

Научная статья

УДК 614.8

doi: 10.34987/2712-9233.2023.99.67.001

Безопасность в условиях цифровых коммуникаций учащихся

Кокорев Николай Михайлович

Сибирская пожарно-спасательная академия ГПС МЧС России, Железногорск, Россия

Автор ответственный за переписку: Кокорев Николай Михайлович, kokarev.nikolaj@mail.ru

Аннотация. Безопасность детей - одна из основных задач общества. В настоящее время каждый учащийся имеет личное электронное устройство с неограниченным доступом в сеть Интернет. Учитывая, что современный образовательный процесс неотделим от использования информационных ресурсов – неконтролируемый доступ в сеть является основной проблемой образования. Проводя большую часть времени в новой сетевой реальности учащемуся очень непросто увидеть и осознать опасность, не поддаться негативному влиянию сети Интернет. Главная задача родителей, педагогов и в целом общества – обеспечить безопасность учащихся при взаимодействии их с информационным пространством.

Ключевые слова: пожар, предприятие, взрывоопасные концентрации, кратность воздухообмена, статистика.

Для цитирования: Кокорев Н.М. Безопасность в условиях цифровых коммуникаций учащихся // Актуальные проблемы безопасности в техносфере. 2023. № 3 (11). С.6-9. URL: <https://doi.org/10.34987/2712-9233.2023.99.67.001>.

Development of an event to reduce the likelihood of an emergency at an object of protection

Nikolay M. Kokorev

Siberian Academy of state Fire Service of EMERCOM of Russia, Zheleznogorsk, Russia

Corresponding author: Nikolay Mikhailovich Kokorev, kokarev.nikolaj@mail.ru

Abstract. The safety of children is one of the main tasks of society. Currently, each student has a personal electronic device with unlimited Internet access. Considering that the modern educational process is inseparable from the use of information resources, uncontrolled access to the network is the main problem of education. Spending most of the time in the new online reality, it is very difficult for a student to see and realize the danger, not to succumb to the negative influence of the Internet. The main task of parents, teachers and society as a whole is to ensure the safety of students when they interact with the information space.

Keywords: safety, Internet, safe information educational environment, students' safety.

For citation: Kokorev N.M. Safety in the Conditions of digital communications of students // Actual problems of safety in the technosphere. 2023. No.3(11). P. 6-9. URL:<https://doi.org/10.34987/2712-9233.2023.99.67.001>.

В настоящее время информационная учебная среда дает принципиально новую возможность организовать учебную и внеучебную деятельность учащихся, повышать эффективность учебного процесса, выстраивать индивидуальный процесс обучения, способствует высокому уровню самореализации и самостоятельности обучающихся. Доступ к Интернет-ресурсам позволяет учащимся использовать основные и дополнительные учебные материалы, необходимые для обучения, выполнять задания, и самостоятельно обучаться. Можно выделить основные виды деятельности учащихся, использующих сеть Интернет

в процессе обучения: переписка через электронную почту, поиск, хранение и передача необходимой учебной информации, обмен учебным материалом, использование электронного образовательного ресурса и программы обучения, информационное сотрудничество с педагогами, участие в сетевых проектах, конкурсах, конференциях.

Однако, при организации образовательного процесса с использованием Интернет-ресурсов, в особенности во внеурочные периоды, следует обратить особое внимание на безопасность учащихся. Использование интернета влечет за собой множество различных рисков. Согласно статистическим данным, сегодня в России около 129,8 млн интернет-пользователей. Доля пользователей интернета в возрасте от 12 до 24 лет самая большая по сравнению с другими возрастными категориями — 97,1%.

В условиях всеобщего развития цифровых технологий, учащиеся все чаще сталкиваются с рисками и угрозами для своей безопасности в сети Интернет.

Как правило, учащиеся самостоятельно выходят в мировую сеть, без надзора родителей, педагогов. Некоторые посещают сайты с нежелательным и запрещённым содержанием.

Бесконтрольное использование сети Интернет может привести к серьезным последствиям, таким как игровая зависимость, неправильное формирование нравственных ценностей, кибербуллинг, насилие в сети, утечка личной информации, и многое другое.

Нарастающая угроза требует решительных действий по обеспечению безопасности учащихся в информационной образовательной среде, по организации для них безопасного образовательного пространства.

Кто же несет ответственность за обеспечение безопасности учащихся в информационном образовательном пространстве? Я считаю это общим делом и ответственностью: государства, системы образования, семьи. Каждый из них в той или иной мере отвечает за безопасное взаимодействие учащихся с информационным гиперпространством.

Ряд нормативных документов федерального уровня устанавливает запрет на распространение информации, наносящей вред психике детей и подростков, но стремительный рост средств связи, коммуникаций способствует возникновению новых методов и методик воздействия на учащихся, и на сегодняшний день назревает потребность в совершенствовании законодательства по информационной безопасности.

Особо следует подчеркнуть ответственность родителей за защиту учащихся в информационной среде, именно родители как никто другой отвечают за безопасность собственных детей.

Родителям необходимо ежедневно контролировать количество времени, проведенное их детьми в Интернете, понимать с кем они общаются по сетевым сервисам, какую информацию получают и обрабатывают. Необходимо понимать истинные нужды своих детей, находить силы и время для общения, совместных игр, уметь слушать и слышать своего ребёнка. Родители должны постараться сформировать у себя информационно-коммуникационную культуру, дающую им возможность разбираться в современных средствах коммуникации, и тогда виртуальное пространство станет для семьи помощником в образовании и развитии детей.

Далее рассмотрим роль системы образования в обеспечении информационной безопасности учащихся. Деятельность педагога в обязательном порядке должна включать в себя: организацию и проведение тематических профилактических встреч с родителями, которые могут быть разнообразными: родительские собрания, индивидуальные встречи и консультации, встречи со специалистами.

Кроме работы с родителями, важнейшую роль в организации безопасного информационно-образовательного пространства играют профилактические работы с учащимися организованные с учетом их возраста. Целесообразно проводить такие мероприятия в форме бесед, диспутов, тренингов, проектов, выпуска стенгазет, участия в олимпиадах и конкурсах, анкетирования учащихся.

Помимо профилактики, для предотвращения негативного влияния интернета каждое образовательное учреждение должно проводить целенаправленную воспитательную работу как с учащимися, так и с педагогами.

Работа может вестись в форме классных часов, семинаров, мастер-классов, круглых столов.

В целом для достижения положительных результатов необходимо проводить совместную комплексную работу родителей и педагогов. Именно такое взаимодействие семьи и образовательного учреждения поможет в полной мере предотвратить возможные негативные последствия, избежать возможных опасностей и ошибок, обеспечить безопасность образовательного пространства.

Безопасное информационное образовательное пространство включает в себя:

организацию технического надзора за безопасностью;

подготовку педагогов к использованию Интернет-ресурсов;

создание условий педагогической безопасности для информационной безопасности обучающихся, пользующихся Интернетом в образовательном процессе;

разъяснительные работы среди учащихся, информационное обеспечение процесса образования.

Используя Интернет, как инструмент образовательного процесса, образовательные учреждения должны проводить следующие организационно-методические мероприятия:

- назначение ответственного за работу Интернет-точки;
- утверждение инструкций для ответственного за работу Интернет-точки;
- организация контроля использования учащимися сети Интернет;
- осуществление информационного и методического обеспечения для работы с Интернет-ресурсами;
- утверждение документов, регламентирующих деятельность образовательных субъектов в сети интернет: регламент о работе педагогов и учащихся в сети интернет, правила пользователя о безопасности работы в сети Интернет, инструкция для педагогов по порядку действий при контроле использования учащимися Интернета.

Чтобы ограничить доступ к информации, способной негативно влиять на учащихся, образовательные учреждения устанавливают специальные системы фильтрации контента и антивирусные программы. Контроль использования учащимися Интернета можно осуществлять с использованием программных средств и видеоконтроля.

Итак, важнейшая задача каждого образовательного учреждения – обеспечить безопасность той информационно-образовательной среды, в которую оказывается погружен ученик, участвующий в образовательном процессе.

Для более детальной разработки теоретических и практических основ информационной безопасности, учащихся в сети Интернет необходим научный алгоритм, который будет учитывать особенности возникновения угроз и рисков в условиях цифровых коммуникаций учащихся.

Шаг 1. Разработка комплексной модели учащегося в информационном пространстве сети Интернет.

Данная модель должна содержать совокупность взаимосвязанных профилей учащегося для доступа к различным сервисам сети Интернет. Анализ подобной модели позволит сделать обоснованные выводы об интересах учащегося во всемирной паутине, получить представление о его предпочтениях и мотивах. Модель учащегося в сети Интернет можно дополнить загружаемым, скачиваемым и порождаемым им контентом, который может включать в себя текстовые, графические, аудио и видео материалы.

Шаг 2. Выполнение анализа угроз информационной безопасности обучающихся в сети Интернет.

В ходе анализа необходимо изучить источники информации на тему интернет-безопасности, дать оценку влияния технологического развития на возникновение угроз и рисков, выявить основания для их классификации и описания.

Результаты анализа позволят определить наиболее вероятные риски, а также составить подробный список технологических угроз.

Шаг 3. Детальное изучение существующих проблем интернет-зависимости учащихся во всех аспектах.

Здесь можно выделить актуальные примеры интернет-зависимости: от социальных сетей, от сайтов развлекательной направленности, от социальных сетей, от видеохостингов, от онлайн-игр.

Шаг 4. Исследование основных принципов организации защиты учащихся от вредной информации в сети Интернет.

Желательно изучить позитивный и негативный опыт в России и в зарубежных странах. Проанализировать его эффективность и определить область использования и применения.

Шаг 5. Контроль за безопасностью в сети с использованием аппаратных и программных средств.

Пятый шаг заключается во внедрении правил безопасности и мониторинге деятельности учащихся в интернете. Необходимо изучить рынок современных аппаратных и программных средств обеспечения информационной безопасности в сети Интернет (антивирусные программы, фильтры для родительского контроля и т.п.), проанализировать их эффективность и обеспечить их использование в процессе обучения.

Шаг 6. Определение правил поведения в сети.

Шестой шаг заключается в определении правил поведения учащихся в интернете. Важно выработать критерии, которые будут привлекать внимание к вопросу безопасности и формированию сетевой культуры. Например, необходимо разработать правила поведения в чатах, социальных сетях, мессенджерах и т.д. Особое внимание следует уделить умению отличать достоверные данные от недостоверных, критически относиться к получаемой информации.

Шаг 7: Обучение учащихся.

Детальное изучение теоретических и практических основ информационной безопасности учащихся в глобальной сети Интернет позволит выработать список мер позволяющих значительно повысить уровень информационной безопасности в сети Интернет. Проведение уроков об информационной безопасности должно обеспечить информирование учащихся о видах информации, способной причинить вред здоровью, а также о незаконных способах и негативных последствиях распространения такой информации, о мерах ответственности за вышеуказанные действия. Важно уделить внимание развитию навыков продуктивного использования интернета и осознанному подходу к защите своих персональных данных.

Шаг 8. Оценка эффективности решений.

Последний шаг заключается в оценке эффективности решений и их дальнейшей корректировке. На основе анализа результатов можно создать индивидуальный подход к каждому ученику, учитывающий его особенности и потребности. Это поможет обеспечить наивысшую эффективность использования мер безопасности в интернете.

Заключение:

Применение Интернета в образовательном процессе влечет за собой множество рисков для учащихся, порождает немалое количество сложных ситуаций, решение которых требует значительных ресурсов.

Решение проблемы требует комплексного подхода – работа должна быть организована со всеми заинтересованными аудиториями: школьниками, студентами, педагогами и родителями.

Процесс обеспечения безопасности в условиях цифровых коммуникаций учащихся является важной задачей, которая требует научного подхода. На основе вышеприведенного научного алгоритма, можно создать систему мероприятий, которые будут учитывать особенности рисков и угроз в условиях цифровых коммуникаций и позволят обеспечить максимальный контроль за безопасностью учащихся в Интернете.

Список источников

1. Информационная безопасность в 2021 году. Угрозы, отраслевые тренды / [Электронный ресурс] // <https://habr.com/> [сайт]. — URL: <https://habr.com/ru/company/itglobalcom/blog/540748/> (дата обращения: 11.09.2023).
2. Актуальные тренды кибербезопасности в 2021 году / [Электронный ресурс] // <https://habr.com/>: сайт. — URL: <https://habr.com/ru/articles/579724/> (дата обращения: 11.09.2023).
3. Федеральный закон Российской Федерации О защите детей от информации, причиняющей вред их здоровью и развитию" от 29.12.2010 N 436-ФЗ (последняя редакция) / Федеральный закон Российской Федерации [Электронный ресурс] // consultant.ru: сайт. — URL: https://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 11.09.2023).
4. Как защитить ребенка от угроз в интернете? / [Электронный ресурс] // 02.mchs.gov.ru: сайт. — URL: <https://02.mchs.gov.ru/deyatelnost/poleznaya-informaciya/rekomendacii-naseleniyu/detskaya-bezopasnost/kak-zashchitit-rebenka-ot-ugroz-v-internete> (дата обращения: 11.09.2023).
5. Безопасность в интернете: возрастные рекомендации для детей и подростков / [Электронный ресурс] // www.kaspersky.ru: сайт. — URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/kids-guidelines> (дата обращения: 11.09.2023).

Статья поступила в редакция 26.09.2023; одобрена после рецензирования 29.09.2023, принята к публикации 02.10.2023.

The article was submitted 26.09.2023, approved after reviewing 29.09.2023, accepted for publication 02.10.2023.