ФОРМИРОВАНИЕ В РАННЕМ ПОДРОСТКОВОМ ВОЗРАСТЕ ГОТОВНОСТИ К ОБЕСПЕЧЕНИЮ ЛИЧНОЙ КИБЕРБЕЗОПАСНОСТИ

Е. В. Чернова[1], **А. С. Доколин**[2], **И. В. Гаврилова**[1]

[1] ***Магнитогорский государственный технический университет им. Г. И. Носова***
455000, Россия, Челябинская область, г. Магнитогорск, пр-т Ленина, д. 38

[2] ***МОУ СОШ № 28, г. Магнитогорск***
455038, Россия, Челябинская область, г. Магнитогорск, пр-т К. Маркса, д. 141/4

Аннотация

Современный этап развития образования в России характеризуется ранним включением детей и подростков в информационное пространство, противостоять негативному информационному воздействию которого они зачастую не готовы. Несмотря на то что формирование личности, способной обеспечить устойчивость к киберугрозам, — актуальная потребность школьного образования, активно вовлекающего школьника в цифровую информационную среду, на текущий момент наблюдается недостаток эффективных педагогических средств решения данной проблемы. В данной статье описан эксперимент по формированию у школьников младшего подросткового возраста готовности к обеспечению личной кибербезопасности на основе разработанной авторами методики, затрагивающей преимущественно внеучебную деятельность подростков. Результаты эксперимента подтвердили эффективность разработанных педагогических средств решения исследуемой проблемы. Таким образом, авторам удалось создать методику, которую можно рекомендовать для работы со школьниками раннего подросткового возраста, аналогов которой не существует.

Ключевые слова: ИКТ, информационная безопасность, кибербезопасность, киберугрозы, обеспечение личной кибербезопасности, девиантное поведение, ранний подростковый возраст.

DOI: 10.32517/0234-0453-2018-33-7-16-26

Для цитирования:

Чернова Е. В., Доколин А. С., Гаврилова И. В. Формирование в раннем подростковом возрасте готовности к обеспечению личной кибербезопасности // Информатика и образование. 2018. № 7. С. 16–26.

Статья поступила в редакцию: 31 июля 2018 года.

Статья принята к печати: 20 августа 2018 года.

Сведения об авторах

Чернова Елена Владимировна, канд. пед. наук, доцент, доцент кафедры бизнес-информатики и информационных технологий Магнитогорского государственного технического университета им. Г. И. Носова; HelenaVChernova@gmail.com

Доколин Андрей Сергеевич, канд. пед. наук, учитель информатики МОУ СОШ № 28, г. Магнитогорск; a.dokolin@gmail.com

Гаврилова Ирина Викторовна, канд. пед. наук, доцент, доцент кафедры бизнес-информатики и информационных технологий Магнитогорского государственного технического университета им. Г. И. Носова; Irina.V.Gavrilova@yandex.ru

Введение

Стремительно ускоряющиеся темпы развития информационно-коммуникативных технологий, вовлеченность подростков и молодежи в информационное пространство, информатизация образования, внедрение в процесс обучения высокотехнологичного инструментария не только приводят к положительным результатам, но и зачастую порождают девиации поведения школьников в ИКТ-среде. Не только подростки считают необязательным соблюдение общественно-правовых норм в информационной среде — многие взрослые демонстрируют девиантное поведение в интернете, превращая такое поведение в образец для подражания, привлекательный из-за сопровождающей его популярности. К сожалению, подростки не осознают в полной мере, что любые действия как в реальном, так и в виртуальном мире имеют отдаленные последствия. В современном информационном пространстве достаточно много угроз, направленных на подростков, которые пока не способны критически осмысливать получаемую информацию, не обладают богатым жизненным опытом, отличаются максимализмом, активной жизненной позицией и поэтому особенно уязвимы. Мошенники различного уровня, сектанты-проповедники, активисты всевозможных движений (политических, религиозных, социальных и др.), психически больные люди, преступники — малая часть пользователей, окружающих подростка и завлекающих его в свой мир. Самый частый вопрос, который получают преподаватели, проводящие беседы и мастер-классы по обеспечению безопасности личной информации в ИКТ-среде, — технология взлома аккаунта в социальной сети, ящика электронной почты или мобильного устройства. Дети и подростки не осознают реальных угроз интернета, его связи с реальными законами и нормами общества, и современный курс информатики не может в полной мере подготовить их к пониманию этого. В апреле 2017 года на слушаниях в Совете Федерации министр образования России О. Ю. Васильева отметила необходимость обучения ребенка основам кибербезопасности буквально с дошкольного возраста, материалы по безопасности в информационной среде должны изучаться не только в курсе информатики, но и вне занятий.

Неготовность подростков к обеспечению личной кибербезопасности способствует возникновению у них под воздействием различных киберугроз девиантного поведения в сфере ИКТ, от которого может пострадать не только сам подросток, но и его ближайшее окружение, а также все те, с кем он может контактировать. При этом следует отметить отсутствие педагогических средств диагностики для выявления детей с отклонениями в поведении в среде ИКТ. Самый известный тест на выявление интернет-зависимости авторства К. Янг был разработан в 1994 году, и в 2004 году В. А. Лоскутова перевела его на русский язык и адаптировала к современным условиям [1]. Еще менее известны методики российских ученых А. Е. Жичкиной и Е. А. Щепилиной [2]. В России проблемой негативного воздействия ИКТ на личность в разное время занимались также О. Н. Арестова, Ю. Д. Бабаева, А. Е. Войскунский, М. С. Иванов, Г. Н. Чусавитина, Е. А. Щепилина и др. Однако до сих пор не разработан стандартизованный диагностический инструментарий, позволяющий педагогам, психологам и родителям своевременно отслеживать поведенческие изменения в среде ИКТ у подростков. В своей работе мы опирались на разработанный нами набор средств диагностики девиантного поведения школьников в сфере ИКТ.

Киберугрозы личности подростка

Согласно терминологии ЮНФПА — Фонда ООН Организации в области народонаселения, подростки — это лица в возрасте 10–19 лет, при этом ранним подростковым возрастом считается период с 10 до 14 лет. Как правило, в это время человек активно перенимает знания и умения в рамках обучения в каком-либо образовательном учреждении (школе, гимназии и т. п.). В настоящее время процесс школьного образования неминуемо вовлекает подростка в активное использование информационно-коммуникативных технологий. Анализ современного состояния проблемы обеспечения кибербезопасности школьника позволил нам выделить следующие **разновидности угроз ИКТ-среды** [3]:

- нежелательная информация;
- агрессивное информационное пространство;
- манипуляции и пропаганда;
- девиантное поведение в среде ИКТ;
- киберпреступления.

Дадим краткий анализ данным явлениям.

Сейчас в законодательстве отсутствует четкое определение понятия ***«нежелательная информация»***, поэтому под ней будем понимать:

1) информацию, не запрашиваемую пользователем;
2) информацию, наносящую вред здоровью и психике;
3) иную информацию, за распространение которой предусмотрена уголовная или административная ответственность.

Критерии отнесения информации к нежелательной сформулированы в Конституции РФ, законах «Об информации, информационных технологиях и о защите информации», «О государственной тайне», «О средствах массовой информации», Доктрине информационной безопасности, Уголовном кодексе РФ и законе «О защите детей от информации, причиняющей вред их здоровью и развитию» [4–7].

Агрессивное информационное пространство включает в себя все случаи проявления агрессии либо провоцирующих действий в отношении подростка для вызова у него агрессии. Оно может проявляться в форме:

- межличностной агрессии в процессе общения;
- агрессии личности относительно информационных ресурсов;
- компьютерных игр с насилием, способных побудить детей к агрессии в реальном мире;
- агрессивной подачи информации (реклама, пропаганда).

Цель ***манипуляций и пропаганды*** — заставить подростка выполнить необходимое для манипулятора действие: передать информацию, совершить деяние, непристойные действия. Подростков вовлекают в политические движения, псевдонаучные группы, навязывают асоциальный и делинквентный образ жизни, выманивают пожертвования и многое другое.

Девиантное поведение в сфере ИКТ — «вид девиантного поведения индивида (группы индивидов), представляющий систему поступков (или отдельные поступки), опосредованных применением ИКТ (либо направленных в отношении ИКТ), причиняющую ущерб (моральный, физический, экономический и иной) обществу, организациям, частным лицам или самой личности» [8]. Девиации поведения в ИКТ-среде могут проявляться различным образом, наиболее известны [9]:

- зависимость от компьютера (интернет-аддикция) и компьютерных игр (геймерство);
- раннее вовлечение в виртуальный секс;
- асоциальное поведение.

Проведенное нами исследование позволило выделить **четыре основных типа девиантного поведения в сфере ИКТ** (рис. 1) [8, 10]:

- асоциальное поведение;
- делинквентное поведение;
- аддиктивное поведение;
- гиперспособности в сфере ИКТ.

Дадим краткую характеристику каждому виду девиантного поведения в сфере ИКТ.

Асоциальное поведение в сфере ИКТ — «поведение, противоречащее общественным нормам и принципам, выступающее в форме безнравственных или противоправных деяний, совершаемых с использованием ИКТ» [11]. «Асоциальный — значит, почти граничащий с антисоциальным. Проявляется асоциальное поведение в широких пределах — от легких, незначительных нарушений правил поведения до противоправных действий, вызванных глубокой моральной запущенностью» [12]. Незрелость подростка, как личностная, так и физиологическая, очень часто проявляется в виде асоциального поведения, и информационно-коммуникативные технологии являются средой и инструментом, с помощью которых подросток может хулиганить, так как считает, что в виртуальном мире требования общества соблюдать не обязательно и можно не опасаться наказания за свои выходки [13].

Делинквентное (антисоциальное) поведение в сфере ИКТ — «отклоняющееся поведение, представляющее собой проступок либо уголовно

Рис. 1. Классификация видов девиантного поведения в сфере ИКТ

наказуемое деяние, совершенное посредством либо в сфере ИКТ, влекущее за собой получение выгоды и/или нанесение материального, психологического, информационного вреда жертве» [8].

Аддиктивное поведение в сфере ИКТ — «одна из форм девиантного поведения с формированием стремления к уходу от реальности путем постоянной фиксации внимания на определенных видах деятельности, опосредованных ИКТ» [8]. В. Д. Менделевич отмечает, что «основным мотивом личностей, склонных к аддиктивным формам поведения, является активное изменение не удовлетворяющего их психического состояния, которое рассматривается как “серое”, “скучное”, “монотонное”, “апатичное”» [14]. Вследствие этого подростку сложно в реальности найти такие занятия, которые могли бы увлечь его, удержать внимание или эмоционально привлечь. Для подростка жизнь становится насыщенной только в той виртуальной реальности, которую он для себя настроил. «Аддиктивное поведение связано с желанием человека уйти из реальной жизни путем изменения состояния своего сознания» [15]. Психологи выделяют два варианта развития зависимости: зависимость от компьютера или интернета и зависимость от компьютерных игр (геймерство).

Особо стоит отметить такой вид девиантного поведения, как ***гиперспособности в сфере ИКТ***. Как считает К. К. Платонов, «одаренный человек часто неприспособлен к “бытовой” жизни, неспособен к правильной оценке поступков и поведения других людей, живет в своей реальности. Весь интерес такого индивидуума сосредоточен на деятельности, связанной с его способностями, он не принимает активного участия во взаимодействии с окружающим миром» [16]. В целом феномен гиперспособностей в области информационно-коммуникативных технологий на данный момент слабо изучен, однако подростки, обладающие гиперспособностями в сфере ИКТ, должны вовлекаться в реальную жизнь, а не быть зацикленными только на своих успехах и достижениях.

Киберпреступления — это преступления, совершенные в информационном пространстве либо с применением информационных технологий. Исследователи выделяют следующие основные виды киберпреступлений:

- распространение порочащей информации (диффамация);
- киберпреступления;
- кибертерроризм;
- киберэкстремизм;
- киберсуицид.

Среди них наиболее частое и разрушительное воздействие на личность подростка оказывают киберэкстремизм и киберсуицид.

Киберэкстремизм — «деятельность экстремистов, связанная с реализацией системы мер, сосредоточенных против существующих в обществах норм, правил, принципов, обычаев и традиций, с применением информационных технологий» [17]. В современном виртуальном пространстве наблюдается активизация экстремистских и террористических групп, вовлекающих в свою деятельность подростков и молодых людей.

Киберсуицид — разновидность группового или индивидуального самоубийства, совершаемого в результате общения с использованием интернет-ресурсов [18]. В 2016–2017 годах по России прокатилась волна подростковых самоубийств, катализатором которых выступали так называемые «группы смерти», целью которых была провокация подростка на суицид путем различных психологических манипуляций.

Следует отметить, что киберпреступления здесь отмечены дважды: и как пример девиантного поведения подростков, и как активное действие, направленное против личности подростка.

Данная классификация не претендует на полноту и достаточность, мы обозначили наиболее явные и острые явления в информационной среде общества на сегодняшний день, которые выявляют проблему формирования у подростков готовности к негативным информационным воздействиям.

Понятие готовности к обеспечению личной кибербезопасности

Готовность личности к обеспечению собственной кибербезопасности, проявляющаяся, прежде всего, в противодействии негативному информационному воздействию, неразрывно связана с понятием **психологической устойчивости**, которое в последнее время является предметом пристального внимания ученых-психологов, отмечающих усиливающееся отрицательное влияние информационно-коммуникационных технологий на развитие личности. Так, в работе С. П. Ивановой [19] приводится всестороннее изучение понятия «устойчивость личности» в трудах отечественных и зарубежных исследователей, на основании которого формируется вывод о трех важных составляющих:

- стойкости — способности сохранять себя в изменяющихся условиях;
- уравновешенности — соразмерности силы и активности ответной реакции уровню и значению воздействующего фактора;
- сопротивляемости — способности противостоять всем факторам, способным ограничить свободу личности в принятии решений и аксиологическом выборе.

В том или ином виде все они должны быть присущи личности, готовой к жизни в агрессивном информационном пространстве.

Под **готовностью к обеспечению личной кибербезопасности** будем понимать сложное образование, сочетающее в себе три компонента: рационально-познавательный, поведенческий и рефлексивный.

Рационально-познавательный компонент характеризуется уровнем информированности и знаний методов и средств противодействия негативному информационному воздействию.

Поведенческий компонент характеризуется готовностью подростков к активному личному противостоянию киберугрозам, обеспечивающей информационную безопасность личности в ситуациях фрустрирующего и стрессогенного воздействия.

Рефлексивный компонент характеризуется способностью осознать и адекватно описать свое эмоциональное состояние и причины его изменения, а также способностью удерживать свое психологическое состояние в равновесии [20].

Наиболее активными и неопытными пользователями в информационном пространстве являются подростки среднего школьного звена (11–15 лет), что обусловливается процессом взросления, попытками выйти из-под контроля взрослых, проявить свои таланты и возможности, раскрыть личностный потенциал [21]. Подростковый максимализм данного возраста не позволяет школьникам вовремя заметить угрожающие процессы, направленные на них, попытки взрослых взять деятельность подростка в ИКТ-среде под контроль вызывают отторжение и конфликты. Поэтому цель педагога, работающего в среднем звене, — обучить подростка основам безопасного взаимодействия с киберсредой, навыкам обеспечения личной безопасности, защиты собственной информации.

Анализ содержания подготовки подростков показал, что в рамках предметной подготовки обеспечить системное формирование готовности к обеспечению личной кибербезопасности не представляется возможным. По этой причине **целесообразно перенести занятия во внеурочную деятельность.**

Внеурочная деятельность — это «организуемая участниками образовательного процесса деятельностная организация на основе вариативной составляющей базисного учебного (образовательного) плана, отличная от урочной системы обучения: экскурсии, кружки, секции, “круглые столы”, конференции, диспуты, КВНы, школьные научные общества, олимпиады, соревнования, поисковые и научные исследования и т. д., а также занятия по направлениям внеучебной деятельности учащихся, позволяющие в полной мере реализовать требования Федеральных государственных образовательных стандартов общего образования» [7].

Особое внимание уделяется **диагностике девиантного поведения подростков в сфере ИКТ**, так как носитель подобного поведения сам по себе представляет угрозу для остальных учащихся и, следовательно, требует иного подхода к воспитанию. Диагностика девиантного поведения в сфере ИКТ позволяет педагогу выявлять индивидуальные особенности и потенциальные возможности школьника в сфере ИКТ, устанавливать особенности класса и благодаря этому научно обоснованно управлять учебно-воспитательным процессом.

Опытно-экспериментальная работа по формированию готовности к обеспечению личной кибербезопасности

Опытно-экспериментальная работа по оценке эффективности методики формирования готовности к обеспечению личной кибербезопасности осуществлялась в **три этапа**.

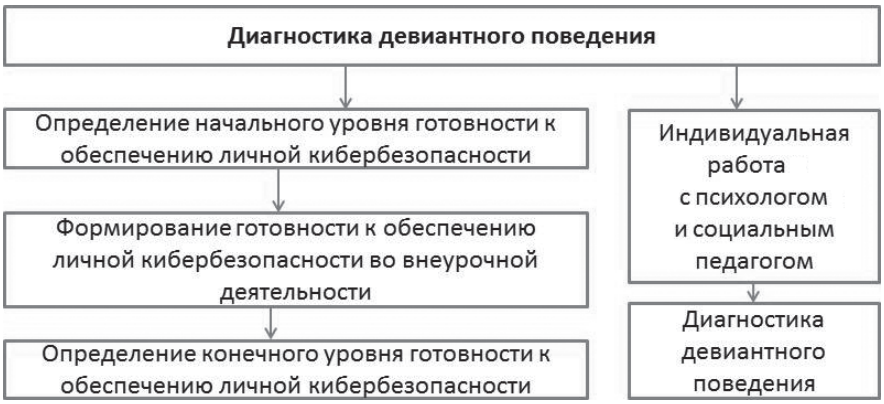

Рис. 2. Схема ежегодного обследования подростков

На первом этапе были разработаны методические материалы, критериально-оценочный инструментарий, определена экспериментальная площадка. В общей сложности в эксперименте приняли участие более 300 школьников раннего подросткового возраста, обучающихся в образовательных учреждениях г. Магнитогорска и близлежащих населенных пунктов.

Второй этап работы осуществлялся с 2015 по 2018 год в форме лонгитюдного исследования по схеме, представленной на рисунке 2. Обследование школьников проводилось в соответствии с авторскими методиками в начале и конце учебного года, одновременно с этим велась работа с родителями на родительских собраниях (анкеты, опросы, беседы). Данные, полученные в результате работы со школьниками, накапливались для отслеживания появившихся изменений в поведении подростка в связи с тем, что раннее выявление проявлений девиантного поведения упрощает его профилактику. Элементы диагностики использовались в течение всего учебного года для пополнения или обновления информации о каждом учащемся, сбора сведений о новых учениках. Своевременность проведения опросов, приведенных в методике, позволила составить достаточно полную картину о каждом школьнике, о характере его поведения в сфере ИКТ.

В начале учебного года проводилось групповое обследование, в ходе которого школьники заполняли:

- анкету для сбора основных сведений об учащемся, включающую в себя вопросы о взаимодействии с коммуникативными средствами (компьютером, смартфоном, планшетом), времени, способах, цели взаимодействия, отношении других членов семьи к ИКТ и др.;
- разработанный Е. В. Черновой (Зеркиной) вопросник диагностики девиантного поведения, основанный на опроснике «Восприятие интернета» (автор Е. В. Щепилина), учитывающий факторы зависимости, особенности восприятия интернета и последствия зависимости;
- адаптированный для среднего звена тест на интернет-зависимость К. Янг (перевод В. А. Лоскутовой (Буровой)).

По результатам обследования **школьники были разделены на две группы:**

1) подростки, у которых выявлены признаки вероятного девиантного поведения в сфере ИКТ или склонности к нему;
2) подростки, у которых не было обнаружено ни проявлений девиантного поведения, ни склонности к нему.

В таблице 1 представлены результаты диагностики девиантного поведения подростков на начало каждого года.

Таким образом, на начало эксперимента:

- 60 % респондентов имели проблемы с целенаправленной работой с ИКТ;
- 29 % респондентов считали мотивирующим фактором своей деятельности развлечения;
- 24 % респондентов часто/иногда «уходили» от реальности при помощи компьютерных игр;
- 29 % респондентов имели игровую зависимость;
- 51 % находились в зоне риска.

Для школьников из первой группы (подростки, у которых выявлены признаки вероятного девиантного поведения в сфере ИКТ или склонности к нему) социальным педагогом и школьным психологом было проведено индивидуальное обследование, после которого была разработана индивидуальная линия работы с каждым учащимся. Для анализа результатов мы опирались на схему анализа отклоняющегося поведения, разработанную Е. В. Змановской [22].

Для учащихся из второй группы (подростки, у которых не было обнаружено ни проявлений девиантного поведения, ни склонности к нему) была проведена первичная диагностика готовности к обеспечению личной кибербезопасности подростков, а также во внеурочное время проведены мастер-классы, лекции и различные конкурсы по тематике обеспечения безопасности личности школьников в сети Интернет, в ходе которых они познакомились с вышеописанными угрозами в среде ИКТ и способами их предупреждения и защиты от воздействий. Был разработан ряд методических пособий, содержащих научно-исследовательские проекты [13, 23–29] и освещающих основные аспекты проблемы кибербезопасности в современном информационном мире.

Негативизм подростков, их психическая и психологическая нестабильность выдвигают особые требования к **формам организации внеурочной деятельности**. По этой причине в качестве основных форм выступали:

- *мастер-классы*, направленные на формирование рационально-познавательного компонента готовности;

Таблица 1

Показатели на начало учебного года, чел.

Показатели		Учебный год		
		2015/2016	2016/2017	2017/2018
Целенаправленность работы с ИКТ	Имеет четкую цель работы	121	140	158
	Легко отвлекается от поставленной цели	183	164	146
Мотивация поведения	Жизнь	152	164	155
	Развлечения	87	62	47
	Обучение, работа с информацией	65	78	102
Уход от реальности	Иногда	43	37	28
	Часто	31	25	22
	Редко	230	242	254
Отклонения в поведении	Нарушения правил и норм поведения в среде ИКТ	60	59	44
	Иногда нарушаю	78	74	68
	Поведение аналогично реальному миру	166	171	192
Игры	Каждый день	87	78	62
	3–5 раз в неделю	155	155	143
	Реже 3 раз в неделю	62	71	99
Жанры игр	Логические	30	43	49
	Симуляторы	47	43	45
	Шутеры	112	108	98
	Стратегии	78	87	82
	Настольные	37	23	30

- *кейсы* для лучшего усвоения материала мастер-класса;
- *игры*, способствующие развитию поведенческого и рефлексивного компонентов.

Занятия позволяли развивать понятийный строй мышления и речевой интеллект, а также совершенствовать внутренний план действий. Особое внимание уделялось сложности учебного материала, так как чрезмерная сложность заданий, помноженная на склонность к глубокому переживанию подростком собственного неблагополучия, может оказать негативное влияние на формирование готовности к обеспечению личной кибербезопасности.

В связи с тем что наше исследование проводилось на протяжении трех учебных лет, цели, **задачи и структура родительского собрания менялись из года в год.**

В 2015/2016 учебном году целью родительского собрания являлось информирование родителей об основных проявлениях девиантного поведения в сфере ИКТ.

Ставились задачи:

- обозначить типологию девиаций поведения в сфере ИКТ;
- познакомить с инструментами выявления проявлений девиантного поведения в сфере ИКТ как у ребенка, так и его окружения;
- провести анкетирование для раннего выявления родителями компьютерной зависимости у подростка;
- ознакомить с основными ошибками родителей, подталкивающими подростка к закрытию своей виртуальной жизни.

Результаты анкетирования были использованы для уточнения характеристик школьников после проведения группового обследования. Был замечен интересный момент — не все родители в своих анкетах отметили отклонения, выявленные у их детей (например, «потерю интереса к спортивным и другим внеклассным мероприятиям», «неспособность рассказать вам о том, как протекает общественная жизнь в школе» и др.), которые свидетельствовали о том, что ребенку не интересна активная жизнь сверстников, что он предпочитает находиться в виртуальном мире и получать аналогичные достижения посредством ИКТ. Однако такие школьники и родители находились вне нашей компетенции, и работа с ними была передана школьному психологу и социальному педагогу (первая группа).

В 2016/2017 учебном году целью родительского собрания уже являлось углубление знаний родителей о виртуальных угрозах и инструментах по защите от них.

Ставились задачи:

- познакомить с классификацией интернет-угроз;
- обозначить инструментарий защиты (антивирус, родительский контроль);
- провести анкетирование для раннего выявления родителями компьютерной зависимости у подростка.

Результат анкетирования показал, что несмотря на проделанную работу некоторые родители обозначили наличие проблем у своих детей, однако большая их часть была связана со спецификой виртуальных сообществ, в которых проводили время дети во время летних каникул. Кроме этого добавились дети, перешедшие из других образовательных учреждений, что в целом немного исказило картину исследования.

В 2017/2018 учебном году мы ставили перед собой цель сформировать у родителей компетенцию по самостоятельному выявлению признаков девиаций в поведении в сфере ИКТ у своих детей.

Для этого были выполнены следующие задачи:

- проведен тренинг на опознание девиаций поведения в сфере ИКТ;
- психологом была проведена мини-лекция о методах поведения при различных вариантах действий подростка (закрытие виртуальной жизни, скрытность и т. д.);
- отработаны ситуации, иллюстрирующие нормальное и отклоняющееся поведение школьников в сфере ИКТ (кейс-метод).

Для школьников кроме классного часа, посвященного анкетированию и сбору данных, **в течение учебного года проводились по три внеклассных мероприятия**.

В 2015/2016 учебном году были проведены интерактивная лекция, виртуальная игра и мастер-класс.

Интерактивная лекция «Безопасность — мое кредо».

Цель лекции — познакомить школьников с основными угрозами в виртуальном мире. Интерактивная лекция — это лекция с активным участием обучающихся, вовлечение их в диалог и полилог. Следует отметить, что несмотря на довольно сложный и обширный материал школьники были знакомы практически со всеми проблемами, которые им предлагались для обсуждения. Что еще раз подчеркнуло важность работы в этом направлении, так как дети уже столкнулись с угрозами личной безопасности, но не все готовы и умеют адекватно на них реагировать.

Виртуальная игра «Гарри Поттер и запрещенный мир» проводилась в виде веб-квеста, целью которого являлась проверка умений школьников реагировать на угрозы ИКТ-среды. Был разработан ряд заданий, основанных на распространенных киберугрозах (фишинг, кибербуллинг, пропаганда преступлений, девиации поведения в сфере ИКТ и др.), и для победы необходимо было их деактивировать «заклинаниями» из ключевых слов. Например, Гарри Поттер получил электронное письмо со следующим текстом: «Гарри! Я чистил компьютер и нашел последние фото с твоими родителями, пересылаю их тебе» и прикрепленным архивом Potter.7zip.exe. Участникам необходимо было выбрать правильное заклинание для открытия письма и архива. В данном случае это было заклинание «Леттерус Удалятус». Особенность проведения данной игры — назначение капитанами команд школьников с диагностированными девиациями в поведении в сфере ИКТ. Это необходимо для того, чтобы вовлечь школьника в коллективную деятельность, но сделать это в комфортной для него среде, где он может выступить в качестве лидера.

Мастер-класс «Социальный интернет».

Цель — научить школьника настраивать аккаунт в социальной сети.

Задачи:

- анализ ошибок существующего аккаунта в социальной сети;
- настройка аккаунта с учетом поставленных целей и возрастных особенностей;
- некоторые аспекты самопрезентации в интернете.

В 2016/2017 учебном году проводились интерактивная лекция и игра.

Интерактивная лекция «Деструктивные течения виртуальности».

Цель — рассказать школьникам о том, какие деструктивные группы и направления активно распространяются в виртуальном мире и несут в себе угрозу для личной безопасности.

Задачи:

- рассмотреть деструктивные группы, их разновидности и особенности;
- обменяться опытом опознания деструктивных посылов;
- выработать правила безопасности.

Лекция посвящена не только суицидальным группам и играм по типу «Синего кита», но в целом рассматривает деструктивные направления воздействий на психику, особый акцент в лекции делается на предупреждениях «геройств», когда на волне всеобщего обсуждения подростки стали вступать в группы типа «Синий кит» для того, чтобы посмотреть, как работает механизм доведения до самоубийства.

Игра «Что делать, если...» основана на поиске решения в кризисной ситуации.

Цель игры — отработать навыки противодействия киберугрозам.

Правила игры: команды по три—пять человек получают набор карточек «решение»: «игнорировать», «рассказать родителям», «присоединиться», «удалить», «скачать» и т. д. Ведущий показывает на экране описание ситуации. Какая команда быстрее поднимет карточку с наиболее точным ответом, та и получает один балл.

Например:

- учитель прислал в социальной сети задание на дом, решение — «скачать»;
- получено sms с неизвестного номера «а вот и фоточки, ссылка», решение — «удалить».

Эта игра также имеет своей целью вовлечение в коллектив школьников с выявленными отклонениями в поведении. Идеальный вариант, когда команды составляет психолог с учетом выявленных отклонений и характеров, тогда каждый ребенок имеет возможность не быть статистом, а полностью участвовать в игре.

В 2017/2018 учебном году в качестве завершающего мероприятия был проведен ***мастер-класс «Цена свободы — вечная бдительность!»***, целью которого является систематизация знаний о наиболее часто встречающихся киберугрозах и формирование навыков их выявления и защиты. Мастер-класс проводится в форме интерактивной лекции с включением кейсов, иллюстрирующих определенный вид киберугроз, которые школьники должны сами

опознать, охарактеризовать и под руководством ведущего сформулировать в сжатом виде основные рекомендации по защите. Например: «Все врут — доверяй, но проверяй!», «Держи свою информацию при себе», «Не кормите тролля» и т. д. По окончании мастер-класса проводится игра «Боюсь! Не боюсь!», в ходе которой демонстрируются объекты, связанные с различными киберугрозами или вполне мирные, не несущие в себе опасности: реклама виртуального казино — «боюсь!»; электронная библиотека — «не боюсь!». Школьники должны отреагировать определенным образом на демонстрируемый объект, тем самым закрепляя полученные знания и одновременно позволяя педагогу проверить, насколько успешно был проведен мастер-класс.

В таблице 2 представлены результаты диагностики школьного коллектива подростков на конец учебного года, включая результаты детей, демонстрировавших девиации поведения в среде ИКТ.

На конец эксперимента были получены следующие результаты:

- 32 % респондентов имели проблемы с целенаправленной работой с ИКТ;
- 5 % респондентов считали мотивирующим фактором своей деятельности развлечения;
- 15 % респондентов часто/иногда «уходили» от реальности при помощи компьютерных игр;
- 15 % респондентов имели игровую зависимость.

По некоторым критериям показатель значительно снизился: целенаправленность работы с ИКТ — с 60 % до 32 %; развлечение как мотивирующий фактор — с 29 % до 5 %.

Сводные данные с показателями на начало и конец учебного года представлены в таблице 3.

На третьем этапе для второй группы подростков была выполнена оценка динамики уровня готовности к обеспечению личной кибербезопасности. Для этого были использованы следующие показатели динамических рядов:

- средний показатель (АР), отражающий количественную оценку роста уровня готовности к обеспечению личной кибербезопасности, который вычислялся по формуле:

$$\text{АР} = \frac{a + 2b + 3c}{100}, \quad (1)$$

где a, b, c — выраженное в процентах количество подростков, находящихся на низком, среднем и высоком уровнях;

- показатель темпа роста (Y), который отражает качественный рост исследуемого показателя и вычисляется по формуле:

$$\text{Y} = \frac{y_1 + 2y_2 + 3y_3}{x + 2x_2 + 3x_3}, \quad (2)$$

где y_1, y_2, y_3 — выраженное в процентах количество респондентов, имеющих соответ-

Таблица 2

Показатели на конец учебного года, чел.

Показатели		Учебный год		
		2015/2016	2016/2017	2017/2018
Целенаправленность работы с ИКТ	Имеет четкую цель работы	136	158	202
	Легко отвлекается от поставленной цели	168	146	102
Мотивация поведения	Жизнь	167	171	180
	Развлечения	62	47	19
	Обучение, работа с информацией	75	86	105
Уход от реальности	Иногда	34	25	28
	Часто	25	22	16
	Редко	245	257	260
Отклонения в поведении	Нарушения правил и норм поведения в среде ИКТ	59	50	25
	Иногда нарушаю	81	68	78
	Поведение аналогично реальному миру	164	186	201
Игры	Каждый день	78	62	47
	3–5 раз в неделю	161	140	124
	Реже 3 раз в неделю	65	102	133
Жанры игр	Логические	37	40	47
	Симуляторы	40	37	37
	Шутеры	99	81	68
	Стратегии	84	74	65
	Настольные	44	72	87

Таблица 3

Сводные показатели, чел.

Показатели		Учебный год					
		2015/2016		2016/2017		2017/2018	
		Начало года	Конец года	Начало года	Конец года	Начало года	Конец года
Целенаправленность работы с ИКТ	Имеет четкую цель работы	121	136	140	158	158	202
	Легко отвлекается от поставленной цели	183	168	164	146	146	102
Мотивация поведения	Жизнь	152	167	164	171	155	180
	Развлечения	87	62	62	47	47	19
	Обучение, работа с информацией	65	75	78	86	102	105
Уход от реальности	Иногда	43	34	37	25	28	28
	Часто	31	25	25	22	22	16
	Редко	230	245	242	257	254	260
Отклонения в поведении	Нарушения правил и норм поведения в среде ИКТ	60	59	59	50	44	25
	Иногда нарушаю	78	81	74	68	68	78
	Поведение аналогично реальному миру	166	164	171	186	192	201
Игры	Каждый день	87	78	78	62	62	47
	3–5 раз в неделю	155	161	155	140	143	124
	Реже 3 раз в неделю	62	65	71	102	99	133
Жанры игр	Логические	30	37	43	40	49	47
	Симуляторы	47	40	43	37	45	37
	Шутеры	112	99	108	81	98	68
	Стратегии	78	84	87	74	82	65
	Настольные	37	44	23	72	30	87

ственно низкий, средний и высокий уровни сформированности на конец эксперимента; $x1$, x_2, x_3 — выраженное в процентах количество респондентов, имеющих соответственно низкий, средний и высокий уровни сформированности на начало эксперимента.

Результаты оценки представлены в таблице 4.

Анализ полученных результатов свидетельствует о заметном возрастании уровня готовности подростков к обеспечению личной кибербезопасности, при этом наиболее успешно развивается рефлексивный компонент. Основываясь на полученных данных, можно сделать вывод о положительном эффекте разработанной методики.

Таблица 4

Экспериментальные данные

Компонент	Этап	Высокий	Средний	Низкий	Средний показатель	Темп роста Y
Рационально-познавательный	Начало эксперимента	17,76	42,43	39,80	1,78	1,30
	Конец эксперимента	41,12	48,36	10,53	2,31	
Рефлексивный	Начало эксперимента	5,26	10,53	84,21	1,21	1,75
	Конец эксперимента	25,00	62,17	12,83	2,12	
Поведенческий	Начало эксперимента	11,84	71,05	18,09	1,96	1,13
	Конец эксперимента	37,50	52,96	2,96	2,21	

Заключение и выводы

В данной работе была доказана эффективность методики формирования готовности к обеспечению личной кибербезопасности во внеурочной деятельности. Проведенное исследование показало, что ранняя диагностика у подростков девиаций поведения в среде ИКТ позволяет при правильно налаженном контакте педагогов, психологов и родителей предупредить их дальнейшее развитие.

Следует заметить, что, несмотря на активную работу педагогического коллектива, количество детей с девиациями поведения в сфере ИКТ постоянно выявлялось. Это обусловлено особенностями психофизиологического периода развития подростка, а также слабой готовностью родителей осуществлять профилактику появления девиаций поведения в сфере ИКТ либо неспособностью осуществлять контроль над деятельностью ребенка в сети. В ходе работы некоторые родители оказались удивлены результатами первого этапа обследования, так как ответы детей абсолютно не совпадали с их представлениями о том, чем и как занимается их ребенок в ИКТ-среде.

Обогащение внеурочной деятельности занятиями по обучению подростков основам личной кибербезопасности не только позволяет закрепить навыки правильного поведения в информационном пространстве, но и способствует формированию устойчивости к негативному информационному воздействию, особенно необходимой в условиях агрессивной информационной среды. Разумеется, такой подход требует от учителей и классных руководителей не только целенаправленности, виртуозного владения отдельными темами информатики и ИКТ, но и готовности использовать нетрадиционные методы и формы обучения.

Важно отметить, что развитие научно-технической мысли приводит к появлению новых видов информационного воздействия и других киберугроз. По этой причине регулярное обновление методического и дидактического обеспечения является одним из наиболее важных условий эффективной работы педагога. Кроме этого требуется ряд исследований, в рамках которых нужно разработать новые формы работы со школьниками раннего подросткового возраста, а также определить их эффективность для различных целевых групп. Это обеспечит достижение результата, в качестве которого выступает здоровый психически, нравственно способный к социально значимому творчеству, социально полезной активности подросток.

Список использованных источников

1. *Лоскутова В. А.* Интернет-зависимость как форма нехимических аддиктивных расстройств: автореф. дис. ... канд. мед. наук. Новосибирск, 2004.

2. *Жичкина А. Е.* Интернет-зависимость // Научно-популярный журнал «Ломоносов». 2003. № 7–8. С. 13–15.

3. *Чернова Е. В.* Потенциальные угрозы в ИКТ-насыщенной среде // VIII Международная конференция «Стратегия качества в промышленности и образовании» (8–15 июня 2012 года, г. Варна, Болгария). В 3 т. Т. III. Днепропетровск; Варна, 2012. С. 490–492.

4. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646). http://www.garant.ru/products/ipo/prime/doc/71456224/#ixzz5SOPhZT5R

5. Закон Российской Федерации от 27.12.1991 г. № 2124-1 (ред. от 25.11.2017 г.) «О средствах массовой информации». http://www.consultant.ru/document/cons_doc_LAW_1511/

6. Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». http://www.consultant.ru/document/cons_doc_LAW_108808/

7. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». http://www.consultant.ru/document/cons_doc_LAW_61798/

8. *Зеркина Е. В., Чусавитина Г. Н.* Подготовка будущих учителей к превенции девиантного поведения школьников в сфере информационно-коммуникативных технологий: монография. Магнитогорск: МаГУ, 2008.

9. *Chernova E., Bobrova I., Movchan I., Zerkina N., Trofimov E., Chusavitina G.* Teachers' training for prevention of pupils' deviant behaviour in ICT // Proceedings of the 2016 conference on Information Technologies in Science, Management, Social Sphere and Medicine. Vol. 51. https://www.atlantis-press.com/proceedings/itsmssm-16/25856093

10. *Чернова Е. В.* Информационная безопасность для гуманитариев: учебник для студентов вузов. Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г. И. Носова, 2016.

11. *Зеркина Е. В., Чусавитина Г. Н.* ИКТ: инновация небезопасная // Народное образование. 2008. № 8. С. 273–276.

12. *Подласый И. П.* Курс лекций по коррекционной педагогике для средних специальных учебных заведений. М.: ВЛАДОС, 2003.

13. *Chernova E. V., Dokolin A. S.* Project method in the prevention of youth involvement in cyber extremism activity // SWORLDJOURNAL. 2015. Vol. 8. No. 1. С. 25–31.

14. *Менделевич В. Д.* Клиническая и медицинская психология: практическое руководство. М.: Медпресс, 2001.

15. *Качалов В.* Об аддикциях и аддиктивном поведении. http://lib.world-mobile.net/psychology/ showfull&id=1176211603&archive=&start_from=&ucat=30&

16. *Платонов К. К.* Структуры и развитие личности. М.: АН СССР, Ин-т психологии, 1986.

17. *Доколин А. С.* Развитие явления киберэкстремизма в информационно-коммуникативной среде // Теория и практика современной науки: Материалы XVI Международной научно-практической конференции (г. Москва, 30 декабря 2014 года). М.: Институт стратегических исследований, 2014. С. 361–366.

18. Психология общения. Энциклопедический словарь. https://communication_psychology.academic.ru/

19. *Иванова С. П.* Психологическая устойчивость личности как фактор противодействия негативным влияниям социальной среды в ранней юности и молодости // Вестник псковского государственного педагогического университета. Серия «Социально-гуманитарные и психолого-педагогические науки». Псков: Псковский государственный университет, 2008. С. 99–108.

20. *Гаврилова И. В.* Профилактика киберэкстремизма среди молодежи // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи: Сборник статей / под ред. Г. Н. Чусавитиной, Л. З. Давлеткириевой, Е. В. Черновой. Магнитогорск, 2013. С. 24–28.

21. *Розенова М. И.* Педагогическая психология: учебное пособие. М: МГУП, 2003.

22. *Змановская Е. В.* Девиантология (Психология отклоняющегося поведения): учебное пособие для студентов высших учебных заведений. 3-е изд., испр. и доп. М.: Академия, 2006.

23. *Доколин А. С., Чернова Е. В.* Метод проектов в превенции вовлечения молодежи в киберэкстремистскую деятельность // Психология и педагогика: на рубеже веков: монография. В 2 кн. Кн. 1. Одесса: КУПРИЕНКО СВ, 2015. С. 6–38.

24. *Чернова Е. В., Доколин А. С.* Применение интерактивных методов обучения для противодействия киберэкстремистской деятельности среди молодежи // Informative and communicative space and a person: Materials of the V international scientific conference (Prague, April 15–16, 2015). Prague: Vědeecko vydavatelské centrum «Sociosféra-CZ», 2015. P. 167–172.

25. *Зеркина Е. В.* Методика диагностики и профилактики девиантного поведения школьников в сфере информационно-коммуникативных технологий: учебно-методическое пособие. Магнитогорск: МаГУ, 2006.

26. *Зеркина Е. В., Чусавитина Г. Н.* Проблемы организации учебно-воспитательной деятельности со школьниками в целях нейтрализации негативного воздействия ИКТ // Вестник Московского государственного открытого университета. Серия «Открытое образование». 2006. № 2 (33). Т. 1. С. 97–102.

27. *Зеркина Е. В.* Совместная работа учителя и родителей по преодолению негативного воздействия ИКТ-среды на школьника // Применение новых технологий в образовании: Сборник материалов XIX международной конференции (г. Троицк, 26–27 июня 2008 года). Троицк: Торвант, 2008. С. 130–132.

28. *Романова М. В., Чернова Е. В.* Методика организации внеурочной деятельности по информатике и ИКТ. Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г. И. Носова, 2017.

29. *Мовчан И. Н., Чернова Е. В., Чусавитина Г. Н.* Учебный проект как одна из форм противодействия киберэкстремизму среди школьников // Фундаментальные исследования. 2015. № 9-3. С. 486–490.

FORMATION IN THE EARLY ADOLESCENCE OF THE WILLINGNESS TO ENSURE PERSONAL CYBERSECURITY

E. V. Chernova[1], **A. S. Dokolin**[2], **I. V. Gavrilova**[1]

[1] ***Nosov Magnitogorsk State Technical University***
455000, Russia, Chelyabinsk Region, Magnitogorsk, Lenin Ave., 38

[2] ***School 28, Magnitogorsk***
455038, Russia, Chelyabinsk Region, Magnitogorsk, K. Marx Ave., 141/4

Abstract

The current stage of education development in the Russian Federation is characterized by early inclusion of children and adolescents in the information space, to resist the negative information impact of which they are often not ready. In spite of the fact that the formation of a person capable of ensuring resistance to cyber threats is an urgent need for school education, actively involving the student in the digital information environment, at the moment the lack of effective pedagogical cures of this problem is observed. This paper describes an experiment on the formation of younger adolescence schoolchildren readiness to ensure personal cybersecurity on the basis of the technique developed by authors affecting mainly extracurricular activities for young adolescents. Results of an experiment have confirmed efficiency of the developed pedagogical cures of the studied problem. Thus, authors managed to create a technique which can be recommended for work with school students of early teenage age which analogs don't exist.

Keywords: ICT, information security, cyber security, cyber threats, personal cybersecurity, deviant behavior, early adolescence.

DOI: 10.32517/0234-0453-2018-33-7-16-26

For citation:

Chernova E. V., Dokolin A. S., Gavrilova I. V. Formirovanie v rannem podrostkovom vozraste gotovnosti k obespecheniyu lichnoj kiberbezopasnosti [Formation in the early adolescence of the willingness to ensure personal cybersecurity]. *Informatika i obrazovanie — Informatics and Education*, 2018, no. 7, p. 16–26. (In Russian.)

Received: July 31, 2018.

Accepted: August 20, 2018.

About the authors

Elena V. Chernova, Ph.D. of Pedagogic Sciences, Associate Professor, Associate Professor at the Department of Business Informatics and Information Technologies of Nosov Magnitogorsk State Technical University; HelenaVChernova@gmail.com

Andrey S. Dokolin, Ph.D. of Pedagogic Sciences, Informatics Teacher at School 28, Magnitogorsk; a.dokolin@gmail.com

Irina V. Gavrilova, Ph.D. of Pedagogic Sciences, Associate Professor, Associate Professor of the Department of Business Informatics and Information Technologies of Nosov Magnitogorsk State Technical University; Irina.V.Gavrilova@yandex.ru