

Научная статья
УДК 159.9
<https://doi.org/10.36511/2078-5356-2022-4-174-178>

Психологические особенности формирования личности несовершеннолетнего киберпреступника

Федосеева Ольга Игоревна

Нижегородская академия МВД России, Нижний Новгород, Россия, olfedoseeva_2011@mail.ru

Аннотация. В статье рассматривается проблема формирования личности несовершеннолетнего киберпреступника: раскрывается психологическая сущность взаимодействия несовершеннолетнего киберпреступника и потерпевшего; описывается эффект онлайн-дезингибиции (или эффект растормаживания), возникающий на базе ослабления психологических барьеров и действия факторов диссоциативной анонимности, «невидимости», асинхронности действий, солипсической интроекции, диссоциативного воображения и минимизации авторитета. Понимание психологических особенностей формирования личности несовершеннолетнего киберпреступника позволит, по мнению автора, определить основные направления совершенствования профилактики и раннего выявления киберпреступлений среди молодежи.

Ключевые слова: цифровая реальность, киберпространство, киберпреступления, личность несовершеннолетнего киберпреступника, эффект онлайн-дезингибиции

Для цитирования: Федосеева О. И. Психологические особенности формирования личности несовершеннолетнего киберпреступника // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 174—178. <https://doi.org/10.36511/2078-5356-2022-4-174-178>.

Original article

Psychological features of the underage cybercriminal personality formation

Olga I. Fedoseeva

Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russian Federation, olfedoseeva_2011@mail.ru

Abstract. The article reviews the problem of the underage cybercriminal personality formation: it reveals the psychological essence of the interaction between the underage cybercriminal and the victim; describes the online disinhibition effect, which occurs on the basis of the weakening psychological barriers and the action of dissociative anonymity factors, invisibility, asynchronicity, solipsistic introjection, dissociative imagination and minimizing authority. Understanding the psychological features of the formation of the personality of a minor cybercriminal will, according to the author, determine the main directions for improving the prevention and early detection of cybercrime among young people.

Keywords: digital reality, cyberspace, cybercrimes, underage cybercriminal personality, online disinhibition effect

For citation: Fedoseeva O. I. Psychological features of the underage cybercriminal personality formation. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2022, no. 4 (60), pp. 174—178. (In Russ.). <https://doi.org/10.36511/2078-5356-2022-4-174-178>.

«Цифровая реальность», «цифровой мир», «цифровизация», «цифровые технологии», «цифровое пространство», «киберпространство» — эти слова прочно вошли в наш лексикон и принимаются одной половиной человечества как благо, другой — как неизбежность.

Действительно, цифровые технологии проникают в нашу повседневную жизнь, с одной стороны, упрощая ее, но с другой — делая уязвимей. Поэтому киберпреступления становятся одной из глобальных угроз в современном мире.

© Федосеева О. И., 2022

Согласно последним данным, сейчас каждое четвертое преступление совершается с использованием IT-технологий. По данным Главного управления экономической безопасности и противодействия коррупции МВД России за восемь месяцев 2021 года возбуждено 385 000 дел в сфере кибермошенничества. От 85 до 97 % киберпреступлений остаются невыявленными, раскрывается не более 25 % преступлений [1]. Серьезность проблемы подтверждает тот факт, что 7 декабря 2021 года Генеральная Ассамблея ООН одобрила без голосования российско-американскую резолюцию о нормах поведения в киберпространстве и о предотвращении преступлений в этой сфере [2; 3].

Чаще всего киберпреступниками оказываются молодые люди — школьники и студенты. Так, например, одним из первых групповых киберпреступлений стал интернет-взлом персональных компьютеров *группой несовершеннолетних*, назвавших себя «группа-414»; взлом информационной системы плотины в Аризоне *12-летним хакером* в 1998 году. Если бы он открыл все сливные ворота плотины, то могли быть затоплены несколько городов с общей численностью более одного миллиона жителей [3].

По данным исследования Лаборатории Капсера «Взрослые и дети в цифровом мире», проведенного в январе 2019 года, с электронными устройствами большинство детей знакомятся в 3 года, к 4—6 годам более чем у половины (54 % детей) есть планшет или смартфон, в 7—10 лет около 43 % детей имеют аккаунты в соцсетях, к 11—14 годам имеют гаджеты 97 % подростков [4]. Раннее знакомство с электронными устройствами и цифровыми сервисами, возможность самостоятельно действовать в цифровом пространстве, таким образом, становятся факторами для формирования личности несовершеннолетнего киберпреступника. Согласно последним исследованиям, «все подростки в той или иной степени являются киберзависимыми (половина — на стадии увлеченности—прилипания, другая половина имеют первую и вторую стадии зависимости), деструктивная киберсоциализация подростков преобладает над конструктивной» [5].

Исходя из приведенных данных, может быть сделан вывод о том, что *решение проблемы растущего уровня киберпреступности неразрывно связано с пониманием особенностей формирования личности современных детей и молодежи в условиях цифровой реальности*, поэтому неслучайным является появление

новой отрасли психологии — киберпсихологии, изучающей конкретные аспекты онлайн-поведения. По мнению многих исследователей, действия в цифровом пространстве могут «негативно повлиять на психическое, духовное, нравственное здоровье и развитие несовершеннолетнего» [6].

Предметом обсуждения настоящей статьи являются психологические особенности формирования личности несовершеннолетнего киберпреступника. Понимание этих особенностей поможет прогнозированию поведения несовершеннолетних в различных ситуациях риска и выделению мишеней воздействия со стороны экстремистских организаций, деструктивных культов, опасных групп и сообществ [7], а также позволит определить основные направления совершенствования профилактики и раннего выявления киберпреступлений среди молодежи.

Отличительная особенность киберпреступлений — среда их совершения — киберпространство. Эта особенность определяет и психологическую сущность взаимодействия несовершеннолетнего киберпреступника и потерпевшего (рис. 1):

— устранение материальной составляющей взаимодействия и опосредование (виртуализация) психологического содержания взаимосвязей ведет к восприятию киберпреступником собственных действий как нематериальных и, соответственно, не несущих материальных, «серьезных» последствий [6, с. 88];

— уход от реальности, подмена истинного мира ложным является результатом действия механизма расщепления — психологической защиты, основанной на искажении реальности, защиты, посредством действия которой киберпреступник стремится оправдать собственные действия;

— психике несовершеннолетних свойственны, в той или иной степени, определенные комплексы и фобии, заниженная самооценка, неуверенность в собственных силах (внешности, знаниях, социальном статусе и т. д.), создающие препятствия полноценному общению со сверстниками вне виртуального пространства [6; 7]; цифровая среда обеспечивает снятие этих барьеров и оказывается для юного киберпреступника наиболее комфортной, предпочтительной;

— дистанцирование от объекта преступления позволяет киберпреступнику не ощущать вины за собственные преступные действия, «обесценивать» потерпевшего;



Рис. 1. Сущность взаимодействия киберпреступника и потерпевшего

— незрелость мышления как следствие недостаточного опыта и знаний, склонность к подражанию, определенная податливость отрицательным влияниям микросреды [6, с. 69] сочетается у юных киберпреступников с высоким уровнем интеллекта и компетентности в отношении знаний о механизмах работы «среды», где совершается преступление [8]; положительное подкрепление в случае успеха ведет к последующему совершению преступлений;

— это приводит к нивелированию и замещению социальных норм, снижению критичности, развитию ощущения безнаказанности, вседозволенности, формированию деструктивного поведения и специфической субкультуры [9].

Джон Сулер, доктор философии, преподаватель кафедры психологии научно-технического центра Университета Райдера (США) описал в серии статей под единым названием «Психология киберпространства» «эффект онлайн-дезингибиции» (или эффект растормаживания). Согласно этому эффекту, человек действует в киберпространстве более свободно, нежели чем в реальном социуме [10]. Возникновение этого эффекта обеспечивается действием пяти взаимодействующих и взаимодополняющих факторов:

— диссоциативная анонимность («ты меня не знаешь») — фактор сокрытия собственной идентичности и создания нового образа, благодаря ему киберпреступник полагает, что может не брать на себя ответственность за свои действия [10]; помимо этого, «за анонимностью закреплена возможность для несовершеннолетнего пользователя создать новый образ собственной личности» [9];

— невидимость («ты меня не видишь») — возможность быть физически невидимым

приводит к повышению уверенности в себе, снижению страха быть обнаруженным, эмоциональной свободе, ослаблению психологических барьеров, расчетливости и хладнокровию при планировании своих действий «даже в условиях полной неопределенности» [7];

— асинхронность («увидимся позже») — фактор, характеризующийся одновременными действиями в интернет-пространстве несовершеннолетнего киберпреступника и его жертвы, при этом исчезает необходимость «немедленной реакции на слова или действия; этот фактор порождает, в свою очередь, эффект «эмоционального удара и бегства» [9]: несовершеннолетнему кажется, что, если в момент совершения киберпреступления его никто не схватит за руку, то и дальнейшего наказания не последует;

— солипсическая интроекция («это все в моей голове») [9] — представление о том, что реальность является результатом воображения киберпреступника, обеспечивает уверенность в собственной безопасности;

— диссоциативное воображение («это все игра») — киберпреступник оценивает свое поведение как игру, не случайно путь к преступлениям начинается в большинстве случаев именно с компьютерных игр, таких как *Grand Theft Auto* (в основе ее сюжета — путешествие по городу, поиск «прохожих» и их ограбление), *Counter-Strike* (одна из популярнейших «ходилок», целью которых является убийство и победа над «врагами»), *Doom* (жанр этой игры традиционный — убийства — шутинг от первого лица) и другие. У несовершеннолетнего при совершении киберпреступления возникает аналогичное игровое состояние: ему кажется, что от совершаемого преступления «можно в

любое время отключиться, а правила поведения — свои и жертвы — можно контролировать самому» [9];

— минимизация авторитета («мы равны») — статус пользователя в киберпространстве не имеет такого большого влияния, как в реальном мире, его статус главным образом зависит от навыков коммуникации, технических навыков, качества выражаемых идей и твердости убеждений; страх перед авторитетами, боязнь неодобрения и наказания исчезают.

Если обратиться к практике раннего выявления киберпреступлений среди молодежи, то на основе анализа сайтов общеобразовательных организаций следует констатировать, что основная профилактическая работа сосредоточена вокруг вопросов цифровой безопасности. Но никто не задумывается о том, что подростковый возраст имеет одну характерную особенность: мнение взрослых (педагогов, родителей, сотрудников правоохранительных органов) в этот период, к сожалению, не всегда является значимым. Поэтому, выслушав информацию о преступлениях в цифровом пространстве, несовершеннолетние могут воспринять ее в перевернутом виде — как призыв к действию, например: «Попробуй, а у тебя получится... взломать чужую страницу в соцсетях?».

Среди особенностей несовершеннолетних, повышающих риски возникновения радикальных установок и вовлечения в противоправную деятельность в киберпространстве, согласно исследованиям А. М. Столяренко, Н. В. Сердюк, В. В. Вахниной, О. М. Боевой и Л. Л. Грищенко — не критичность восприятия поступающей информации (принимают на веру все, что предлагают им социальные сети), повышенная внушаемость, стремление безусловно принимать мнение значимой для подростка референтной группы [11], основанную на потребности в принятии значимыми в данный возрастной период сверстниками. Таким образом, взрослые могут подтолкнуть несовершеннолетнего к попыткам «более глубокого» освоения цифрового пространства.

Именно поэтому проводимая профилактическая работа должна быть взвешенной: необходимо не только знакомить подростков с правилами цифровой гигиены, но и предостерегать от попыток киберпреступлений, рассказывая об их правовых последствиях. Следует помнить, что формирование личности несовершеннолетнего киберпреступника происходит сразу в двух пространствах: реальном и цифровом, и решение проблемы растущего уровня

киберпреступности неразрывно связано с пониманием особенностей формирования личности современных детей и молодежи в условиях цифровой реальности.

Список источников

1. Арапов В., Заруцкая Н. Почему киберпреступления — угроза национальной безопасности // Ведомости. 07.12.2021. URL: <https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti> (дата обращения: 27.06.2022).
2. Юшков М. ООН приняла резолюцию России и США против преступного использования ИТ // РБК. Ру. URL: <https://www.rbc.ru/politics/07/12/2021/61ae9e609a79479108eef855> (дата обращения: 27.06.2022).
3. Буз С. И. Киберпреступления: понятие, сущность и общая характеристика // Юрист-Правоведь, 2019. № 4 (91). С. 78—82.
4. Взрослые и дети в цифровом мире: когда онлайн встречается с офлайн, исследование «Лаборатории Касперского». URL: <https://kids.kaspersky.ru/digest/issledovanie-vzroslye-i-deti-v-tsifrovom-mire-kogda-onlajn-vstrechaetsya-s-oflajnom> (дата обращения: 24.06.2022).
5. Харарбахова М. А., Мусатова О. А., Шпагина Е. М. Интернет и одиночество подростков // Психология и право. 2021. Том 11. № 4. С. 2—13.
6. Рыбакова О. С. Безопасность несовершеннолетних в информационном обществе: анализ киберрисков и угроз // Мониторинг правоприменения. 2020. № 2 (35). С. 65—73.
7. Расторгуев А. Ю. К вопросу о киберрискованном онлайн-поведении несовершеннолетних подростков // Проблемы современного педагогического образования. 2021. № 72 (1). С. 362—365.
8. Мавринская Т. В. Психологические особенности киберпреступников // Инновационное развитие. 2018. № 21. С. 156—158.
9. Косенков А. Н., Черный Г. А. Общая характеристика психологии киберпреступника // Всероссийский криминологический журнал. 2012. № 3 (21). С. 87—94.
10. Suler J. The Psychology of Cyberspace. URL: <http://users.rider.edu/~suler/psycyber/psycyber.html> (дата обращения: 27.06.22).
11. Столяренко А. М., Сердюк Н. В., Вахнина В. В., Боева О. М., Грищенко Л. Л. Психологические аспекты деструктивного информационно-психологического воздействия // Психология и право. 2019. Т. 9. № 4. С. 75—89.

References

1. Arapov V., Zarutskaya N. Why cybercrime is a threat to national security. *Vedomosti*. 07.12.2021. URL: <https://www.vedomosti.ru/technology/articles/2021/12/>

- 07/899278-kiberprestupleniya-bezopasnosti (accessed 27.06.2022). (In Russ.)
2. Yushkov M. The UN adopted a resolution of Russia and the United States against the criminal use of IT. *RBC.Ru*. URL: <https://www.rbc.ru/politics/07/12/2021/61ae9e609a79479108eef855> (accessed 27.06.2022). (In Russ.).
3. Buz S. I. Cybercrime: concept, essence and general characteristics. *Lawyer-Jurist*, 2019, no. 4 (91), pp. 78—82. (In Russ.)
4. Adults and children in the digital world: when Online meets Offline, research “Kaspersky Labs”. URL: <https://kids.kaspersky.ru/digest/issledovanie-vzroslye-i-deti-v-tsifrovom-mire-kogda-onlajn-vstrechaetsya-s-ollajnopdf/> (accessed 27.06.2022). (In Russ.).
5. Khararabakhova M. A., Musatova O. A., Shpagina E. M. Internet and loneliness of teenagers. *Psychology and law*, 2021, vol. 11, no. 4, pp. 2—13. (In Russ.)
6. Rybakova O. S. The safety of minors in the information society: analysis of cyber risks and threats. *Law enforcement monitoring*, 2020, no. 2 (35), pp. 65—73. (In Russ.)
7. Rastorguev A. Yu. On the issue of cyber risky online behavior of underage teenagers. *Problems of modern pedagogical education*, 2021, no. 72 (1), pp. 362—365. (In Russ.)
8. Mavrinskaya T. V. Psychological characteristics of cybercriminals. *Innovative development*, 2018, no. 21, pp. 156—158. (In Russ.)
9. Kosenkov A. N., Tchorniy G. A. General characteristics of cybercriminal psychology. *All-Russian Journal of Criminology*, 2012, no. 3 (21), pp. 87—94. (In Russ.)
10. Suler J. The Psychology of Cyberspace. URL: <http://users.rider.edu/~suler/psycyber/psycyber.html> (accessed 27.06.2022).
11. Stolyarenko A. M., Serdyuk N. V., Vakhnina V. V., Boeva O. M., Grishchenko L. L. Psychological aspects of destructive informational and psychological impact. *Psychology and law*, 2019, vol. 9, no. 4, pp. 75—89. (In Russ.)

Информация об авторе

О. И. Федосеева — кандидат психологических наук, доцент.

Information about the author

O. I. Fedoseeva — Candidate of Sciences (Psychology), Associate Professor.

Статья поступила в редакцию 24.07.2022; одобрена после рецензирования 24.09.2022; принята к публикации 01.12.2022.

The article was submitted 24.07.2022; approved after reviewing 24.09.2022; accepted for publication 01.12.2022.