Приложение 2 к приказу
Муниципального общеобразовательного учреждения
«Тоншаевская средняя школа»
от 25.09.2018 № 01-02/285

Политика информационной безопасности
Муниципального общеобразовательного учреждения
«Тоншаевская средняя школа»

1. Общие положения

1.1. Политика информационной безопасности Муниципального общеобразовательного учреждения «Тоншаевская средняя школа» (далее – Учреждение) определяет цели и задачи системы обеспечения информационной безопасности (далее - ИБ) и устанавливает совокупность правил, процедур, практических приемов,требований и руководящих принципов в области ИБ, которыми руководствуются участники образовательных отношений Учреждения.

1.2. Основная цель Политики ИБ Учреждения – защита информации Учреждения, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения, целостности и доступности и информации, обеспечения процесса автоматизированной обработки данных в управлении.

1.3. Политики ИБ Учреждения обязательна для соблюдени всеми сотрудниками Учреждения.

2. Цель и задачи Политики ИБ Учреждения

2.1. Основными целями Политики ИБ являются:

- сохранение конфиденциальности критичных 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 сотрудников по обеспечению информационной безопасности в управлении;

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

- предотвращение и/или снижение ущерба от инцидентов ИБ.

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 Учреждения;

- выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ Учреждения;

- организация антивирусной защиты информационных ресурсов Учреждения;

- защита информации Учреждения от несанкционированного доступа (далее-НСД) и утечки по техническим каналам связи;

- организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору Учреждения.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика ИБ 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 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 персонал 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 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 учреждения.

4. Основные принципы обеспечения информационной безопасности

4.1.Основными принципами обеспечения ИБ:

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

- своевременное обнаружение проблем, потенциально способных повлиять на ИБ, корректировка моделей угроз и нарушителя;

- разработка и внедрение защитных мер;

- контроль эффективности принимаемых защитных мер;

- персонификация и разделение ролей и ответственности между сотрудниками Учреждения за обеспечение ИБ исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5.Объекты защиты

5.1.Объектами защиты с точки зрения ИБ в управлении являются:

- информационный процесс профессиональной деятельности;

- информационные активы Учреждения.

5.2.Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности;

- 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. Требования по информационной безопасности

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

Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами Учреждения должна доводиться до сведения директора Учреждения.

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

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

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

6.5. 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 лицам, в том числе членам своей семьи и близким.

6.6. 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.

6.7. Каждый сотрудник обязан немедленно уведомить директора 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 должен быть четко определен, контролируем и защищен.

6.8. Сотрудникам, использующим в работе портативные компьютеры

Учреждения, может быть предоставлен удаленный доступ к сетевым ресурсам Учреждения в соответствии с правами в корпоративной информационной системе.

6.9. Сотрудникам, работающим за пределами Учреждения с использованием компьютера, не принадлежащего управлению, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

6.10. Сотрудники, имеющие право удаленного доступа к информационным ресурсам Учреждения, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Учреждения и к каким-либо другим сетям, не принадлежащим Учреждению.

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

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

Рекомендованные правила:

- сотрудникам 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 не должны использовать сеть Интернет для хранения корпоративных данных;

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

- сотрудники 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 сотрудниками Учреждения, включая членов семьи сотрудников Учреждения.

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

6.14. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения.

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, предоставленное управлением, является его собственностью и предназначено для использования исключительно в производственных целях. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

6.15. 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 системному администратору. 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. 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.

6.17. Порты передачи данных, в том числе FDD и CD дисководы в стационарных компьютерах сотрудников блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись системного администратора.

6.18. Все программное обеспечение, установленное на предоставленном управлением компьютерном оборудовании, является собственностью Учреждения и должно использоваться исключительно в производственных целях.

6.19. 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 непосредственному директору Учреждения.

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

- персональный межсетевой экран;
- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков;
- программное обеспечение шифрования почтовых сообщений.

6.21. Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты.

6.22. Сотрудники не должны:

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

6.23. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию

Учреждения по электронной почте без использования систем шифрования. Строго конфиденциальная информация Учреждения, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

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

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

6.26. 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. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

6.27. Не допускается при использования 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.

6.28. Объем пересылаемого сообщения по электронной почте не должен превышать 2 Мбайт.

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

6.30. В случае кражи переносного компьютера следует незамедлительно сообщить системному администратору.

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

- проинформировать администратора;
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети Учреждения до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование.

6.32. Конфиденциальные встречи (заседания) должны проходить только в защищенных техническими средствами информационной безопасности помещениях.

6.33. Участникам заседаний запрещается входить в помещения с записывающей аудио/видео аппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами без предварительного согласования с администрацией Учреждения.

6.34. Аудио/видео запись, фотографирование во время конфиденциальных заседаний может вести только сотрудник Учреждения, который отвечает за подготовку заседания, после получения письменного разрешения руководителя группы организации встречи.

6.35. Доступ участников конфиденциального заседания в помещение для его проведения осуществляется на основании утвержденного перечня, контроль за которым ведет лицо, отвечающее за организацию встречи.

6.36. Сотрудникам запрещается:

- нарушать информационную безопасность и работу сети Учреждения;

- сканировать порты или систему безопасности;

- контролировать работу сети с перехватом данных;

- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;

- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;

- передавать информацию о сотрудниках или списки сотрудников Учреждения посторонним лицам;

- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

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

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

6.39. Только сетевой администратор на основании заявок сотрудников может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

6.40. 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.

6.41. Все заявки на проведение технического обслуживания компьютеров должны направляться системному администратору.

6.42. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы и

согласованны с системным администратором.

7. Управление информационной безопасностью

Управление ИБ школы 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;

- оценку рисков, связанных с нарушениями ИБ.

8. Реализация политики информационной безопасности

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

9. Порядок внесения изменений и дополнений в Политику ИБ

Внесение изменений и дополнений в Политику ИБ 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 ИБ

10.1. Текущий контроль за соблюдением выполнения требований Политики ИБ возлагается на сотрудника, назначенного приказом директора Учреждения.

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

Принято с учетом мнения педагогического совета (Протокол от 25.09.2018 № 12)