурацию антивирусного программного обеспечения.

Использование сотрудниками школы публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации при условии применения механизмов шифрования.

Сотрудники школы для обмена документами должны использовать только свой официальный адрес электронной почты.

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.

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.

В случае кражи переносного компьютера следует незамедлительно сообщить администратору безопасности информации и/или директору школы.

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

1) проинформировать администратора безопасности информации;
2) не использовать и не включать зараженный компьютер;
3) не подсоединять этот компьютер к компьютерной сети школы до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором.

Сотрудникам школы запрещается:

1) нарушать информационную безопасность и работу сети школы;
2) сканировать порты или систему безопасности;
3) получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
4) передавать информацию о сотрудниках или списки сотрудников школы посторонним лицам;
5) создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

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.

Все заявки на проведение технического обслуживания Компьютеров должны направляться администратору безопасности информации.

7. Управление информационной безопасностью

Управление ИБ школы включает в себя:

1) разработку и поддержание в актуальном состоянии Политики информационной безопасности;
2) разработку и поддержание в актуальном состоянии нормативно- методических документов по обеспечению ИБ;
3) обеспечение бесперебойного функционирования комплекса средств ИБ;
4) оценку рисков, связанных с нарушениями ИБ.

8. Реализация политики информационной безопасности

Реализация Политики ИБ школы осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в управлении.

9. Порядок внесения изменений и дополнений в политику информационной безопасности

Внесение изменений и дополнений в Политику информационной безопасности производится не реже одного раза в три года с целью приведения в соответствие

определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

10. Контроль за соблюдением политики информационной безопасности

Текущий контроль за соблюдением выполнения требований Политики информационной безопасности школы возлагается на сотрудника, назначенного приказом директора школы.

Директор школы на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.