

МАЙОРОВ АНДРЕЙ ВЛАДИМИРОВИЧ

*Заведующий кафедрой прокурорского надзора и организации
правоохранительной деятельности
Челябинского государственного университета,
профессор кафедры уголовного права имени М. И. Ковалева
Уральского государственного юридического университета
ab_majorov@mail.ru*

ВИКТИМНОСТЬ ЦИФРОВОЙ ЛИЧНОСТИ («ЦИФРОВАЯ ВИКТИМОЛОГИЯ»)

Аннотация. Развитие цифровых технологий вносят свои коррективы и трансформирует процессы, происходящие в современном обществе. Цифровизация оказывает не только позитивное, но негативное воздействие на современное общество. Уровень криминализации в российском обществе свидетельствует о распространении противоправных деяний, совершаемых с использованием информационно-телекоммуникационных технологий, сети «Интернет», а также с использованием цифровых технологий. Появление новых видов преступной деятельности, совершение преступлений удаленным (дистанционным) способом порождает и новый вид виктимизации — цифровую виктимизацию.

Высказывается необходимость о развитии нового научного направления виктимологических исследований, направленного на изучение цифровой виктимности жертв преступлений и выработки соответствующих мер виктимологической профилактики.

Ключевые слова: виктимность, виктимизация, цифровизация, цифровые технологии, преступность, дистанционные преступления, цифровая виктимизация, цифровая виктимность.

MAYOROV ANDREI VLADIMIROVICH

*Head Chair of Prosecutor's Supervision and Organization
of Law Enforcement Activity of the Chelyabinsk State University,
Professor of the M. I. Kovalev Chair of Criminal Law of the Ural State Law University*

VICTIMIZATION OF THE DIGITAL PERSON (“DIGITAL VICTIMOLOGY”)

Abstract. The development of digital technologies makes its own adjustments and transforms the processes occurring in modern society. Digitalization has not only a positive but also a negative impact on modern society. The level of criminalization in Russian society indicates the spread of unlawful acts committed with the use of information and telecommunication technologies, the Internet, as well as with the use of digital technologies. The emergence of new types of criminal activity, committing crimes remotely gives rise to a new type of victimization — digital victimization.

There is a need to develop a new scientific direction of victimization research, aimed at studying the digital victimization of victims of digital crimes and the development of appropriate victimization prevention measures.

Key words: victimhood, victimization, digitalization, digital technology, crime, remote crime, digital victimization, digital victimization, digital victimization, digital victimhood.

Процесс внедрения современных цифровых технологий переживает в настоящее время все общество. Безусловно, государство заинтересовано в совершенствовании и развитии новейших технологий, принимает активное участие и выступая в качестве регулятора, инвестора и стимулятора инноваций, определяет направление и темпы развития новых технологий на уровне страны.

Применение цифровизации в государственных структурах, на производстве, в бизнесе, в быту, в образовании и т.д. упрощает многие процессы, делая их более простыми и доступными¹. Цифровизация оказывает колоссальное влияние на основные подсистемы социума (экономику, политику и управление, образование, культуру здравоохранение и т.д.), на социальную структуру

¹ См. подр.: Майоров А. В. Влияет ли цифровизация на виктимизацию в современном обществе? // Виктимология. 2022. Т. 9, № 2. С. 148-156; Майоров А. В. Виктимологическое обеспечение информационной безопасности личности // Правопорядок: история, теория, практика. 2024. № 3(42). С. 80-88.

общества и его функционирование, вызывая новые социальные и коммуникативные формы взаимодействия¹. Какие же риски несет в себе внедрение цифровых технологий и какое влияние они оказывают на уровень криминализации и виктимизации в российском обществе? Эти и многие другие вопросы стали поводом для проведения научных исследований криминологами и виктимологами².

Цифровые технологии

Многие социальные процессы стали возможны за счет внедрения цифровых технологий в общественные отношения. Стоит отметить, что именно сейчас более чем когда-либо, социальное существование определяется как физической, так и цифровой реальностью. Любые процессы, происходящие в обществе, связаны с определенными переменами, которые трансформируют его в новое состояние, требующее анализа и выявления возможных рисков, связанных с угрозой для общества³.

Криминализация (Цифровая преступность)

Изменения происходят не только в обществе, меняется и преступность. Криминальная статистика за последние годы свидетельствует о том, что с развитием новых технологий меняются и сферы преступной активности. Границы киберпреступности расширяются за счет появления новых способов и средств совершения противоправных деяний трансформируясь в цифровую преступность, — преступления, совершаемые в сфере цифровых технологий или с их использованием.

Совершение преступлений с использованием цифровых технологий уже очевидный факт, свидетельством этому является официальная статистика количества зарегистрированных преступлений в России, данные, полученные от организаций, осуществляющих кибербезопасность и мнение экспертов.

Количество киберпреступлений в России за пять лет выросло в 2,3 раза. По итогам 2023 года их доля в числе всех зарегистрированных уголовных посягательств составила почти 35%. Для сравнения — по итогам 2022 года этот показатель равнялся 26,5%⁴.

В январе — июле 2024 года зарегистрировано 434,7 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 17,1% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 32,6% в январе — июле 2023 года до 38,9%. Почти половина таких преступлений (47,1%) относится к категориям тяжких и особо тяжких (205,0 тыс.; +5,2%), четыре преступления из пяти (82,9%) совершаются с использованием сети «Интернет» (360,6 тыс.; +26,5%), почти половина (46,5%) — средств мобильной связи (202,0 тыс.; +20,8%). Почти 2/3 таких преступлений (63,8%) совершается путем кражи или мошенничества: 277,5 тыс. (+5,5%), каждое девятое (11,1%) — с целью незаконного производства, сбыта или пересылки наркотических средств: 48,2 тыс. (+1,0%)⁵.

¹ Комлев Ю. Ю. Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии // Вестник Казанского юридического института МВД России. 2020. Т. 11, № 1(39). С. 31.

² См.: Антонян Е. А., Клешина, Е. Н. Кибервиктимность // Вестник Пермского института ФСИН России. 2019. № 3 (34). С. 5-10; Жмуров Д. В. Кибервиктимология. Москва: Юрлитинформ, 2023. 296 с.; Жмуров, Д. В. Модели реализации виктимности в цифровой среде // Защита жертв преступлений в современном обществе (PVCMS 2023): материалы VI Международной научно-практической интернет-конференции, Челябинск, 21-22 февраля 2023 года. Челябинск, 2023. С. 88-93; Кабанов П. А. Жертвы киберкраж как объект современной российской кибервиктимологии: криминологический анализ статистических показателей криминальной виктимности 2021-2022 гг. // Виктимология. 2024. Т. 11, № 1. С. 25-42; Комлев Ю. Ю. Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии // Вестник Казанского юридического института МВД России. 2020. Т. 11, № 1(39). С. 31-40; Майоров, А. В. Виктимология цифровой преступности: концепция научного направления // Виктимология. 2024. Т. 11, № 1. С. 7-12.

³ Майоров А. В. Влияет ли цифровизация на виктимизацию в современном обществе? // Виктимология. 2022. Т. 9, № 2. С. 149.

⁴ Количество киберпреступлений в России выросло в 2,3 раза за пять лет. URL: <https://www.pnp.ru/social/kolichestvo-kiberprestupleniy-v-rossii-vyroslo-v-23-raza-za-pyat-let.html> (дата обращения: 10.09.2024).

⁵ Сайт МВД России/ Статистика. URL: <https://xn--b1aew.xn--p1ai/dejatelnost/statistics> (дата обращения: 10.09.2024).

При этом за последнее время сам характер киберпреступности заметно изменился: специалисты отмечают рост утечек и незаконной коммерциализации персональных данных. Так, по информации Роскомнадзора, в 2022 году в России произошло около 150 крупных утечек, а в 2023 — уже 168, по итогам которых в Сеть в открытый доступ попало более 510 миллионов записей о гражданах России¹.

Последствия цифровой преступности

Цифровая преступность создает более широкое предметное поле как в теории, так и в исследовательской деятельности. Исследованию цифровой преступности, в последние годы, как уже было отмечено выше, посвящено не мало работ отечественных ученых.

Анализ проводимых исследований в этой области позволяет говорить о том, что цифровые технологии используются преступниками для:

- получения информации на стадии приготовления к совершению преступления;
- изготовления приспособлений и орудий преступлений;
- сокрытия следов преступления и т.д.

Такая ситуация свидетельствует о том, что использование достижений цифровых технологий в преступных целях порождает новые виды виктимизации общества — цифровую виктимизацию.

Виктимизация (Цифровая виктимизация)

Цифровая виктимизация включает в себя весь спектр противоправных деяний, распространенных в физическом мире — как **количественные** (абсолютные числа, коэффициенты и индексы), так и **качественные показатели** (виды преступлений, факторы виктимности, причиненный ущерб (вред))². Такая ситуация вызывает необходимость проведения виктимологических исследований в этой сфере и требует новых форм и методов виктимологического противодействия преступности.

При этом стоит отметить и особенности в возникновении, изучаемой криминологами и виктимологами взаимосвязи «преступник — жертва», которая прослеживается при совершении преступлений с использованием цифровых технологий. Такая взаимосвязь носит особый характер — удаленность (дистанционность) и анонимность. «Дистанционные (удаленные)»³ способы совершения преступлений по оценкам специалистов и экспертов составляют значительную массу среди регистрируемых преступлений.

Цифровая виктимность

Стать пользователем интернет-пространства не сложно, для этого даже порой не нужна регистрация в сети. Однако большинство приложений, сайтов и платформ требует регистрацию пользователя. Оцифрованный набор данных о человеке — имя и фамилия, фотографии и подписи к ним, интересы и увлечения, позволяют создать цифровой профиль личности. Цифровой профиль является наиболее важная часть цифровой личности, представляющая собой совокупность персональных и иных связанных с ними данных индивида в виртуальном пространстве, содержащихся в информационных базах уполномоченных на их обработку субъектов⁴. Именно цифровой профиль личности и является тем самым уязвимым звеном, обладающим определенным уровнем виктимности, потенциальной жертвы цифрового преступления.

¹ Количество киберпреступлений в России выросло в 2,3 раза за пять лет. URL: <https://www.pnp.ru/social/kolichestvo-kiberprestupleniy-v-rossii-vyroslo-v-23-raza-za-pyat-let.html> (дата обращения: 10.09.2024).

² Майоров А. В. Влияет ли цифровизация на виктимизацию в современном обществе? // Виктимология. 2022. Т. 9, № 2. С. 151.

³ См.: Жмуров Д. В. Жертвы кибервымогательства // Власть и общество: история, современное состояние и тенденции развития: сборник материалов Всероссийской научно-практической конференции, Абакан, 21 апреля 2023 года. Абакан, 2023. С. 24-26; Евтушенко И. И. Виктимологическая защита жертв дистанционных хищений // Виктимология. 2023. Т. 10, № 1. С. 78-88; Кабанов П. А. Жертвы киберкраж как объект современной российской кибервиктимологии: криминологический анализ статистических показателей криминальной виктимности 2021-2022 гг. // Виктимология. 2024. Т. 11, № 1. С. 25-42.

⁴ См. подр.: Майоров А. В. Виктимологическое обеспечение информационной безопасности личности // Правопорядок: история, теория, практика. 2024. № 3 (42). С. 80-88.

Жертвы цифровых преступлений («цифровая жертва»)

Необходимо отметить, что жертвы цифровой преступности как правило онлайн-пользователи. Средний возраст онлайн-жертв составляет 35 лет.

К жертвам обладающих цифровой виктимностью (жертвам цифровой преступности) можно отнести:

- потерпевших от киберпреступлений имущественного характера;
- потерпевших от домогательств в сети Интернет;
- потерпевших от насильственных преступлений, совершённых с помощью сети Интернет;
- потерпевших от преступлений, связанных с неправомерным доступом и хищением информации¹.

Федеральный закон «Об информации, информационных технологиях и о защите информации» наделяет правом владельца информации по ее защите, — «обладателю информации предоставляется право самостоятельно в пределах своей компетенции устанавливать режим защиты информации» (ч. 4 ст. 6, ч. 1 ст.16).

Несмотря на осведомленность большинства потенциальных жертв, а главное известность и распространенность мер пассивной виктимологической защиты², уровень цифровой виктимности остается высоким в силу пренебрежения цифровой гигиеной.

Существует необходимость проработки эффективных механизмов защиты цифровой личности со стороны государства по обеспечению информационную безопасность личности. Большинство виктимологических ситуаций связаны с наличием у преступника доступа к базам данных различных организаций, персональным данным о потерпевшем, его фотографиям, служебной и личной информации, переписке в рабочих «чатах» различных мессенджеров, вызваны отсутствием должного уровня защиты цифровых данных.

Полагаем, что одним из способов предотвращения негативных последствий в цифровой виктимизации является цифровая гигиена, которая входит в систему виктимологической профилактики как пассивный метод обеспечения цифровой безопасности личности.

Совокупность обозначенных проблем в рассматриваемой сфере, а также наличие научных разработок по противодействию цифровой виктимизации общества указывает на перспективу развития такого научного направления как цифровая виктимология (виктимология цифровой преступности).

СПИСОК ЛИТЕРАТУРЫ

1. Антонян, Е. А. Кибервиктимность / Е. А. Антонян, Е. Н. Клещина // Вестник Пермского института ФСИН России. — 2019. — № 3 (34). — С. 5-10.
2. Евтушенко, И. И. Виктимологическая защита жертв дистанционных хищений / И. И. Евтушенко // Виктимология. — 2023. — Т. 10, № 1. — С. 78-88. — DOI: <https://doi.org/10.47475/2411-0590-2023-10108>.
3. Жмуров, Д. В. Кибервиктимология / Д. В. Жмуров. — Москва: Юрлитинформ, 2023. — 296 с. — ISBN 978-5-4396-2502-4. — EDN FDSGFA.
4. Жмуров, Д. В. Виктимологическая характеристика жертв киберпреступлений России / Д. В. Жмуров // Вопросы российского и международного права. — 2024. — Т. 14, № 4-1. — С. 532-538. — EDN BXKYAG.
5. Жмуров, Д. В. Последствия кибервиктимизации и ее основные признаки / Д. В. Жмуров // III Байкальский юридический форум: материалы международных научно-практических конференций и конкурса молодых ученых, Иркутск, 04-06 октября 2023 года. — Иркутск: Издательский дом БГУ, 2023. — С. 238-242. — EDN IWNMIK.
6. Жмуров, Д. В. Жертвы кибервымогательства / Д. В. Жмуров // Власть и общество: история, современное состояние и тенденции развития: сборник материалов Всероссийской научно-практической конференции, Абакан, 21 апреля 2023 года / науч. ред. В. В. Наумкина, отв. ред. В. Н. Козлова. — Абакан: Хакасский государственный университет им. Н. Ф. Катанова, 2023. — С. 24-26. — EDN PLBCQF.
7. Жмуров, Д. В. Модели реализации виктимности в цифровой среде / Д. В. Жмуров // Защита жертв преступлений в современном обществе (PVCMS 2023) : материалы VI Международной научно-практической интернет-конференции, Челябинск, 21-22 февраля 2023 года. — Челябинск: Общество с ограниченной ответственностью «Эскуэла», 2023. — С. 88-93. — EDN ZQIMNY.

¹ См. подр.: Жмуров, Д. В. Виктимологическая характеристика жертв киберпреступлений России // Вопросы российского и международного права. 2024. Т. 14, № 4-1. С. 532-538.

² См.: Майоров, А. В. Виктимологическое обеспечение информационной безопасности личности // Правопорядок: история, теория, практика. 2024. № 3(42). С. 84.

8. Игнатов, А. Н. Информационно-когнитивные технологии в механизме цифровой виктимизации / А. Н. Игнатов, В. С. Соловьев // Вестник Казанского юридического института МВД России. — 2023. — Т. 14, № 1(51). — С. 59-66. DOI 10.37973/KUI.2023.20.15.008. — EDN QAVUVP.
9. Кабанов, П. А. Жертвы киберкраж как объект современной российской кибервиктимологии: криминологический анализ статистических показателей криминальной виктимности 2021-2022 гг / П. А. Кабанов // Виктимология. — 2024. — Т. 11, № 1. — С. 25-42. — DOI 10.47475/2411-0590-2024-11-1-25-42. — EDN TJLGYE.
10. Комлев, Ю. Ю. Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии / Ю. Ю. Комлев // Вестник Казанского юридического института МВД России. — 2020. — Т. 11, № 1(39). — С. 31-40. — DOI 10.24420/KUI.2020.39.1.004. — EDN DSWICP.
11. Майоров, А. В. Влияет ли цифровизация на виктимизацию в современном обществе? / А. В. Майоров // Виктимология. — 2022. — Т. 9, № 2. — С. 148-156. — DOI 10.47475/2411-0590-2022-19202. — EDN MLRFKH.
12. Майоров, А. В. Виктимологическое обеспечение информационной безопасности личности / А. В. Майоров // Правопорядок: история, теория, практика. — 2024. — № 3(42). — С. 80-88. — DOI 10.47475/2311-696X-2024-42-3-80-88. — EDN OGMEQV.
13. Майоров, А. В. Виктимология цифровой преступности: концепция научного направления / А. В. Майоров // Виктимология. — 2024. — Т. 11, № 1. — С. 7-12. — DOI 10.47475/2411-0590-2024-11-1-7-12. — EDN ZRALDW.
14. Майоров, А. В. Виктимологическое обеспечение безопасности общества в современных реалиях: постановка проблемы / А. В. Майоров // Защита жертв преступлений в современном обществе (PVCMS 2023): материалы VI Международной научно-практической интернет-конференции, Челябинск, 21-22 февраля 2023 года. — Челябинск: Общество с ограниченной ответственностью «Эскуэла», 2023. — С. 160-171. — EDN LFMCCZ.
15. Фоминых, Е. С. Нарушения информационной безопасности в контексте цифровой виктимизации детей и подростков / Е. С. Фоминых // Виктимология. — 2024. — Т. 11, № 1. — С. 69-77. — DOI 10.47475/2411-0590-2024-11-1-69-77. — EDN AUDIJK.