ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ СРЕДЫ

Известия Балтийской государственной академии рыбопромыслового флота. 2025. № 3(73). С. 165–169.
Научная статья
УДК 377, 378
Doi:10.46845/2071-5331-2025-3-73-165-169

Формирование культуры кибербезопасности обучающихся

Юрий Александрович Бахарев[1]✉, Алексей Владимирович Гущин[2], Мария Петровна Прохорова[3]
[1]Нижегородский государственный университет им. Н. И. Лобачевского, Нижний Новгород, Россия
[2]Нижегородская государственная консерватория им. М. И. Глинки, Нижний Новгород, Россия
[3]Нижегородский государственный педагогический университет им. К. Минина, Нижний Новгород, Россия
[1]baharev_84@list.ru✉, http://orcid.org/0000-0001-8505-3387
[2]aland-ag@mail.ru, http://orcid.org/0000-0001-7855-2831
[3]prohorova_mp@mininuniver.ru, http://orcid.org/0000-0003-0357-4213

Аннотация. Рассматривается проблема кибербезопасности. Формировать культуру кибербезопасности населения, особенно у подрастающего поколения, – один из наиболее важных факторов, обеспечивающих эффективное развитие цифровой экономики. Это новое направление, требующее всестороннего изучения, является необходимым в современном мире. На настоящий момент можно рассмотреть такие виды угроз, как киберпреступления, кибербуллинг, киберсуицид, киберэкстримизм, предупредить от которых необходимость не только образовательных организаций, но и родителей. Формировать культуру необходимо различными методами, средствами и формами по любому предмету образовательной программы, а также во внеучебной деятельности.

Ключевые слова: Кибербезопасность, формирование культуры поведения в интернете, образовательный процесс, цифровое общество.

Для цитирования: Бахарев Ю. А., Гущин А. В., Прохорова М. П. Формирование культуры кибербезопасности обучающихся // Известия Балтийской государственной академии рыбопромыслового флота. – 2025. – № 3(73). – С. 165–169.

С каждым днем растет зависимость обучающихся от мобильных устройств, гаджетов, интернета вещей, систем городской среды и промышленных объектов, подключенных к облачным ресурсам. Сбор и утечка личных данных – реальность, которая диктует новые принципы цифровой безопасности всему обществу.

Уже сегодня злоумышленники могут собирать информацию или получать доступ к функциям пользовательских устройств, в том числе при помощи особого программного обеспечения, использующего «закладки» или уязвимости на аппаратном уровне.

Формирование культуры кибербезопасности – вызов общества, который требует быстрых решений и современных методик. Поскольку большинство людей тратит огромное временя в Интернете, значит сами создаем и передаем больше данных о себе и своих близких. Переданные личные данные могут быть использованы без вашего ведома, личная и финансовая информация может оказаться под угрозой.

Таким образом, как для всех организаций и для всех людей защита конфиденциальных данных имеет большое значение [2, 7].

Кибербезопасность – это деятельность, направленная на защиту систем, сетей и программ от цифровых атак. Целью кибератак обычно является получение доступа к конфиденциальной информации, ее изменение или уничтожение, вымогательство денег у пользователей или нарушение нормального бизнес-процесса.

В последнее время самым серьезным и необратимым процессом воздействия на детей и подростков стало вовлечение их в суицидальные группы, в которых романтизируется смерть, популяризируется уход из жизни и другие отрицательные воздействия, список которых постоянно растет.

Преступники воздействуют на детей и подростков не только путем прямого контакта в переписке в социальных сетях, но и предлагая посмотреть видео, фотографии, поучаствовать в обсуждении фильмов. Также детям могут предлагать определенные онлайн-книги, рекомендации по прочтению литературы и прослушиванию музыки, вовлекать их в разные игровые сообщества, виртуальные клубы по интересам в зависимости от их, вычисленных наклонностей и личностных особенностей. Тем самым преступники устанавливают круг интересов ребенка, получают данные о его личной жизни и могут влиять на его психику и поведение. Причем они будут доминировать над мнениями родителей и близких.

Не каждый взрослый понимает, чего нужно остерегаться в сети Интернет. Тем не менее, ребенок и подросток должен быть не только проинформирован о том, какие угрозы существуют, но и понимать, как их избежать в случае возникновения нестандартных ситуаций. Знакомство с такими угрозами нужно начинать уже в семье и продолжаться в школе и в профессиональных образовательных организациях.

К угрозам можно отнести:

– опасность заражения компьютера с помощью вредоносного программного обеспечения;

– беспрепятственный доступ к нежелательному, запретному контенту (содержание интернет-страниц);

– знакомство и общение с другими пользователями сети;

– афиширование конфиденциальных данных;

– осуществление неконтролируемых покупок.

Необходимо обсуждать уже в семье с ребенком все вышеперечисленные пункты, причем это должно быть не какое-то одноразовое мероприятие, а систематические беседы, которые должны стать традицией. Необходимо контролировать присутствие в сети ребенка и тем более подростков.

В ряду угроз и опасностей, подстерегающих все нас, можно выделить следующие:

– Киберпреступления (кража денег со счетов с помощью фишинговых писем или вирусов-троянов, обман, вымогательство и др.).

– Кибербуллинг (намеренные травля, оскорбления, угрозы, сообщение компрометирующих).

– Киберсуицид (групповое или индивидуальное самоубийство, согласованное при помощи интернет-ресурсов).

– Киберэкстремизм (скрытая или открытая пропаганда экстремистских взглядов в киберпространстве).

Формировать культуру кибербезопасности населения, особенно у подрастающего поколения – один из наиболее важных факторов, обеспечивающий эффективное развитие цифровой экономики. Согласимся, что это новое направление, требующее всестороннего изучения, но необходимого в современном мире.

Число пользователей Интернета с каждым днем н растет (причем самыми активными являются именно обучающиеся школ и профессиональных образовательных организаций), и становится все более актуальной проблема обеспечения информационной безопасности обучающихся в интернет-среде и формирование культуры пользования интернет-ресурсами [3,5].

В связи с этим встает вопрос об обеспечении информационной безопасности (в том числе и психологической) обучающихся при работе в Интернете. Решать этот вопрос необходимо комплексно: обучать компьютерной грамотности и в то же время формировать у них навыки соблюдения правил информационной (электронной) безопасности.

Педагог должен помочь обучающимся найти дополнительные источники через библиотечные каталоги, поисковые системы Интернета, научить их отбирать и систематизировать полученную информацию. Необходимо научить [1,6]:

– анализировать информацию с позиции общечеловеческих ценностей;

– отделять факты от субъективных мнений;

– отделять эмоции от фактов;

– рассматривать проблему с разных сторон, а не только с позиции автора;

– устанавливать взаимосвязь явлений;

– связывать разнородные объекты;

– объединять противоположности, стараясь найти дополнительные аспекты рассмотрения проблемы;

– обобщать полученную информацию и делать выводы, принимать решения; оценивать полученную информацию по совокупности проведенного анализа;

– прогнозировать последствия принятого решения.

Этому необходимо обучать в процессе познавательной деятельности по любому предмету образовательной программы, а также во внеучебной деятельности.

Для анализа представленной проблемы в рамках исследования был проведен опрос «С каким видом мошенничества вы сталкивались в сети Интернет»

В данном опросе, проведенном с помощью Google-формы, участвовали обучающиеся первого курса Нижегородских государственных образовательных организаций в возрасте 15–18 лет, в общем количестве 90 человек. Первый курс был выбран не случайно, так как данная группа обучающихся является более уязвимой и нет конкретной информации по формированию информационной культуры. Из 90 опрошенных обучающихся на вариант вопроса «Были ли вы жертвой обмана телефонных мошенников», ответили 36 % опрошенных. На вопрос «Сталкивались ли вы с взломом аккаунтов в соцсетях», ответ «да» выбрали 33 % опрошенных.

Респондентам были предложены 9 вопросов закрытого типа:

1. Были ли вы жертвой обмана телефонных мошенников?
2. Сталкивались ли вы с взломом аккаунтов в соцсетях?
3. Сталкивались ли вы с грубостью игроков во время онлайн-игры?
4. Сталкивались ли вы с обманом в Интернет-магазине?
5. Сталкивались ли вы с финансовыми пирамидами в сети?
6. Сталкивались ли вы с обучающими курсами-пустышками по подготовке к ЕГЭ?
7. Знаете ли вы, что такое искусственный интеллект?
8. Какова роль искусственного интеллекта? (Используется для кибератак, используется для отражения кибератак)
9. Что такое машинное обучение?

Результаты анкетирования приведем и проанализируем ниже. Из 90 опрошенных обучающихся на вариант вопроса «Были ли вы жертвой обмана телефонных мошенников» ответили 32 человека (36 %) опрошенных.

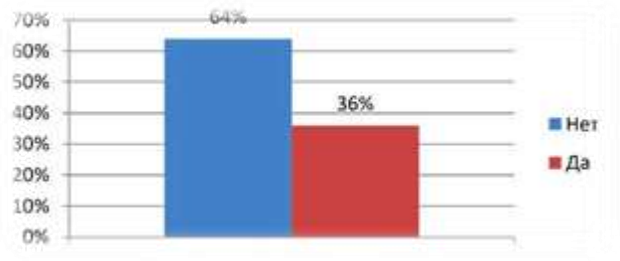

Рис. 1. Жертвы телефонных мошенников?
Вопрос «Сталкивались ли вы с взломом аккаунтов в соцсетях?»
утвердительно ответили 29 обучающихся, что составляет 32 %

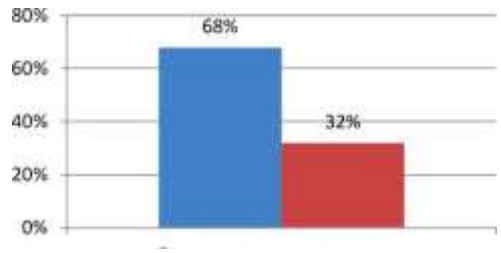

Рис. 2. Взломом аккаунтов в соцсетях
Вопрос «Сталкивались ли Вы с грубостью игроков во время онлайн-игры?»
утвердительно ответили 36 обучающихся, что составляет 40 %

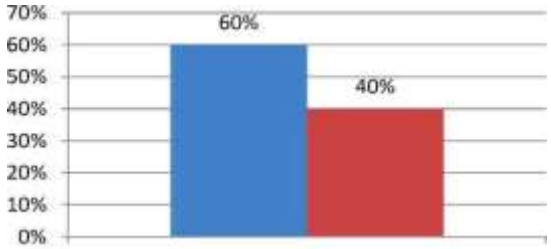

Рис. 3. Грубость игроков в онлайн-играх
Вопрос «Сталкивались ли Вы с обманом в интернет-магазинах?»
утвердительно ответили 9 обучающихся, что составляет 10 %

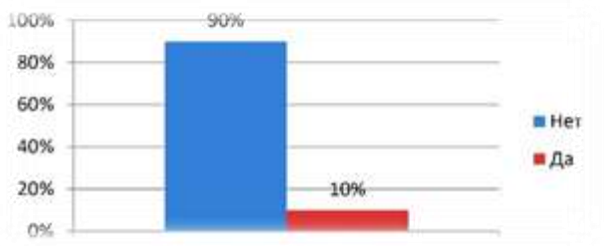

Рис. 4. Обман в Интернет-магазине
Вопрос «Сталкивались ли вы с финансовыми пирамидами?»
так же утвердительно показал 10 %, 9 обучающихся ответили положительно

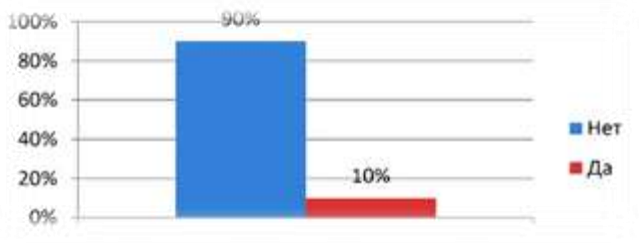

Рис. 5. Сталкивались с финансовыми пирамидами
Вопрос «Сталкивалась ли Вы с курсами «Пустышками» в процессе подготовке к ЭГЕ?»
утвердительно ответили 18 обучающихся, что составило 20 %

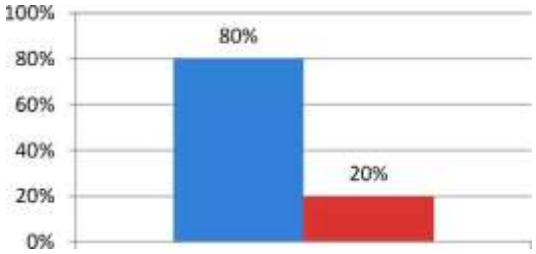

Рис. 6. Сталкивалась с курсами «Пустышками»

С каждым годом тема кибербезопасности становится все более актуальной и необходимой в современном мире. Всем, пользователям сети Интернет, требуется сформировать эффективную политику безопасности информационных технологий, быть в курсе происходящего, т. е. следить за новостями в сфере защиты информации, а также не забывать о том, что виртуальный мир, как и реальный – требует внимание к мелочам, даже к тем, который порой кажутся совсем незначительными [4, 8].

Обучать правилам безопасности необходимо не только на занятиях, но и во внеурочной деятельности, а также в семье, так как больше времени подростки проводят в сети не в учебное время.

Проведенное исследование показало, что практически каждый респондент сталкивался с теми или иными киберугрозами на просторах сети Интернет. Знаний об искусственном интеллекте и его роли в обеспечении кибербезопасности у обучающихся недостаточно. И это при том, что проводятся занятия цифровой безопасности, ежегодно обучающиеся участвуют в образовательных проектах «Урок цифры», «Цифровой диктант» и других похожих мероприятиях. Необходимо постоянно внедрять новые формы и методы формирования культуры кибербезопасности, учитывая возраст, интерес, а самое главное опыт уже имеющихся методик и практик.

Список источников

1. Булаева, М. Н. Анализ применения активных методов обучения в среднем профессиональном образовании / М. Н. Булаева, О. Н. Филатова, Е. Н. Мольков // Проблемы современного педагогического образования. – 2025. – № 86-3. – С. 53–55.

2. Гущин, А. В. Информационно-коммуникационная культура педагога как ведущий аспект перехода педагогического образования в новое качественное состояние / А. В. Гущин, О. Н. Филатова // Фундаментальные исследования. – 2014. – № 8-2. – С. 454–458.

3. Канатьев, П. В. Применение нейросетей в образовательном процессе среднего и высшего профессионального образования / П. В. Канатьев, О. Н. Филатова, С. А. Зиновьева // Проблемы современного педагогического образования. – 2024. – № 84(4). – С. 67–69.

4. Колдина, М. И., Методические рекомендации применения платформы Google в профессиональном образовании / М. И. Колдина, А. С. Лобанов, Н. В. Фролова // Проблемы современного педагогического образования. – 2024. – № 82–4.

5. Славутская, Е. В. Анализ погрешностей методов машинного обучения как основа формирования навыков их использования / Е. В. Славутская, Л. А. Славутский // Вестник Мининского Университета. – 2024. – Т. 12. – № 2.

6. Филатова, О. Н. Применение искусственного интеллекта в профессиональном образовании / О. Н. Филатова, Е. В. Лукина, М. В. Гринина // Проблемы современного педагогического образования. – 2024. – № 82-1. – С. 407–409.

7. Филатова, О. Н. Цифровые помощники профессионального обучения / О. Н. Филатова, Е. В. Барабашкина, А. А. Трифанова // Известия Балтийской государственной академии рыбопромыслового флота. – 2023. – № 4(66).

8. Щеглова, А. А. AR-технология как условие развития современного образования / А. А. Щеглова, О. Н. Филатова // Вестник Башкирского государственного педагогического университета им. М. Акмуллы. – 2023. – Т. 3. – № S1(68). – С. 10–13.

Информация об авторах

Ю. А. Бахарев – кандидат педагогических наук, профессор;
А. В. Гущин – кандидат педагогических наук, доцент;
М. П. Прохорова – кандидат педагогических наук, доцент.

Статья поступила в редакцию 14.07.2025; одобрена после рецензирования 15.08.2025; принята к публикации 22.08.2025.