Муниципальное автономное общеобразовательное учреждение
«Гимназия № 39»
Петропавловск-Камчатского городского округа

ПРИКАЗ № 13
от 08 .09. 2020 г.

Каурцева Светлана Петровна
Подписано цифровой подписью: Каурцева Светлана Петровна
Дата: 2021.12.23 12:18:38 +12'00'

«Об организации информационной безопасности в гимназии»

Во исполнение требований Федерального закона от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», в соответствии с Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях по защите информации». В целях исключения доступа обучающихся к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания, усиления профилактической работы по вопросу защиты детей от информации, причиняющей вред их здоровью и развитию,

ПРИКАЗЫВАЮ:

1. Назначить ответственным за обеспечение информационной безопасности заместителя директора по УВР Гудзь С.В.

2. Назначить ответственным за организацию доступа к образовательным ресурсам сети Интернет и мониторинг системы контентной фильтрации доступа к сети Интернет в гимназии инженера-программиста Чаплыгина С.А..

3. Назначить ответственными за контроль использования интернет-ресурсов обучающимися во время доступа к сети Интернет гимназии во время уроков и вне учебных занятий:

- в кабинете информатики - учителя информатики;
- в учебных кабинетах - учителей-предметников;
- в библиотеке – заведующего библиотекой.

4. Утвердить:

4.1. Политику информационной безопасности МАОУ «Гимназия № 39» (Приложение №1).

4.2. Утвердить План мероприятий по обеспечению информационной безопасности обучающихся и при использовании ресурсов сети Интернет на 2020-2021 уч. г. (Приложение № 2).

5. Утвердить формы документов:

5.1. Журнал регистрации случаев обнаружения сайтов с информацией, причиняющей вред здоровью и (или) развитию обучающихся, а также не соответствующей задачам образования. (Приложение № 3)

6. Сотрудникам гимназии неукоснительно выполнять требования локальных нормативных актов по информационной безопасности.

7. Ответственному за информационную безопасность Гудзь С.В.:

7.1. взять на контроль порядок размещения персональных данных на официальном сайте гимназии и передачи их посредством сети Интернет;

7.2. выявлять случаи нарушения безопасности использования сети Интернет с анализом причин и предпринимать меры по недопущению нарушений;

7.3. при обнаружении факта использования нелицензионного программного обеспечения (ПО):

- принимать меры по прекращению использования данного ПО;
- предпринимать необходимые действия по приобретению необходимых лицензий или использованию аналогичных программных продуктов, распространяемых бесплатно;

8. Ответственному за ведение официального сайта гимназии инженеру-программисту Чаплыгину С.А.:

8.1. пополнять официальный сайт информацией по защите обучающихся от информации, приносящей вред здоровью и развитию.

8.2. пополнять официальный сайт информацией для и родителей (законных представителей) по проблеме безопасности детей в Интернете;

9. Заместителю директора по воспитательной работе Емелиной В.В. совместно с ответственным за информационную безопасность:

9.1. определить комплекс мер воспитательной работы по формированию пользовательской культуры работы обучающихся в сети Интернет;

9.2. организовать проведение классных часов, бесед и иных форм просвещения (программ обучения) по тематике, раскрывающей правила безопасного поведения детей в сети Интернет;

9.3. продолжить проведение родительских собраний по правилам безопасного поведения в интернет-пространстве, профилактике интернет-зависимости (по возможности с участием специалистов в области компьютерной коммуникации);

10. Контроль за исполнением приказа оставляю за собой.

Директор
МАОУ «Гимназия № 39» Каурцева С.П.

Приложение № 1 к приказу «Об организации информационной безопасности в учреждении» от 08.09.2020 №13

Политика информационной безопасности муниципального автономного общеобразовательного учреждения «Гимназия № 39» Петропавловск-Камчатского городского округа

Общие положения

1.1. Политика информационной безопасности МАОУ «Гимназия №39» (далее - Гимназия) 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 гимназии при осуществлении своей деятельности.

1.2.Основной целью Политики информационной безопасности гимназии 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, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в управлении.

1.3. Политика информационной безопасности разработана в соответствии с: Федеральным законом от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных», Федеральным законом от 10 января 2002 № 1-ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 06 марта 1997 № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства РФ №781 от 17.11.2007 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах

персональных данных», Постановление Правительства РФ №687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также рядом иных нормативных правовых актов в сфере защиты информации.

1.4. Выполнение требований Политики ИБ является обязательным для всех структурных подразделений гимназии.

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

2. Цель и задачи политики информационной безопасности

2.1.Основными целями политики ИБ являются:

- сохранение конфиденциальности критичных информационных ресурсов;

- обеспечение непрерывности доступа к информационным ресурсам гимназии;

- защита целостности информации с целью поддержания возможности гимназии по оказанию услуг высокого качества и принятию эффективных управленческих решений;

- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами гимназии;

- 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 гимназии;

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

- организация антивирусной защиты информационных ресурсов гимназии;

- защита информации гимназии 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 гимназии.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика ИБ гимназии 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 гимназии, 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 гимназии. 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 гимназии 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 гимназии.

4. Основные мероприятия и принципы обеспечения информационной безопасности

4.1.Мероприятия по обеспечению информационной безопасности:

- защита интеллектуальной собственности гимназии;

- защита компьютеров, локальной сети гимназии и подключения к системе Интернет;

- организация защиты конфиденциальной информации.

4.2. Обладатель информации обязан обеспечить:

- предотвращения несанкционированного доступа к информации и (или) передачи ее лицам , не имеющим права на доступ к информации;

- своевременное обнаружение фактов несанкционированного доступа к информации;

Предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

- не допущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

- возможность незамедлительного востановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

- постоянный контроль за обеспечением уровня защищенности информации.

4.3. Основными принципами обеспечения ИБ:

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

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

- разработка и внедрение защитных мер;

- контроль эффективности принимаемых защитных мер;

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

5. Объекты защиты

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

- информационный процесс профессиональной деятельности;

- информационные активы гимназии.

5.2.Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности гимназии;

- 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 гимназии, активов, находящихся под контролем гимназии, а также активов, используемых для получения доступа к инфраструктуре гимназии, должна быть определена ответственность соответствующего сотрудника гимназии.

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

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

6.3. Использование в гимназии личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы гимназии производится только при согласовании с инженером-программистом.

6.4. Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну гимназии 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. 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.

6.7. 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.

6.8. Каждый сотрудник обязан немедленно уведомить ответственного за информационную безопасность обо всех случаях предоставления доступа третьим лицам к ресурсам сети гимназии. Доступ третьих лиц к информационным системам гимназии должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам гимназии должен быть четко определен, контролируем и защищен.

6.9. Сотрудникам, использующим в работе портативные компьютеры гимназии, может быть предоставлен удаленный доступ к сетевым ресурсам гимназии в соответствии с правами в информационной системе.

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

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

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

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

Рекомендованные правила:

- сотрудникам гимназии разрешается использовать сеть Интернет только в служебных целях;

- разрешается посещение сайтов в сети Интернет только для осуществления образовательной и воспитательной деятельности;

- сотрудники гимназии не должны использовать сеть Интернет для хранения персональных данных;

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

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

- запрещен доступ в Интернет через сеть гимназии для всех лиц, не являющихся сотрудниками гимназии, включая членов семьи сотрудников гимназии.

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

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

6.16. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит инженер-программист.

6.17. 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 гимназией, является ее собственностью и предназначено для использования исключительно в производственных целях.

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

6.19. 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 инженеру-программисту. 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.

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

6.21. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности.

6.22. 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

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

6.24. Сотрудники гимназии не должны:

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

6.27. Сотрудникам запрещается направлять конфиденциальную

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

6.28. Не допускается при использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

- 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.

6.29. Объем пересылаемого сообщения по электронной почте не должен превышать 10 Мбайт.

6.30. 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.

6.31. В случае кражи переносного компьютера следует незамедлительно сообщить директору гимназии.

6.32. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан: -проинформировать ответственного по информационной безопасности гимназии;

- не пользоваться и не выключать зараженный компьютер;

- не подсоединять этот компьютер к компьютерной сети гимназии до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование инженером-программистом.

6.35. Информационная обработка персональных данных должна

проходить только на защищенных техническими средствами информационной безопасности компьютерах.

6.36. Перечень помещений с техническими средствами информационной безопасности утверждается директором гимназии.

6.37. Сотрудникам гимназии запрещается:

- нарушать информационную безопасность и работу сети гимназии;
- 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 конечного устройства;
- передавать информацию о сотрудниках гимназии, обучающихся и их родителях (законных представителях) посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

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

6.42. 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.

6.43. Все заявки на проведение технического обслуживания компьютеров должны направляться инженеру-программисту.

6.47. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, и согласованны с ответственным по информационной безопасности.

7. Управление информационной безопасностью

7.1. Управление ИБ гимназии включает в себя:

- разработку и поддержание в актуальном состоянии Политики

информационной безопасности;

- 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 гимназии 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

10.1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности гимназии возлагается на ответственного по информационной безопасности, назначенного приказом директора гимназии.

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