DOI 10.37882/2223-2974.2023.07.12

РАЗВИТИЕ ГОТОВНОСТИ К БЕЗОПАСНОМУ ПОВЕДЕНИЮ В ЦИФРОВОЙ СРЕДЕ

DEVELOPING READINESS FOR SAFE BEHAVIOR IN THE DIGITAL ENVIRONMENT

M. Dolgachev

Summary. This article examines the issue of victim behavior among youth in the digital environment and methods of cyber victimization prevention. The research includes an analysis of theoretical concepts, a review of educational programs, and the role of social studies in predicting cyber victimization, as well as considering self-defense methods in the digital space. The authors rely on scientific literature, statistical data, and interviews with experts. In conclusion, a comprehensive analysis of modern approaches and strategies for preventing cyber victimization among youth is provided, emphasizing the importance of developing readiness for safe behavior in the digital environment.

Keywords: victim behavior, cyber victimization, safe behavior in the digital environment, prevention of cyber victimization, cybersecurity.

Долгачев Михаил Владимирович
Кандидат технических наук, доцент,
Тихоокеанский государственный университет
007428@pnu.edu.ru

Аннотация. В данной статье рассматривается проблема виктимного поведения молодёжи в цифровой среде и методы профилактики кибервиктимизации. Исследование включает анализ теоретических концепций, обзор образовательных программ и роли социальных исследований в прогнозировании кибервиктимизации, а также рассмотрение методов самозащиты в цифровом пространстве. Авторы опираются на научную литературу, статистические данные и интервью с экспертами. В итоге предоставлен обширный анализ современных подходов и стратегий профилактики кибервиктимизации молодёжи, подчёркнута важность развития готовности к безопасному поведению в цифровой среде.

Ключевые слова: виктимное поведение, кибервиктимизация, безопасное поведение в цифровой среде, профилактика кибервиктимизации, кибербезопасность.

Проблема виктимного поведения молодёжи и его негативных последствий в современном обществе является актуальной и требует серьёзного исследования. В нашей работе мы ставим перед собой цель изучить механизмы профилактики кибервиктимизации и развития готовности к безопасному поведению в цифровой среде. Наше исследование предназначено для более глубокого понимания проблемы кибервиктимизации, а также для определения методов и стратегий по её предотвращению.

Исследование охватывает следующие ключевые области:

- изучение теоретических концепций безопасного поведения в цифровой среде и психологической готовности к нему;
- анализ существующих образовательных программ и тренингов, направленных на профилактику кибервиктимизации;
- оценка роли социальных исследований в прогнозировании и предотвращении кибервиктимизации;
- рассмотрение методов самозащиты и саморегуляции в цифровом пространстве.

Мы стремимся дать общее представление о современных подходах и тенденциях в профилактике кибервиктимизации и развитии безопасного поведения в цифровой среде. В то же время, мы признаем, что область кибербезопасности быстро развивается, и, хотя наше исследование охватывает большую часть этой области, оно не претендует на исчерпывающую полноту. В нашем исследовании мы опираемся на научную литературу, отчёты по происшествиям, статистические данные и интервью со специалистами в области кибербезопасности.

Психологические предпосылки кибервиктимизации

Кибервиктимизация представляет собой процесс, когда индивидуум или группа лиц становятся жертвами преступления, использующего цифровые технологии и интернет-коммуникации. Целью могут быть кража средств, информации, шантаж, запугивание или унижение. Исследование судебных дел показывает, что многие люди, будь то преступники или жертвы, не полностью осознают меру своей ответственности, несмотря на прохождение обучения, включающего знакомство с правилами неразглашения коммерческой тайны или персональных данных клиентов.

Возьмём, к примеру, случай с сотрудниками мобильного оператора, которые устроили преступный сговор. Имея доступ к системе SBMS, они создали дополнительные сим-карты для клиентов, с которых затем переводили деньги на фальшивые банковские карты через сервисы Киви кошелёк и Яндекс.Деньги, после чего обналичивали их. В Саратовской области продавец мобильных телефонов незаконно активировал ПО SBMS, скопировав сертификат доступа.

Или рассмотрим случай из Ижевска, где местный житель, сговорившись с неким лицом из интернета, попы-

тался украсть деньги из банкомата. Он был осуждён на 4 года условно. В Астрахани служащий, используя своё служебное положение, передал информацию о телефонных разговорах абонента третьим лицам.

Нерегулированные трудовые отношения в Казани, сопряжённые со свободным доступом к компьютеру и личной антагонией, привели к разрушению базы данных клиентов и научных разработок для диссертации. Тем временем в Саранске, бывшая сотрудница попросила менеджера пообещать ей вознаграждение за передачу данных о клиентах. Житель Югры модифицировал телевизионный пакет «Ростелекома» для просмотра каналов без дополнительной платы, а затем рекламировал его [1–5].

Проанализировав эти преступления, мы сможем более точно определить профиль преступника и его жертвы.

1. Недостаток цифровой грамотности может привести к безрассудному поведению, включая загрузку подозрительного ПО, переход по неизвестным ссылкам, оставление учётных данных на неизвестных сайтах, распространение фальшивых сообщений, игнорирование настроек конфиденциальности в соцсетях, а также бездумное распространение своих фотографий, мыслей и чувств.
2. Импульсивность и низкий уровень эмоционального контроля ухудшают критическое мышление. Люди принимают решения, опираясь на быстрое, эмоциональное мышление, искажающее реальность. Это включает в себя тенденцию к необдуманным выводам, катастрофизации, сверхобобщению и другим мыслительным ловушкам, известным в когнитивной психологии. Эти ошибки обычно возникают из-за глубоко укоренённых убеждений о самом себе, об окружающем мире и своём месте в нем, включая негативное самовосприятие.
3. Человек с низкой самооценкой, находясь в состоянии неуверенности или перед лицом угрозы, может испытывать стресс и тревогу. Это, в свою очередь, отключает рациональное мышление, приводя к некорректным решениям, недооценке серьёзности риска или к избеганию проблемы, основанного на предположении, что справиться с ней не по силам. Такие индивиды часто сознательно или несознательно отказываются от признания угрозы или противостоят предложенным профилактическим мерам, таким как улучшение самооценки или киберграмотности. Идеальным решением в рамках обучающих мероприятий по информационной безопасности является достижение осознания людьми глубины риска и их способности принимать необходимые действия для контроля над угрозой.
4. Низкий уровень жизненного удовлетворения, например, отсутствие дружеских отношений, проблемы в общении, одиночество, сопровождающийся негативными эмоциями, может вести к повышению уровня тревоги и депрессии. Известно, что такие люди проводят больше времени онлайн из-за страха пропустить что-то важное или интересное, что называется синдромом упущенной выгоды. Они часто активно обновляют свои социальные сети, непрерывно проверяют свои аккаунты, пытаясь постоянно находиться в сети.
5. Продолжительное время, проведённое в интернете, увеличивает риск стать жертвой киберпреступления. Учёные выяснили, что чем больше время человек проводит в сети, тем больше он подвержен мошенничеству со стороны злоумышленников, которые используют ботов для распространения мошеннических сообщений, всплывающих окон и ложной информации. Боты — это автоматизированные аккаунты, которые проводят мониторинг и выполняют автоматические действия, такие как лайки и посты. Они также могут отправлять фишинговые письма, ссылки на поддельные сайты случайным пользователям. Это объясняет почему пребывание в сети увеличивает вероятность столкнуться с мошенничеством.
6. Согласно некоторым данным, примерно 51,8 % всего интернет-трафика генерируется ботами, среди которых есть как «благожелательные» боты, предназначенные для управления базами данных крупных компаний и знаменитостей, так и те, что распространяют ложные новости. Опасность этих последних заключается в том, что многие люди считают ботов достоверным источником информации, что, в свою очередь, увеличивает распространение фейковых новостей. Исследования подтверждают, что пользователи, которые часто используют отрицательные выражения, более подвержены влиянию получаемых от ботов сообщений.

Учёные из Италии разработали методику, позволяющую с точностью 93,27 % определить пользователей, имеющих «друзей-ботов» в социальных сетях, поскольку именно они являются главными распространителями фейковых новостей в своём социальном окружении. Это представляет собой серьёзную угрозу для социальной стабильности и искусственно увеличивает уровень неопределённости.

Для того чтобы понять масштабы проблемы кибервиктимизации, важно рассмотреть статистические данные.

Согласно отчёту Norton Cyber Safety Insights Report за 2021 год, около 330 миллионов человек по всему миру

стали жертвами киберпреступлений, что свидетельствует о глобальной значимости этой проблемы.

По данным Pew Research Center, в США около 59% подростков сталкивались с некоторой формой кибердомогательства, включая оскорбительные сообщения, намеренное распространение ложной информации или угрозы.

Ещё один исследовательский центр, EU Kids Online, показал, что в Европе 12% детей в возрасте от 9 до 16 лет сталкивались с кибердомогательством.

Также стоит отметить, что кибервиктимизация может принимать различные формы, включая кибердомогательство, кибersталкинг, фишинг и другие. По данным отчёта Verizon's Data Breach Investigations Report, фишинг является одной из наиболее распространённых форм кибератак.

Развитие готовности обучающихся к безопасному поведению в виртуальном мире

Важнейшим психолого-педагогическим условием безопасной жизнедеятельности молодёжи и студентов в цифровой среде является развитие готовности обучающихся к безопасному поведению в виртуальном мире, которая включает: развитие знаний о информационно-коммуникационных технологиях (ИКТ) и связанных с ними угроз, формирование навыков безопасного поведения в виртуальной среде, а также осознание ответственности за использование различных средств и методов для соблюдения правил безопасности.

Для формирования и развития этой готовности к безопасному поведению в виртуальном мире необходимо рассмотреть два основных подхода: создание условий для безопасного использования ресурсов виртуальной среды в процессе обучения и развитие навыков безопасного поведения в виртуальной среде. Исследование каждого из этих направлений является важным этапом в обучении безопасности в цифровой среде.

Проанализируем каждое из названных направлений формирования и развития готовности обучающихся к безопасному поведению.

Для безопасного взаимодействия в виртуальной среде пользователю необходимо активно выполнять несколько основных действий. Эти действия включают ограничение доступа, особенно для молодых пользователей, к негативному контенту, а также минимизацию угрозы заражения компьютера и других устройств, используемых для подключения к интернету, вредоносным ПО.

При рассмотрении ограничения доступа к негативной информации следует отметить, что глобальная практика фильтрации контента в интернете обширна и многообразна. Например, в Саудовской Аравии система фильтрации явно изложена на официальном веб-сайте, где объясняется причины блокировки конкретных материалов. В Китае используется более скрытый подход к фильтрации, часто замаскированный под техническую ошибку, тогда как во Франции блокируются сайты, которые могут способствовать разжиганию межэтнического и религиозного конфликта.

Существуют три основные модели блокировки доступа к сайтам: сетевая, инфраструктурная и блокировка подключения пользователя. Исследователи выделяют URL-блокировку с предварительной сортировкой запросов по IP-адресам как наиболее быструю, экономичную и минимизирующую негативные последствия. Однако, стоит учесть, что блокировка потенциально опасного контента часто имеет запаздывающий характер, поскольку сайт с негативным содержимым должен существовать и активно посещаться некоторое время перед тем, как будет признан информационно опасным.

Сайты, считающиеся вредоносными для несовершеннолетних, включают в себя контент, который глорифицирует физическое и психологическое насилие, сексуальные действия, наркоманию, курение, алкоголизм, нездоровый образ жизни, самоубийство, участие в азартных играх и лотереях, сексуальную распущенность, демонстрацию гипноза и паранормальных явлений, а также компьютерные игры, провоцирующие агрессию. В статье 14 Федерального закона Российской Федерации от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» сказано, что «…доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети интернет, в местах, доступных для детей, предоставляется…при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию».

Улучшение безопасности в образовательных процессах может быть достигнуто через использование специализированного программного обеспечения, которое способствует фильтрации и блокировке определённых сайтов. Такой подход позволяет ограничивать доступ учащихся к неподходящему контенту, либо предотвращать случайные визиты на такие ресурсы.

Программы этого типа предоставляют возможность настройки, которая ограничивает доступ пользователей к утверждённым веб-ресурсам. ИТ-специалисты и методисты могут подсказать, какие веб-страницы нуждаются

в блокировке в контексте образовательного процесса. Дополнительно, регулярный аудит применяемых ресурсов поможет выявить нежелательный контент и определить, требуется ли дополнительная фильтрация или блокировка.

Создание безопасной цифровой среды в учебных заведениях предполагает обязательное использование фильтрующего ПО и механизмов блокировки вредоносных сайтов. Настройка и конфигурация таких технических средств должны гарантировать разделение пользовательских прав доступа к выбору и настройкам режимов работы фильтров, исключая возможность несанкционированного отключения.

С целью минимизации рисков, связанных с «заражением» компьютеров вредоносными программами, следует использовать комплексные программы защиты. Несмотря на то, что общепринятым термином для обозначения таких программ является «антивирус», эта защита охватывает больше, чем только вирусы.

В современном цифровом мире ежедневно появляется несколько сот тысяч новых вредоносных программ, включая вирусы, трояны, черви и т.д. Их хитроумность и разнообразие таковы, что даже опытные пользователи могут стать жертвами. Для противостояния этой угрозе, комплексные защитные программы обновляются в режиме реального времени, предоставляя надёжную защиту от большинства интернет-угроз.

Формирование и развитие навыков безопасного поведения в виртуальной среде

Цифровая безопасность требует не только разработки и внедрения стратегий и технологий для преодоления потенциальных угроз, но и культивирования индивидуальных ресурсов, способных предотвращать возникновение высокорисковых ситуаций.

Ключевые аспекты готовности к безопасному поведению в цифровом пространстве включают:

1. Устойчивые знания о цифровых угрозах и способах их минимизации.
2. Разработанные стратегии для минимизации онлайн-угроз. Это подразумевает способность адекватно оценивать уровень опасности, анализировать доступные внутренние и внешние ресурсы для преодоления угрозы, а также выбирать правильные стратегии и технологии поведения. Кроме того, это включает готовность привлечь дополнительные ресурсы при необходимости, выполнить нужные действия, и принять ответственность за последствия своих действий.
3. Развитие личных навыков и ресурсов, которые могут помочь преодолеть сложные ситуации. Сюда входит ответственность, критическое мышление, умение просить и принимать помощь, а также стрессоустойчивость.

Поддержание безопасности в цифровой среде требует от пользователей не только знания информационно-коммуникационных технологий и использование инструментов для защиты своего онлайн-пространства, но и активное и ответственное поведение в виртуальном мире, а также соблюдение правил безопасного взаимодействия в нем.

Анализ безопасного поведения в цифровом мире позволяет определить критерии и показатели готовности к безопасной деятельности в цифровой среде:

1. Когнитивный критерий: знания о способах безопасного поведения в цифровой среде, активность в обучении, аналитическое мышление.
2. Мотивационно-потребностный критерий: стремление и желание обеспечивать личную и общественную безопасность, внутренняя мотивация к саморазвитию в области цифровой безопасности.
3. Деятельностно-практический критерий: навыки и способности, необходимые для безопасного поведения в цифровом мире, устойчивость к стрессу, способность реализовать безопасные действия в цифровой среде.
4. Творческий критерий: способность к нестандартному мышлению и поиску новых решений в цифровой среде.

Далее представлены некоторые известные программы, которые направлены на предотвращение и вмешательство в виктимное поведение молодых людей в сети Интернет [6]:

1. Проект «TABBY вИнтернете» (Athanasiades, Kamariotis, Psalti, Baldry и Sorrentino, 2015) предлагает школьникам просмотреть четыре видеоролика, посвящённых различным формам киберзапугивания. Затем происходит обсуждение фильмов, выявление негативных последствий киберзапугивания и разработка правил ответственного поведения в Интернете. Также в рамках программы изучаются технологии борьбы с кибержертвами.
2. Программа WebQuest (Lee, Zi-Pei, Svanström, Dalal, 2013) представлена в виде Web-страницы и состоит из шести блоков, включая введение, задачи, процесс, ресурсы, оценки и выводы. Программа включает в себя восемь занятий, на которых учащиеся работают в группах, решают проблемные ситуации и выполняют учебные задачи.
3. ViSC (Gradinger, Yanagida, Strohmeier, Spiel, 2014; Yanagida, Strohmeier, 2016) предусматривает коррекционную работу с индивидуальными школьниками, проявляющими виктимное поведение.

Школьники обучаются распознавать и управлять своими эмоциями, развивают позитивные стратегии справления с негативными эмоциями и получают информацию о том, как избежать становления жертвой в школьной среде. Обучение осуществляется с использованием различных методов, таких как ролевые игры, работа в малых группах и классные дискуссии.

4. Программа антииздевательств KiVa (Williford, Elledge, Boulton, DePaolis, Little, Salmivalli, 2014) включает два основных компонента: универсальные действия и индивидуальные действия. Универсальные действия включают уроки в классе, направленные на повышение осознания роли группы в поддержке издевательств, развитие сочувствия к жертвам и формирование стратегий поддержки жертвы для повышения самоэффективности. Программа также включает уроки, посвящённые профилактике киберзапугивания, обсуждению вопросов вежливого и корректного поведения в онлайн-коммуникации и развитию конкретных способов реагирования на киберзапугивание учащихся.

Эти программы разработаны для предотвращения и устранения виктимного поведения в Интернете среди молодёжи. Они предлагают различные подходы, такие как образовательные видеоролики, групповая работа, коррекционные методы и уроки в классе, чтобы научить учащихся осознавать последствия своих действий в сети, развивать навыки эмоционального управления и находить позитивные способы взаимодействия в онлайн-среде.

Заключение

Проблема безопасности в использовании Интернета и информационных технологий является актуальной и значимой в современном обществе. Работа в этой области ведётся как в России, так и за рубежом. Однако стоит отметить, что большинство исследований посвящены проблемам безопасности в интернете среди детей школьного возраста, в то время как изучение этой проблемы среди более старших возрастных групп остаётся недостаточным. Отдельные исследования затрагивают вопросы безопасности среди студентов, однако их доля остаётся небольшой.

Анализ зарубежной и отечественной литературы выявил три основных направления, в которых исследуются проблемы безопасности в использовании Интернета. Первое направление связано с изучением личностных особенностей и социально-психологических факторов, влияющих на поведение жертв виктимизации. Второе направление посвящено выявлению факторов, причин и видов рисков кибервиктимизации. Третье направление связано с разработкой и предоставлением адресной помощи различным категориям жертв виктимизации.

Необходимо отметить, что данная область исследования продолжает развиваться, и важно продолжать исследования с целью повышения безопасности в сети. Результаты и выводы наших исследований могут быть полезны для специалистов в области психологии, социологии и информационной безопасности, а также для формирования рекомендаций и разработки мер по предотвращению и уменьшению угроз в сфере онлайн-взаимодействия.

ЛИТЕРАТУРА

1. Воробьева, К.И. Психология кибербезопасности: учебное пособие / К.И. Воробьева, М.В. Долгачев; научный редактор Т.Х. Невструева; Министерство науки и высшего образования Российской Федерации, Тихоокеанский государственный университет. — Хабаровск: Издательство ТОГУ, 2022. — 117, [1] с.
2. Баева, И.А. Тренинги психологической безопасности в школе / И.А. Баева. — СПб.: Речь, 2002. — 251 с.
3. Бакулина, А.С. Пленники всемирной сети, компьютерная зависимость у детей и молодежи и социальные инновации в области ее профилактики / А.С. Бакулина // Социально-психологические аспекты практики социальной работы: сб. науч. ст. / ред.-сост. Т.Н. Дорошенко. — М., 2016. — С. 208–219.
4. Наширванова, Р.Р. Психологические аспекты селфи / Р.Р. Наушир— ванова, Е.В. Ахмадеева // Современные научные исследования и инновации— 2016. — № 1.
5. Шарипова, Г.Р. Профилактика селфи-зависимости у младших подростков / Г.Р. Шарипова, А.Р. Дроздикова-Зарипова // Международный студенческий научный вестник. — 2016. — № 5 (часть 1).
6. Калацкая Н.Н., Биктагирова Г.Ф., Валеева Р.А., Дроздикова-Зарипова А.Р., Костюнина Н.Ю. Зарубежный и отечественный опыт профилактики виктимного поведения учащейся молодежи в сети интернет // Современные проблемы науки и образования. — 2021. — № 3.
7. Жмуров Д.В. Кибервиктимизация: оценка последствий / Д.В. Жмуров. — DOI 10.17150/2411-6122.2023.1.5-13. — EDN RABUNM // Сибирские уголовно-процессуальные и криминалистические чтения. — 2023. — № 1. — С. 5–13.

Журнал «Современная наука: актуальные проблемы теории и практики»