

БЕЗЗАТЕЕВА Вероника Сергеевна,
старший преподаватель кафедры гражданского права,
Санкт-Петербургский государственный университет
аэрокосмического приборостроения,
e-mail: bezzateeva@inbox.ru

КОМПЛЕКСНАЯ ЗАЩИТА НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ ИНТЕРНЕТ: ПРОФИЛАКТИКА МОШЕННИЧЕСТВА И АДДИКТИВНОГО ПОВЕДЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В связи со стремительным развитием цифровых технологий и широким распространением Интернета среди несовершеннолетних, у детей и подростков появляются новые возможности для развития и социализации, однако одновременно с этим существуют риски, связанные с киберпреступностью, онлайн-мошенничеством и формированием аддикции (зависимого поведения). В данной статье проведено исследование инновационных подходов в области защиты несовершеннолетних в цифровом пространстве, профилактике аддиктивного поведения и мошеннических действий.

Ключевые слова: защита несовершеннолетних в сети, фильтрация контента, аддиктивное поведение, профилактика мошенничества в сети.

BEZZATEEVA Veronika Sergeevna,
Senior Lecturer of the Department of Civil Law,
Saint-Petersburg State University
of Aeronautical Instrumentation

COMPREHENSIVE PROTECTION OF MINORS IN THE INTERNET: PREVENTION OF FRAUD AND ADDICTIVE BEHAVIOR IN THE RUSSIAN FEDERATION

Annotation. Due to the rapid development of digital technologies and the widespread use of the Internet among minors, children and adolescents have new opportunities for development and socialization, but at the same time, there are risks associated with cybercrime, online fraud, and the development of addiction (dependent behavior). This article explores innovative approaches to protecting minors in the digital space, preventing addictive behavior, and combating fraud.

Key words: online protection of minors, content filtering, addictive behavior, online fraud prevention.

Глобальная цифровизация поспособствовала резкому увеличению числа пользователей сети Интернет, особенно среди несовершеннолетних. По данным Росстата, 90% детей от 4 до 5 лет и 99% от 16 до 18 лет регулярно пользуются Интернет-ресурсами. Цифровая среда является мощным инструментом для образования, коммуникации и творчества, однако возникают серьезные проблемы, связанные с информационной безопасностью несовершеннолетних и профилактикой зависимости от виртуального мира. Интернет становится трансграничным пространством, используемым для манипуляций злоумышленников, направленных на финансовое вымогательство, психологическое

давление и кражу персональных данных. Кроме того, возникает опасность возникновения патологической привязанности к цифровым развлечениям и социальным сетям.

Таким образом, существует необходимость разработки комплексных мер по обеспечению безопасности несовершеннолетних в сети Интернет, выраженных в передовых методиках анализа рисков, инновационной профилактической работе и нормативно-правовом регулировании всех аспектов.

Методология исследования

Исследование основано на теоретическом анализе отечественной и зарубежной литературы

по вопросам психологии, педагогики и правовых основ защиты прав несовершеннолетнего в киберпространстве. Были использованы методы контент-анализа нормативно-правовых актов Российской Федерации, статистического анализа вовлеченности детей в киберпреступность и использование киберпространства в правомерных целях.

Основным целями исследования являются:

- Анализ существующих угроз для несовершеннолетних в интернет-пространстве и выявление особенностей проявления аддиктивного поведения.
- Разработка научно обоснованной модели профилактических мероприятий, направленной на минимизацию риска мошенничества и формирование паттернов безопасного пользования Интернетом.
- Оценка эффективности предложенных моделей и рекомендаций по совершенствованию системы защиты несовершеннолетних пользователей в рамках законодательства Российской Федерации.

Основные угрозы и особенности аддиктивного поведения.

1. Кибермошенничество.

Наиболее распространенными, на сегодняшний день, являются фишинговые атаки, кража паролей и персональных данных, распространение вредоносного программного обеспечения и мошеннические действия, направленные на махинации с финансовыми средствами. Такого рода мошеннические действия чаще всего реализуются посредством шантажа пользователя личной информацией, полученной путем несанкционированного доступа к информации в социальных сетях или электронной почты. Несовершеннолетние являются наиболее уязвимой категорией пользователей, в силу недостаточной осведомленности о правилах безопасного поведения в Интернет.

2. Аддиктивное поведение.

Интернет-зависимость является серьезной проблемой сегодняшней реальности. Выделяют несколько типов аддикций, возникающих из-за чрезмерного увлечения компьютерными играми, социальными сетями, мессенджерами и потоковыми сервисами. Аддиктивное состояние характеризуется определенными признаками:

- Неспособность контролировать количество времени, проведенное в сети.
- Негативное влияние на физическое здоровье, социальную активность и успеваемость по учебе, [1, с. 391].
- Психологические расстройства, такие как депрессия и тревожность.

Причины возникновения зависимых состояний многообразны и связаны с личностными особенностями несовершеннолетних, отсутствием четких границ взаимодействия с интернет-контентом и недостатком родительского контроля, [2, с. 47].

Защита несовершеннолетних в цифровом пространстве требует комплексного подхода, включающего в себя совокупность правового регулирования, технологических решений и воспитательных мероприятий.

Российская Федерация уделяет большое внимание созданию условий для реализации и обеспечения безопасной среды для несовершеннолетних в сети Интернет. Среди ключевых нормативных документов можно выделить Федеральный закон № 434-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон РФ №152-ФЗ «О персональных данных». Эти законы устанавливают ограничения на распространение вредоносной и опасной информации, контроль над содержанием информационных ресурсов и платформ и защиту персональных данных несовершеннолетних. Однако, как показывает практика, эффективность указанных норм недостаточна, в связи с стремительными изменениями технологических решений и поведенческих стереотипов рассматриваемой категории пользователей.

Современные технологические средства защиты позволяют значительно повысить уровень защищенности несовершеннолетних в сети. Одним из эффективных инструментов является использование специализированных фильтров и систем мониторинга активности пользователя в Интернет. Такого рода инструменты дают возможность родителям и лицам их замещающим ограничить доступ к нежелательным ресурсам, отслеживать подозрительные контакты и предотвращать возможные негативные последствия. Наиболее эффективным на сегодняшний день является внедрение антивирусных программ с функцией родительского контроля, таких как Kaspersky Safe Kids и Dr. Web Parental Control, которые обеспечивают автоматическую фильтрацию потенциально опасного контента в зависимости от возрастной категоризации пользователя.

К категории технологических решений, также можно отнести предложение о введении личной карты пользователя (школьника) для доступа к компьютеру, социальной сети или Интернету в целом, так как в отличие от использования, к примеру, системы наподобие «умный город», при помощи которой происходит аутентификация

человека по его лицу, либо использование системы распознавания отпечатка пальца, или руки — как система «Ладони», использование идентификационной карты учащегося или e-Token не разглашает личную информацию несовершеннолетнего, при этом обеспечивая сохранность личных данных несовершеннолетнего, а также возможность разграничения доступа к информации в сети Интернет в зависимости от возраста обладателя данной карты или соответствующего e-Token, [3, с. 317].

На данный момент особое внимание необходимо уделить инициативе введения детских SIM-карт, которые представляют собой специальный вид услуг мобильного оператора, предназначенный исключительно для несовершеннолетних. Подобные карты предоставляют ряд возможностей, таких как:

- Оперативное блокирование нежелательного контента. Автоматическая фильтрация и ограничение доступа к опасным сайтам и приложениям, что снижает риск столкновения с кибербуллингом, мошенничеством и вредным контентом.
- Увеличение ответственности операторов и родителей. Обязательное информирование и контроль обязывают родителей быть более внимательными к онлайн-активности детей и вовремя реагировать на потенциальные угрозы.
- Раннее выявление опасных ситуаций. Мониторинг активности дает возможность своевременно вмешаться и предотвратить опасную ситуацию по ее признакам (контакты с подозрительными пользователями или доступ к запрещенной / вредной информации).
- Создание безопасной среды для онлайн-активности. Обеспечивая контроль и фильтрацию, государство и операторы создают более безопасную среду, где несовершеннолетние могут общаться, учиться, развиваться и проводить свое время, минимизируя риски.

В свою очередь, на примере опыта других стран, становится возможным оценить результаты введения такого рода SIM-карт. Китай является одним из первых государств, успешно реализовавших концепцию детских карт с начала 2010-х годов. Они стали популярны среди китайских семей благодаря простоте своего использования и доступности. Например, китайская компания China Mobile предлагает детскую SIM-карту с функциями отслеживания местоположения ребенка, управления звонками и сообщениями, а также контролем расхода трафика и баланса на

счете, благодаря чему родители могут своевременно реагировать на потенциальные опасности и контролировать деятельность несовершеннолетних в цифровом пространстве. Китайский опыт свидетельствует о положительном влиянии детских SIM-карт на снижение уровня мошенничества в отношении детей и увеличение уровня удовлетворенности родителей качеством предоставляемых услуг оператором мобильной связи. Исследования показывают, что такие карты способствуют уменьшению количества телефонных мошенничеств и сокращению количества несанкционированного доступа к персональным данным пользователей, [4, с. 340].

Великобритания также имеет положительный опыт использования детских SIM-карт. Оператор Vodafone предложил услугу «Vodafone Guardian», предназначенную специально для несовершеннолетних, в рамках которой родители могут устанавливать правила дозвола, запрета на прием входящих звонков и сообщений от неизвестных номеров, включить фильтры на доступ к определенному контенту и определить геозоны, в рамках которой ребенок сможет пользоваться телефоном. Согласно проведенным исследованиям, около 70% британских родителей оценили детские SIM-карты положительно, отметив повышение чувства уверенности относительно безопасности своих детей в период нахождения вне дома, [5, с. 267].

Опыт КНР и Великобритании наглядно демонстрирует преимущества внедрения детских SIM-карт как эффективного механизма обеспечения безопасности несовершеннолетних в мобильной среде.

Относительно образовательной инициативы, одной из наиболее перспективных стратегий предотвращения негативного воздействия сети Интернет является развитие медиаобразования. Несовершеннолетних необходимо обучать грамотному пользованию ресурсами цифрового пространства, критическому восприятию потребляемой информации и правилам поведения в трансграничном пространстве Интернет. В школах целесообразно вводить специализированные курсы по информационной безопасности и формированию здорового представления о роли Интернет в жизни современного человека и общества в целом. Возможно, наиболее оптимальным вариантом будет введение такого рода образовательных проектов, реализуемых государственными учреждениями совместно с некоммерческими организациями и представителями бизнеса. Данные программы должны включать в себя элементы практической подготовки пользователей к противостоянию мошенническим действиям в

сети, к проявлениям аддиктивного воздействия на них и способствовать получению навыков самостоятельного принятия верных решений в сложных ситуациях.

Комплексная защита несовершеннолетних в цифровом пространстве предполагает взаимодействие всех заинтересованных сторон, таких как семья, школа, государственные органы и общество в целом.

Список литературы:

[1] Афанасьева Л.И. Особенности интернет-зависимости подростков // Журнал «Проблемы современного педагогического образования». — 2024. — № 84-1. — С. 390-392.

[2] Дарендорф М.В. Психолого-педагогическая профилактика интернет-зависимости подростков. // Журнал «Наука в жизни человека». — 2024. — №2. — С. 44-51.

[3] Беззатеева В.С. Идентификация несовершеннолетнего в сети Интернет для предотвращения аддиктивного влияния. // Журнал «Закон. Право. Государство». — 2022. — № 3 (35). — С. 316-321.

[4] Zhao Y., Zhang X., Wang H. The impact of children's SIM cards on the safety of minors in mobile communication // Journal «Information Technology and People». — 2022. — № 33(2). — С. 431- 446.

[5] Jonson A., Smith J. Evaluating the effectiveness of child-specific SIM cards for enhancing parental control over children's mobile phone usage // International Journal «Child Computer Interaction». — 2023. — № 24 — С. 264-270.

References:

[1] Afanasyeva L.I. Features of Internet addiction of adolescents//Journal "Problems of modern pedagogical education." — 2024. — № 84-1. — С. 390-392.

[2] Darendorf M.V. Psychological and pedagogical prevention of Internet addiction of adolescents. // Journal "Science in human life." — 2024. — №2. - S. 44-51.

[3] Bezzateeva V.S. Identification of a minor on the Internet to prevent addictive influence. //Journal "Law. Right. State." — 2022. — № 3 (35). - S. 316-321.

[4] Zhao Y., Zhang X., Wang H. The impact of children's SIM cards on the safety of minors in mobile communication // Journal «Information Technology and People». — 2022. — № 33(2). - S. 431-446.

[5] Jonson A., Smith J. Evaluating the effectiveness of child-specific SIM cards for enhancing parental control over children's mobile phone usage // International Journal «Child Computer Interaction». — 2023. - NO. 24 - S. 264-270.





ЮРКОМПАНИ

www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.