Муниципальное автономное общеобразовательное учреждение
«Агинская средняя общеобразовательная школа №2»
Городского округа «Поселок Агинское»

ПРИКАЗ

4 октября 2022 г. № 21.

«Об информационной безопасности»

В целях обеспечения информационной безопасности и в связи с подключением школы к Единой сети передачи данных (ЕСПД) в целях обеспечения безопасного интернет-пространства, защищенного доступа к государственным и муниципальным информационным системам приказываю:

1. Назначить ответственного за мониторинг ежедневной скорости передачи данных сети Интернет (не менее 100 Мбит/с), передачу данных по протоколу IP, распределение выделенных IP-адресов системного администратора Хандамаева Б.Ц.

Системному администратору Хандамаеву Б.Ц. на рабочих станциях установить антивирусную программу.

2. Назначить ответственным за узел доступа ЕСПД, находящегося в каб. 2.2 корпуса №3 МАОУ «АСОШ №2» учителя информатики Лубсанову Н.Б.

3. Ответственным за работу точек доступа к ресурсам Интеренет (хабы, маршрутизаторы локальной сети) заместителя директора по АХЧ Базарон Р.Б.

4. Утвердить инструкции для обучающихся по информационной безопасности (приложение 1).

5. Утвердить инструкции по информационной безопасности для сотрудников (Приложение 2).

6. Утвердить Порядок действий в случае выявления нарушений информационной безопасности (Приложение 3).

7. Утвердить Положение о постоянно действующей комиссии по защите информации (Приложение 4).

8. Утвердить комиссию по защите информации в составе:
   - Базарон Р.Б., зам.директора по АХЧ;
   - Балданов Т.Ж., зам.директора по безопасности;
   - Лубсанова Н.Б., учитель информатики;
   - Тудупова Б.Ц., пдо;
   - Хандамаев Б.Ц., системный администратор.

9. Контроль за состоянием информационной безопасности назначить Тудупову Б.Ц.

Директор Л.Ц. Гонгорова

Ознакомлен

Приложение 1 к приказу №____
от «___»_____2022

Инструкция для сотрудников МАОУ «АСОШ №2» ГО «Поселок Агинское» по обеспечению информационной безопасности при использовании сети Интернет

Сотрудники подразделений несут ответственность за соблюдение информационной безопасности на закрепленных участках работы. Сотрудники подразделений:

– выполняют индивидуальные процедуры получения доступа к объектам информатизации и защищаемой информации;

– эксплуатируют пользовательские средства защиты информации, установленные на рабочих местах (если такие имеются);

– ведут журнал учета доступа к компьютеру и сети Интернет;

– в случае подозрительной активности на рабочем месте (компьютере), попытки несанкционированного доступа к информации, фактов нарушения установленной системы доступа к защищаемой информации довести информацию до системного администратора или члена комиссии по защите информации.

– контролируют состояние информационной безопасности на своих рабочих местах.

Приложение 2 к приказу №____
от «___»_____2022

Инструкция для обучающихся МАОУ «АСОШ №2» ГО «Поселок Агинское» по обеспечению информационной безопасности при использовании сети Интернет

Данная инструкция по обеспечению информационной безопасности при использовании сети Интернет разработана для учащихся начального, основного, среднего уровня обучения с целью урегулирования действия обучающихся во время пользования интернет – ресурсами.

Классным руководителям необходимо ознакомить обучающихся с правилами безопасности в Интернете, провести беседу с учащимися. Приведенные правила безопасности в сети Интернет школьникам необходимо помнить и придерживать их.

1. Правила безопасности в сети Интернет для обучающихся начального общего образования

✓ Всегда задавайте вопросы родителям о незнакомых вам вещах в Интернете. Они подробно расскажут, что безопасно делать, а что может причинить вред.

✓ Перед тем, как подружиться с кем-либо в сети Интернет, спросите у родителей как вести безопасное общение.

✓ Не при каких обстоятельствах не рассказывайте о себе незнакомцам. Где и с кем вы живете, в какой школе обучаетесь, номер телефона должны знать исключительно Ваши друзья и родственники.

✓ Не отсылайте свои фотографии людям, совершенно не знакомым Вам. Нельзя чтобы совершенно незнакомые люди видели Ваши фотографии, фотографии Ваших друзей или Вашей семьи.

✓ Никогда не соглашайтесь на личную встречу с людьми из Интернета без сопровождения родителей. В сети Интернет много людей рассказывающих о себе неправду.

✓ Ведя общение в Интернет сети, всегда будьте дружелюбны к другим людям. Нельзя писать грубые слова, поскольку читать грубости так же неприятно, как и слышать. Вы можете случайно обидеть человека.

✓ В случае, если вас кто-то расстроил или обидел, следует обязательно рассказать родителям.

2. Правила безопасности в сети Интернет для обучающихся основного общего образования

✓ Регистрируясь на различных сайтах, всегда старайтесь не указывать личную информацию, потому что она может быть доступна совершенно незнакомым людям. Так же, не желательно размещать своё фото, давая, тем самым, представление о Вашей внешности, совершенно посторонним людям.

✓ Пользуйтесь веб-камерой исключительно для общения с друзьями. Следите, чтобы посторонние вам люди не могли видеть ваш разговор, т.к. его можно записать.

✓ Нежелательные письма от незнакомцев называются «Спам». Если вы вдруг получили подобное письмо, никогда не отвечайте на него. Если Вы ответите на такое

письмо, отправивший будет знать, что вы используете свой электронный почтовый ящик и будет продолжать слать вам «Спам».

✓ В случае, если вы получили письмо с совершенно незнакомого адреса, его желательно не открывать. Такие письма зачастую содержат вирусы.

✓ Если вы получаете письма с неприятным и оскорбительным для вас содержанием или кто-нибудь ведет себя по отношению к вам неподобающим образом, обязательно сообщите об этом.

✓ Если вдруг вас кто-либо расстроил или обидел, расскажите обо всем взрослому.

3. Правила безопасности в сети Интернет для обучающихся среднего общего образования

✓ Не рекомендуется размещение личной информации в Интернет сети. Личная информация: номер вашего мобильного телефона, адрес электронной почты, домашний адрес и ваши фотографии, фотографии членов вашей семьи или друзей.

✓ Если вы выложите фото или видео в интернете — любой может посмотреть их.

✓ Никогда не отвечайте на «Спам» (нежелательную электронную почту).

✓ Нельзя открывать файлы, полученные от неизвестных Вам людей. Вы ведь не знаете, что в действительности содержат эти файлы в них могут находиться вирусы или фото/видео с «агрессивным» содержимым.

✓ Никогда не добавляйте незнакомых вам людей в свой список контактов.

✓ Не забывайте, что виртуальные друзья и знакомые могут быть не теми на самом деле, за кого себя выдают.

✓ Если около вас или поблизости с вами нет родственников, никогда не встречайтесь в реальности с людьми, с которыми вы познакомились в Интерне сети. Если ваш виртуальный друг в действительности тот, за кого себя выдает, он с пониманием отнесется к вашей заботе о собственной безопасности!

✓ В любое время можно рассказать взрослым, если вас кто-либо обидел.

Приложение 3 к приказу №____
от «___»_____2022

Порядок действий в случае выявления нарушений информационной безопасности

Действия, предпринимаемые в случае выявления нарушений информационной безопасности, состоят в следующем:

– выявление факта нарушения;

– прекращение всех операций, связанных с участком, на котором произошло нарушение;

– принятие экстренных мер для прекращения несанкционированного доступа или использования информации;

– оповещение о нарушении;

– восстановление работоспособности информационной системы;

– расследование причин нарушения информационной безопасности;

– проверка состояния информационной безопасности по факту нарушения.

Выявление факта нарушения, как правило, происходит в ходе контроля состояния информационной безопасности системным администратором.

Немедленно после выявления нарушения сотрудник, который обнаружил его, обязан прекратить все операции по использованию по назначению информации и средств информатизации, которые выполнялись на участке, где произошло нарушение, а также, если необходимо, на смежных участках.

Если выявлен несанкционированный доступ в категорированные помещения, всякий доступ в него должен быть прекращен.

Если на момент выявления нарушения несанкционированный доступ или использование средств информатизации и информации еще продолжаются, сотрудник, выявивший их, обязан немедленно принять меры к их прекращению. Конкретное содержание этих мер зависит от того, каков характер нарушения, то есть информационный объект какой категории попал под нарушение, какой ущерб может быть нанесен нарушением, какие побочные последствия повлечет принятие этих мер. По возможности следует привлечь для выработки и принятия мер системного администратора, заместителя директора по безопасности, учителя по информатике.

Ответственность за адекватность принимаемых мер несут в порядке привлечения сотрудник, выявивший нарушение, системный администратор, комиссия защите информации.

После того, как нарушение выявлено и блокировано, производится срочное оповещение о нем в следующем порядке:

– сотрудник оповещает руководителя, комиссию по защите информации и системного администратора;

– комиссия по защите информации оповещает другие подразделения, на участках ответственности которых могут возникнуть подобные нарушения.

С целью минимизации ущерба от прекращения работы информационной системы немедленно после того, как возможность дальнейшего нарушения информационной безопасности устранена, принимаются меры для восстановления ее работы. Решение на

восстановление работы принимает системный администратор, по согласованию с комиссией по защите информации.

Расследование причин нарушения производится комиссией по защите информации, при этом все связанные с нарушением сотрудники должны оказывать содействие расследованию. Целью расследования является выявление истинных причин нарушения и предпосылок к нему для принятия мер к недопущению его повторения. Расследование проводится сразу после восстановления работоспособности информационной системы, в обязательном порядке, независимо от последствий, которые повлекло нарушение. Результаты расследования оформляются двусторонним Актом комиссией по защите информации, и сотрудником, в котором произошло нарушение.

По факту нарушения комиссия по защите информации проводится также проверка системы информационной безопасности на тех ее участках, где подобные нарушения возможны. Доклад о факте нарушения и ходе работ по его устранению производится в зависимости от характера нарушения и размера возможного ущерба от него.

Ответственность за своевременность доклада несет сотрудник, в котором произошло нарушение (первая очередь) и комиссия по безопасности и защите информации (вторая очередь).

Приложение 4 к приказу №____
от «___»_____2022

Положение о постоянно действующей комиссии по защите информации

1. Общие положения

1.1. Постоянно действующая комиссия по защите информации (далее ПДК) организует и координирует действия МАОУ «АСОШ №2» ГО «Поселок Агинское» (далее - школа) в вопросах защиты информации.

1.2. В своей деятельности ПДК руководствуется законодательством Российской Федерации, постановлениями Правительства Российской Федерации, нормативно-методическими документами по проблемам безопасности и защиты информации, а также приказами и распоряжениями руководителя Организации и настоящим Положением.

1.3. Состав ПДК определяется приказом руководителя Организации.

1.4. ПДК осуществляет свою деятельность в тесном взаимодействии с другими структурными подразделениями школы.

2. Задачи и функции постоянно действующей комиссии по защите информации

2.1. Основными задачами ПДК по защите информации в школе являются:

- своевременное выявление и устранение угроз безопасности информации;
- создание условий и механизма оперативного реагирования на угрозы безопасности информации;
- эффективное пресечение посягательств на информационные ресурсы на основе правовых, организационных, инженерно-технических, программных средств обеспечения безопасности информации;
- создание условий для максимально возможного возмещения ущерба и локализации негативных последствий, возникших в результате неправомерных действий физических лиц или случайных событий, ослабления последствий нарушения безопасности информации.

2.2. С целью достижения наиболее эффективного результата в решении поставленных задач ПДК осуществляет следующие функции:

- установленным порядком решает вопросы изменения конфиденциальности обрабатываемой информации;
- разрабатывает «Перечень информационных ресурсов Организации, подлежащих защите»;
- определяет перечень основных технических средств и систем, предназначенных для обработки информации;
- в случае необходимости проводит категорирование объектов информатизации и классификацию защищенности автоматизированных систем;
- разрабатывает разрешительную систему доступа пользователей и эксплуатационного персонала к обрабатываемой информации, подлежащей защите;
- ведет учет и анализ нарушений режима секретности, попыток несанкционированного доступа к защищаемой информации;
- проводит служебные расследования по фактам нарушения установленной системы доступа к защищаемой информации;

- дает экспертную оценку организационно-распорядительной документации по вопросам защиты информации;
- рассматривает возможность передачи конфиденциальной информации Организации по запросам сторонних организаций;
- принимает решения о возможности использования в Организации и его территориальных органах технических, программных, программно-аппаратных и криптографических средств защиты информации;
- осуществляет контроль полноты и своевременности выполнения мероприятий по защите информации и принятых решений ПДК в подразделениях школы;
- ведет работу по совершенствованию системы защиты информации;

3. Права комиссии

3.1. ПДК имеет право:

- проводить проверки соблюдения режима защиты информации в подразделениях школы;
- вносить предложения директору школы по совершенствованию существующей системы защиты информации;
- привлекать по согласованию к работе по созданию и совершенствованию системы защиты информации других сотрудников школы;
- проводить служебные расследования по фактам утечки информации или грубых нарушений режима защиты информации;
- требовать от сотрудников школы письменных объяснений при проведении служебных расследований;
- вносить предложения директору руководителю школы об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по защите информации;
- давать сотрудникам школы обязательные для выполнения указания по защите конфиденциальной информации, определяемые существующим в Российской Федерации законодательством и требованиями Организации.

3.2. Членам комиссии запрещается

- доводить до сотрудников школы систему защиты информации в полном объеме;
- при выводе из состава комиссии запрещается раскрывать объем работы и конкретные направления деятельности комиссии, разглашать информацию, ставшую известной в ходе работы в составе ПДК.