Муниципальное бюджетное общеобразовательное учреждение
«Подболотная средняя общеобразовательная школа»
(МБОУ «Подболотная СОШ»)

ПРИКАЗ

02 февраля 2024 года № 36

д.Ляменьга

О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ООП
НОО, ООП ООО, ООП СОО

На основании запроса АОУ ВО ДПО «Вологодский институт развития образования» №ИС-01-07/144 от 19.01.2024 года, а также во исполнение поручения Врио Губернатора области от 14.12.2023 года № ПОР.01-295/23, протокола педсовета от 02.02.2024 года №2,

ПРИКАЗЫВАЮ:

1. Внести изменения в содержательный (рабочая программа воспитания) раздел ООП НОО, ООП ООО, ООП СОО: в п.46.3.2.11. ООП НОО, п. 54.3.2.11. ООП ООО, п. 166.3.2.11. ООП ООО для 9 классов, п.46.3.2.11. ООП СОО, п. 130.3.2.11. ООП СОО для 11 класса после слов «Блок безопасности дорожного движения» добавить текст следующего содержания:

«***Блок информационная безопасность***

Информационная безопасность (далее – ИБ) ОО представляет собой комплекс мер различного характера, направленных на реализацию двух основных целей. Первой целью является защита персональных данных и информационного пространства от несанкционированных вмешательств, хищения информации и изменения конфигурации системы со стороны третьих лиц. Вторая цель ИБ – защита учащихся от любых видов пропаганды, рекламы, запрещенной законом информации.

ИБ в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим трем группам:

персональные данные и сведения, которые имеют отношения к учащимся, преподавательскому составу, персоналу организации, оцифрованные архивные документы;

обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения учебного процесса;

защищенная законом интеллектуальная собственность.

Действия злоумышленников могут привести к хищению указанных данных. Также при несанкционированном вмешательстве возможны внесения изменений и уничтожение хранилищ знаний, программных кодов, оцифрованных книг и пособий, используемых в образовательном процессе.

В обязанности лиц, отвечающих за информационную безопасность, входит:

обеспечение сохранности защищаемых данных;

поддержание информации в состоянии постоянной доступности для авторизованных лиц;

обеспечение конфиденциальности подлежащих защите сведений, предотвращение доступа к ним со стороны третьих лиц.

Угрозы ИБ.

Спецификой обеспечения ИБ в информационных учреждениях является состав характерных угроз. К ним относится не только возможность хищения или повреждения

данных хакерами, но также деятельность учащихся. Подростки могут сознательно или ненамеренно повредит оборудование или заразить систему вредоносными программами.

Угрозам намеренного или ненамеренного воздействия могут подвергаться следующие группы объектов:

компьютерное и другое оборудование образовательной организации, в отношении которого возможны воздействия вредоносного ПО, физические и другие воздействия;

программное обеспечение, применяемое в учебном процессе или для работы системы;

данные, которые хранятся на жестких дисках или портативных носителях;

дети и подростки, которые могут подвергаться стороннему информационному воздействию;

персонал, поддерживающий работу ИТ-системы.

Угрозы информационной безопасности ОО могут носить непреднамеренный и преднамеренный характер. К угрозам первого типа относятся:

аварии и чрезвычайные ситуации – затопление, отключение электроэнергии и т. д.;

программные сбои;

ошибки работников;

поломки оборудования;

сбои систем связи.

Особенностью непреднамеренных угроз является их временное воздействие. В большинстве случаев результаты их реализации предсказуемы, достаточно эффективно и быстро устраняются подготовленным персоналом.

Намного более опасными являются угрозы информационной безопасности намеренного характера. Обычно результаты их реализации невозможно предвидеть. Намеренные угрозы могут исходить от учащихся, персонала организации, конкуренты, хакеры. Лицо, осуществляющее преднамеренное воздействие на компьютерные системы или программное обеспечение, должно быть достаточно компетентным в их работе. Наиболее уязвимыми являются сети с удаленным в пространстве расположением компонентов. Злоумышленники могут достаточно легко нарушать связи между такими удаленными компонентами, что полностью выводит систему из строя.

Существенную угрозу представляет хищение интеллектуальной собственности и нарушение авторских прав. Также внешние атаки на компьютерные сети образовательной организации могут предприниматься для воздействия на сознание детей. Наиболее серьезная угроза – возможность вовлечения детей в криминальную или террористическую деятельность.

Меры защиты

Современные технологии информационной безопасности образовательной организации предусматривают обеспечение защиты на 5 уровнях:

нормативно-правовой;

морально-этический;

административно-организационный;

физический;

технический.

Нормативно-правовой способ защиты

Основным документом, определяющим степень угроз и меры обеспечения информационной безопасности обучающихся в ОО, является «Национальная стратегия действий в интересах детей». Она предусматривает приоритет мер, направленных на защиту сознания ребенка от информационного воздействия агрессивного характера. Меры по защите информационных систем и баз данных имеют второй уровень приоритетности.

Законодательством определяются данные, которые должны быть защищены от несанкционированного доступа третьих лиц. К числу таких сведений относятся:

персональные данные;

конфиденциальные сведения;

служебная, профессиональная, коммерческая тайна.

Порядок обеспечения безопасности персональных данных регламентируется Трудовым кодексом, Гражданским кодексом, Федеральным законом «Об информации» и другими актами. Конкретные меры по защите данных, используемое для этого аппаратное и методическое обеспечение определяются законами и профильными ГОСТами.

Морально-этические средства обеспечения информационной безопасности

Система морально-этических ценностей имеет особое значение в сфере образования. Она служит основой для выработки комплекса мер, направленных на защиту детей и подростков от информации этически некорректного, травмирующего, противозаконного характера. Защита детей от пропаганды основывается на законе «О защите прав ребенка». Этим актом определяются права детей на защиту от информации, которая может стать причиной моральной травмы.

В рамках мер по обеспечению ИБ создаются перечни источников (программ, документов и т. д.) способных травмировать детскую психику. В результате принимаемых мер должен предотвращаться доступ таких источников на территорию образовательного учреждения.

Меры административно-организационного характера

Система административно-организационных мер строится на базе внутренних регламентов и правил организации, которыми регламентируется порядок обращения с информацией и ее носителями. В том числе должны быть разработаны:

должностные инструкции;

внутренние методики по ИБ;

перечни не подлежащих передаче данных;

регламент взаимодействия с уполномоченными государственными органами по запросам о предоставлении информации и т. д.

Разработанными методиками должен определяться порядок доступа учеников в интернет во время занятий в компьютерных классах, меры по предотвращению доступа детей к определенным ресурсам, предотвращение использования ими своих носителей информации и т. д.

Физические меры

Ответственность за реализацию мер защиты компьютерной сети и носителей информации физического характера несет непосредственно руководитель образовательной организации и ее IT-персонал. Не допускается перекладывание этих мер на наемные охранные структуры.

К числу физических мер относятся:

реализация пропускной системы для доступа в помещения, в которых находятся носители данных;

создание системы контроля и управления доступом;

определение уровней допуска;

создание правил обязательного регулярного копирования критически важных данных на жесткие диски ПК, не подключенных к интернету.

Также среди физических мер можно назвать правила по созданию паролей и их периодической замене.

Технические меры

Технические меры защиты предусматривают использование специализированного программного обеспечения. В том числе в образовательных организациях рекомендуется использовать DLP и SIEM-системы, которые эффективно обнаруживают угрозы ИБ и обеспечиваю борьбу с ними. При невозможности использования подобных систем по причине бюджетных ограничений, применяются рекомендованные и разрешенные антивирусы и другие виды специального софта.

Применяемое для технической защиты программное обеспечение должно

обеспечивать контроль электронной почты, которой пользуются ученики или персонал образовательной организации. Также могут устанавливаться ограничения на копирование данных с жестких дисков компьютеров. Обязательно рекомендуется использование контент-фильтра, с помощью которого ограничивается доступ детей к определенным ресурсам в интернете.

Программа классных часов является частью комплексной работы по обеспечению информационной безопасности участников образовательного процесса и должна быть включена в план воспитательной работы школы. Разработка формы и содержания программы классных часов базируется на основных принципах деятельностного подхода и развивающего обучения.

Принцип активной включенности школьников в освоение информации предполагает субъектную позицию школьника в образовательном процессе, обращение педагога к личностному опыту учащегося и обогащение его в процессе деятельности на занятии.

Принцип деятельностных технологий заключается в интерактивности образовательного процесса, организации совместной деятельности ребенка и взрослого с учетом возрастных и индивидуальных особенностей обучающихся.

Принцип доступности предполагает, что форма и содержание классных часов соответствует возрастным и психологическим особенностям школьников, а также имеющемуся у них социальному опыту.

Дети младшего школьного возраста (1-4 класс) активно осваивают виртуальное пространство, знакомятся с контентом, играют в сетевые игры. Этот возраст является самым чувствительным для освоения моральных, культурных норм, ценностных, духовных ориентаций, а также наиболее благоприятен для формирования базовых навыков и усвоения основных правил безопасного использования Интернета.

Младшие подростки (5-6 класс) в соответствии с возрастными особенностями более активно начинают использовать Интернет для коммуникации: для них наибольший интерес представляет общение в чатах, мессенджерах, в социальных сетях. Однако особенности онлайн-общения подростков (высокий уровень активности, бесцельное блуждание по Интернет-ресурсам, агрессивная самопрезентация) являются потенциальными источниками угроз для их безопасности, например, таких, как установление случайных контактов с незнакомцами, вовлечение в антисоциальные группы, возникновение конфликтных ситуаций. Для снижения рисков, связанных с Интернет-общением, в этом возрасте целесообразно расширение представлений о правилах личной безопасности при онлайн-коммуникации.

Подростки 13-15 лет (7-9 класс) являются уверенными пользователями Интернета, и их деятельность в сети все меньше подвергается контролю со стороны взрослых. Для детей этого возраста является нормальным желание выяснить, что они могут себе позволить делать без разрешения взрослых. Поэтому, находясь в Интернете, школьник может попытаться посетить сайты или пообщаться в чатах, разрешения на которые он не получил бы от родителей. Соответственно, повышается риск столкновения с негативным контентом и другими Интернет-угрозами. На этом этапе овладение способами противодействия Интернет-угрозам позволит предотвратить нежелательные последствия негативного опыта пользования Интернетом. Старшеклассники (10-11 класс) имеют значительный опыт использования Интернет-пространства, они способны критически оценивать информацию, обладают навыками справляться с Интернет-угрозами или избегать их. Для развития навыков ответственного законопослушного поведения в Интернете старшеклассникам предлагается рассмотреть правовые аспекты использования информации и ресурсов глобальной сети.

Принцип системности реализуется через целостное представление о глобальной сети Интернет, ее позитивных возможностей и рисков ее использования с ориентацией на возрастной аспект.

Принцип рефлексивности предполагает создание условий для осознания обучающимися на доступном уровне полученной информации через самостоятельную познавательную деятельность, что обеспечивает формирование ответственного и безопасного поведения в сети Интернет.

Принцип мотивации заключается в побуждении обучающихся к самостоятельному поиску новой информации по использованию информационно-коммуникационных технологий, в том числе сети Интернет, в познавательных и развивающих целях.

Принцип открытости содержания образования предполагает, что педагог, не искажая логики и содержания представленной информации, может свободно выходить за рамки предлагаемой структуры классного часа. В этой связи, он должен обладать сформированными информационными компетенциями, быть уверенным пользователем сети Интернет, а также владеть терминологией, желательно не только технической, но и сленговой. Особенно это актуально при проведении классных мероприятий со старшеклассниками.»

2. Внести изменения в организационный (календарный план воспитательной работы) разделы ООП НОО, ООП ООО, ООП СОО:

2.1. п. 50.4. ООП НОО, раздел «Профилактика и безопасность» дополнить следующими строками:

Урок Цифры на тему «Кибербезопасность будущего» в рамках Всероссийского образовательного проекта в сфере цифровой экономики «Урок Цифры»	1-4	с 15 января по 4 февраля	Классные руководители Учителя информатики
Викторина «Безопасность пользователей в сети Интернет»	1-4	Март	Классные руководители Учителя информатики
Классные часы-практикумы «Правила кибербезопасности»	1-4	Апрель	Классные руководители Учителя информатики

2.2. п. 58.10. ООП ООО и п. 167.10. ООП ООО для 9 класса, раздел «Профилактика и безопасность» дополнить следующими строками:

Урок Цифры на тему «Кибербезопасность будущего» в рамках Всероссийского образовательного проекта в сфере цифровой экономики «Урок Цифры»	5-9	с 15 января по 4 февраля	Классные руководители, учителя информатики
Викторина «Безопасность пользователей в сети Интернет»	5-6	Март	Классные руководители, учителя информатики
Цифровой квест «Безопасность в сети Интернет»	5-6	Апрель	Классные руководители, учителя информатики
Классный час «Как пользоваться мобильной связью без вреда своему здоровью»	5-6	Май	Классные руководители, учителя информатики
Классные часы с просмотром роликов и обсуждением, диспутом, беседой	7-9	Март	Классные руководители, учителя информатики
Классные часы-практикумы «Правила кибербезопасности»	7-9	Апрель	Классные руководители, учителя информатики

2.3. п. 50.4. ООП СОО и п. 134.4. ООП СОО для 11 класса, раздел «Профилактика и безопасность» дополнить следующими строками:

Урок Цифры на тему «Кибербезопасность будущего» в рамках Всероссийского образовательного проекта в сфере цифровой экономики «Урок Цифры»	10-11	с 15 января по 4 февраля	Классные руководители, учителя информатики

Классные часы с просмотром роликов и обсуждением, диспутом, беседой	10-11	Март	Классные руководители, учителя информатики
Классные часы-практикумы «Формирование навыков безопасного и ответственного поведения в сети», «Предупреждён – значит вооружён»	10-11	Апрель	Классные руководители, учителя информатики

3. Разместить Гоглеву Д.В., инженеру-программисту, указанные в п. 1 – 2 документы на сайте школы до 05.02.2024 года.

4. Возложить контроль за исполнением приказа на Гоглеву Н.В., заместителя директора по УВР.

Директор А.М. Шушков

С приказом ознакомлены: