Дата поступления рукописи в редакцию: 10.07.2026 г.
Дата принятия рукописи в печать: 31.07.2026 г.
DOI: 10.24412/2076-1503-2026-8-723-727

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

ПРАВОВАЯ ПРОФИЛАКТИКА ЦИФРОВОЙ ВИКТИМИЗАЦИИ НЕСОВЕРШЕННОЛЕТНИХ ПРИ ИСПОЛЬЗОВАНИИ ИГРОВЫХ МОДИФИКАЦИЙ

Аннотация. *В статье рассматривается правовая профилактика цифровой виктимизации несовершеннолетних при использовании игровых модификаций, неофициальных лаунчеров, читов и иных файлов, распространяемых в игровых сообществах. Показано, что риск для ребенка возникает не только из вредоносного кода, но и из доверительной игровой среды, социально-инженерной подачи и последующего оборота персональных данных. Предлагается модель профилактического паспорта риска игровой модификации, объединяющая источник файла, способ распространения, состав запрашиваемых разрешений, признаки вредоносности, порядок реагирования образовательной организации и меры правового просвещения несовершеннолетних.*

Ключевые слова: *несовершеннолетние; игровые модификации; цифровая виктимизация; персональные данные; информационная безопасность; правовое просвещение; цифровая гигиена.*

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

PROCESSUAL VALIDITY OF DIGITAL EVIDENCE IN A RISK-ORIENTED MODEL OF CONSOLIDATION AND EVALUATION

Annotation. *The article examines legal prevention of digital victimization of minors when using game modifications, unofficial launchers, cheats and other files distributed in gaming communities. It is shown that the risk for a child arises not only from malicious code, but also from the trust-based gaming environment, social-engineering presentation and subsequent circulation of personal data. The author proposes a preventive risk passport for game modifications that records the file source, distribution method, requested permissions, signs of malicious activity, response procedures of educational organisations and measures of legal education for minors.*

Key words: *minors; game modifications; digital victimization; personal data; information security; legal education; digital hygiene.*

Игровая среда стала для несовершеннолетних не только пространством досуга, но и устойчивым каналом общения, обучения, творчества и самопрезентации. Ребенок участвует в игровых сообществах, смотрит инструкции, обменивается файлами, устанавливает модификации и доверяет рекомендациям блогеров, друзей или участников сервера. В такой ситуации вредоносная игровая модификация представляет собой не только техническую угрозу, но и социально-правовой риск: ребенок добровольно запускает файл, считая его элементом игры, а затем становится объектом сбора учетных данных, переписки, изображений, токенов доступа, сведений об устройстве и иной информации, позволяющей прямо или косвенно идентифицировать его.

Актуальность проблемы определяется тем, что традиционная профилактика детской безопасности в сети часто строится вокруг вредного контента: запрета опасной информации, возрастной классификации, блокировки сайтов, ограничения доступа к материалам, причиняющим вред здоро-

вью и развитию. Однако вредоносная модификация опасна не содержанием описания, а технологическим действием файла после запуска. Страница может выглядеть как нейтральная инструкция по установке улучшенной графики или нового игрового режима, но сам исполняемый объект будет копировать данные, подключаться к внешнему серверу или устанавливать дополнительный компонент. Поэтому профилактика должна учитывать не только информационное сообщение, но и цифровой объект, который передается несовершеннолетнему.

Методология исследования

Исследование основано на формально-юридическом, системном и риск-ориентированном методах. Формально-юридический метод использован для анализа норм о защите персональных данных, информации, причиняющей вред здоровью и развитию детей, а также общих обязанностей субъектов, участвующих в обеспечении детской цифровой безопасности. Системный метод позволил рассмотреть игровую модификацию как элемент единой среды, включающей платформу, сообщество, канал распространения, несовершеннолетнего пользователя, родителей и образовательную организацию. Риск-ориентированный метод применен для разграничения обычной пользовательской модификации, спорного файла и вредоносного цифрового объекта.

Целью настоящего исследования является разработка правовой модели профилактики цифровой виктимизации несовершеннолетних при использовании игровых модификаций.

Игровая модификация может быть рассмотрена как правовой пограничный объект. С одной стороны, моддинг является формой пользовательского творчества и не должен рассматриваться как изначально противоправная деятельность. С другой стороны, именно внешняя легитимность модификации используется злоумышленниками для маскировки вредоносного компонента. В этой связи профилактика не должна сводиться к запрету любых модов. Чрезмерный запрет вытесняет детей в менее контролируемые каналы, где выше вероятность столкновения с вредоносными файлами. Более продуктивной является модель управляемого риска: ребенок должен понимать признаки безопасного источника, а взрослые - иметь понятный порядок проверки и реагирования. Правовая специфика рассматриваемого риска связана с персональными данными. В игровой среде ребенок редко передает паспортные сведения, однако его цифровая идентичность складывается из множества фрагментов: никнейма, игрового аккаунта, токена сессии, IP-адреса, изображения, голоса, переписки, сведений о школе, городе, друзьях, родителях, устройстве и привычках. В совокупности эти сведения могут позволять определить конкретного несовершеннолетнего и использоваться для давления, кибербуллинга, шантажа, создания фейковых профилей или доступа к иным сервисам. Поэтому профилактика должна объяснять детям, что персональные данные - это не только паспорт и адрес, но и цифровые следы, связанные с реальной личностью [3; 4].

Вредоносная игровая модификация формирует особый тип цифровой виктимизации. Ребенок не только теряет доступ к аккаунту или виртуальным предметам, но может столкнуться с утечкой переписки, изображений, контактов, данных о месте учебы и социальных связях. Возникает повторная виктимизация: похищенные сведения используются не один раз, а длительно циркулируют в игровых чатах, закрытых каналах, базах данных или на ресурсах с незаконным оборотом информации. Такая ситуация особенно опасна для несовершеннолетнего, поскольку последствия затрагивают эмоциональное состояние, репутацию, безопасность общения и образовательную среду. Действующее российское законодательство содержит несколько взаимосвязанных блоков защиты. Закон о персональных данных закрепляет принципы законности, минимизации, определенности цели, безопасности обработки и защиты субъекта данных. Закон о защите детей от информации, причиняющей вред их здоровью и развитию, ориентирует правоприменителя на приоритет интересов ребенка. Закон об информации, информационных технологиях и о защите информации содержит публично-правовые механизмы ограничения доступа к противоправным сведениям. Однако эти блоки не образуют полноценного профилактического стандарта именно для вредоносных цифровых объектов, распространяемых в игровой среде. Следовательно, необходима локальная и методическая конкретизация для образовательных организаций, родителей и платформенных сообществ.

В образовательной организации профилактика вредоносных игровых модификаций может рассматриваться как часть правового просвещения и формирования цифровой грамотности. Речь идет не о вмешательстве школы или вуза в досуг ребенка, а о защите права несовершеннолетнего на безопасное участие в цифровой среде. Образовательная организация уже участвует в профилактике буллинга, экстремистских проявлений, мошенничества и опасного поведения в сети. Игровые модификации должны быть включены в этот ряд как самостоятельный объект цифровой гигиены, поскольку именно через них ребенок может потерять персональные данные, доступ к

аккаунту и контроль над собственной цифровой репутацией [3; 4].

Для практического применения предлагается использовать профилактический паспорт риска игровой модификации. Такой паспорт не является процессуальным документом и не заменяет экспертное исследование. Его задача - помочь педагогическому работнику, родителю или самому подростку предварительно оценить, насколько безопасен файл до его установки. В паспорт целесообразно включать следующие блоки: источник файла, доменное имя или площадка размещения, наличие официальной страницы проекта, сведения об авторе, дата обновления, формат файла, необходимость запуска от имени администратора, запрашиваемые разрешения, наличие отзывов на независимых площадках, предупреждения антивируса, требования отключить защиту, просьба ввести пароль или токен, обещание чрезмерного игрового преимущества, наличие сокращенной ссылки или архива с исполняемым файлом.

Ключевым элементом паспорта является не техническая экспертиза, а правовая логика предупреждения риска. Если файл требует отключить антивирус, запустить неизвестный установщик, ввести логин и пароль вне официальной платформы или перейти по ссылке из закрытого чата, ребенок должен понимать, что такие признаки указывают на повышенную вероятность противоправного получения данных. Педагог или родитель, в свою очередь, получает не абстрактный запрет, а набор проверяемых признаков, по которым можно объяснить опасность без морализаторства и без полного запрета моддинга.

Отдельное значение имеет процедура реагирования, если вредоносная модификация уже была установлена. В образовательной профилактике целесообразно закреплять простой алгоритм: прекратить использование файла, сменить пароли к игровым и связанным учетным записям, завершить активные сессии, включить двухфакторную аутентификацию, проверить устройство антивирусным средством, сохранить скриншоты страницы распространения, ссылки, переписку и предупреждения системы, сообщить родителям или ответственному педагогу, при наличии утечки персональных данных обратиться к оператору сервиса и при необходимости в компетентные органы. Такой алгоритм важен потому, что ребенок часто боится наказания за установку «чита» и скрывает проблему до момента, когда последствия становятся более тяжелыми. Профилактика должна учитывать возрастную дифференциацию. Для младших школьников эффективнее работают простые правила: скачивать дополнения только вместе с взрослым, не вводить пароль на постороннем сайте, не отключать защиту устройства, не запускать неизвестный файл. Для подростков необходима более сложная правовая рамка: объяснение ценности персональных данных, рисков продажи аккаунтов, уголовно-правовых последствий умышленного распространения вредоносных файлов, ответственности за шантаж, кибербуллинг и использование чужих данных. Подросток должен понимать, что пересылка «мода» может быть невинной ошибкой, но сознательное распространение файла, похищающего данные, уже имеет иную правовую оценку [5].

Важным субъектом профилактики являются игровые платформы и администраторы сообществ, ориентированных на несовершеннолетних. Минимальный стандарт добросовестного поведения может включать выделение проверенных модификаций, предупреждения перед скачиванием исполняемых файлов, запрет публикации инструкций по отключению средств защиты, механизм жалоб на вредоносные моды, быструю блокировку подтвержденных ссылок, уведомление пользователей о выявленной угрозе, а также недопустимость стимулирования детей к передаче токенов, паролей и иных идентификаторов [6]. При этом платформа не должна отвечать за любой пользовательский файл только из-за его размещения, но должна реагировать на очевидные и подтвержденные признаки риска.

Родительский контроль не должен превращаться только в наблюдение и запреты. Более эффективной является договорная модель цифрового поведения: ребенок заранее знает, где можно искать моды, какие признаки опасны, кому сообщить о проблеме и что обращение за помощью не повлечет автоматического наказания. Такая модель снижает латентность инцидентов. Если ребенок уверен, что за признание в установке подозрительного файла его, прежде всего, защитят, вероятность своевременного реагирования возрастает.

Особую роль играет доказательственное сохранение цифрового следа. Для образовательной и семейной профилактики важно объяснять, что удаление переписки, страницы или файла не всегда помогает, а иногда лишает возможности подтвердить факт угрозы. Необходимо сохранять адрес страницы, скриншоты, дату и время скачивания, название архива, имя отправителя, сообщения с обещаниями «без вирусов» или требованиями отключить защиту. Эти сведения могут потребоваться для обращения к платформе, оператору связи, образовательной организации, правоохранительным органам или специалисту по информационной безопасности. В то же время сбор доказательств не должен приводить к повторно-

му распространению вредоносного файла среди детей.

Предлагаемый профилактический паспорт может быть включен в локальные методические материалы образовательной организации: памятку по цифровой гигиене, план классного часа, курс по информационной безопасности, инструкцию для педагогов и родителей. Для юридической корректности в нем следует отделять три уровня: обычная пользовательская модификация, файл повышенного риска и вероятно вредоносный объект. Такая градация позволит избежать стигматизации легального моддинга, но сохранит возможность быстрого реагирования на признаки угрозы.

На уровне содержания правового просвещения необходимо отказаться от формулы «не скачивай ничего из Интернета» как практически невыполнимой. Для современного подростка такая рекомендация выглядит оторванной от реальной цифровой жизни. Более продуктивными являются конкретные критерии: скачивать файлы с официальных или проверенных площадок, не запускать архивы из комментариев и закрытых чатов, не передавать токены и cookies, не вводить пароль после перехода из видеоописания, проверять доменное имя, не отключать защиту ради установки мода, обсуждать сомнительные файлы со взрослым или специалистом. Правовое содержание таких правил состоит в предупреждении незаконного оборота персональных данных и снижении риска вовлечения ребенка в противоправную активность.

Вредоносные игровые модификации образуют самостоятельную проблему детской цифровой безопасности, находящуюся на пересечении информационного права, защиты персональных данных, профилактики правонарушений и образования. Их опасность обусловлена не только вредоносным кодом, но и игровой формой маскировки, доверием несовершеннолетнего к сообществу, стремлением получить преимущество и недостаточной способностью оценить последствия запуска файла. Поэтому профилактика должна строиться не на запрете моддинга как такового, а на риск-ориентированном управлении цифровым поведением.

Предлагаемый профилактический паспорт риска игровой модификации позволяет соединить юридическую и педагогическую логику. Он фиксирует источник файла, способ распространения, признаки повышенного риска, потенциальные персональные данные, порядок реагирования и правила сохранения цифровых следов. Для образовательных организаций такой инструмент может стать частью программ правового просвещения и информационной безопасности; для родителей - понятным алгоритмом разговора с ребенком; для несовершеннолетних - практической памяткой, позволяющей отличать безопасный моддинг от рискованного запуска неизвестного файла. Защита персональных данных несовершеннолетних в игровой среде требует перехода от контентной модели к модели технологически вредоносного цифрового объекта. Ребенка необходимо защищать не только от опасного текста или изображения, но и от файла, который под видом развлечения получает доступ к его цифровой идентичности. Такая профилактика должна сочетать правовое просвещение, технические меры, участие семьи, ответственность платформ и уважение к возрастной автономии несовершеннолетнего.

Список литературы:

[1] Федорова А. С. Проблемы обеспечения безопасности персональных данных несовершеннолетних в информационно-телекоммуникационных сетях // Юридический мир. - 2023. - № 7. - С. 36-41.

[2] Лахтина Т. А. Персональные данные несовершеннолетних как объект правовой охраны // Вестник Московского университета МВД России. - 2020. - № 4. - С. 190-194.

[3] Беззатеева В. С. Инновационные методы обеспечения информационной безопасности несовершеннолетних в сети Интернет // Волновая электроника и инфокоммуникационные системы: материалы XXVII Международной научной конференции. - СПб.: ГУАП, 2024. - С. 28-32.

[4] Беззатеева В. С. Техническое обеспечение безопасности несовершеннолетних в сети Интернет в Российской Федерации // Экономика и качество систем связи. - 2025. - № 4. - С. 136-142.

[5] Самосват О. И. «Лайк» в социальных сетях как показатель социального одобрения в подростковой среде // Казанский педагогический журнал. - 2023. - № 6-1. - С. 148-150.

[6] Зотова Д. В., Розанов В. А. Патологическое использование и зависимость от социальных сетей - анализ с позиций феномена аддиктивного поведения // Вестник СПбГУ. Серия 16. Психология. Педагогика. - 2020. - № 2. - С. 158-183.

References:

[1] Fedorova A. S. Problems of ensuring the security of personal data of minors in information and telecommunication networks // Legal World. - 2023. - № 7. - S. 36-41.

[2] Lakhtina T. A. Personal data of minors as an object of legal protection // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. - 2020. - № 4. - S. 190-194.

[3] Bezzateeva V. S. Innovative methods for ensuring the information security of minors on the Internet // Wave electronics and information and communication systems: materials of the XXVII International Scientific Conference. - St. Petersburg: GUAP, 2024. - S. 28-32.

[4] Bezzateeva V. S. Technical security of minors on the Internet in the Russian Federation // Economics and quality of communication systems. - 2025. - № 4. - S. 136-142.

[5] Samosvat O. I. "Like" in social networks as an indicator of social approval in a teenage environment // Kazan Pedagogical Journal. - 2023. - № 6-1. - S. 148-150.

[6] Zotova D.V., Rozanov V.A. Pathological use and dependence on social networks - analysis from the standpoint of the phenomenon of addictive behavior // Bulletin of St. Petersburg State University. Series 16. Psychology. Pedagogy. - 2020. - № 2. - S. 158-183.