Р. Р. Сабиров,
аспирант,
Казанский инновационный университет
имени В. Г. Тимирясова

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ЛИЦ, СОВЕРШАЮЩИХ ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация. Актуальность исследования связана с высоким уровнем киберпреступности в России, что требует разработки эффективных мер противодействия. В статье рассматривается криминологическая характеристика лиц, совершающих преступления в сфере компьютерной информации, на основе анализа предыдущих исследований. Предлагается классификация таких преступников в зависимости от способа совершения преступления, уровня навыков в области информационных технологий и демографических признаков. Работа направлена на формирование более глубокого понимания типов киберпреступников, что позволит разрабатывать более целенаправленные и эффективные меры профилактики и борьбы с киберпреступлениями.

Ключевые слова: киберпреступность, киберпреступник, хакер, классификация киберпреступников, типология киберпреступников, личность киберпреступника, преступления в сфере компьютерной информации, способы совершения преступлений в сфере компьютерной информации

CRIMINOLOGICAL CHARACTERISTICS OF PERSONS COMMITTING CRIMES IN THE FIELD OF COMPUTER INFORMATION

Abstract. The relevance of the study is related to the high level of cybercrime in Russia, which requires the development of effective counteraction measures. The article examines the criminological characteristics of persons who commit crimes in the field of computer information, based on the analysis of previous studies. The classification of such criminals is proposed depending on the method of committing the crime, the level of skills in the field of information technology and demographic characteristics. The work is aimed at developing a deeper understanding of the types of cybercriminals, which will allow us to develop more targeted and effective measures to prevent and combat cybercrime.

Keywords: cybercrime, cybercriminal, hacker, classification of cybercriminals, typology of cybercriminals, identity of a cybercriminal, crimes in the field of computer information, methods of committing crimes in the field of computer information

Введение. С каждым годом объем данных, циркулирующих в цифровом пространстве, стремительно растет, что создает благоприятные условия для злоумышленников, использующих уязвимости информационных систем в своих преступных целях. Нарушения в области компьютерной информации могут иметь разрушительные последствия не только для отдельных граждан и организаций, но и для национальной и глобальной безопасности.

Настоящее исследование актуально прежде всего необходимостью понимания мотивации, социальных и демографических особенностей лиц, совершающих преступления в сфере компьютерной информации, а также их профессиональных навыков и методов совершения преступлений. Это понимание играет ключевую роль в разработке эффективных стратегий предупреждения, раскрытия и расследования преступлений в данной области, а также в формировании адекватных законодательных и правоохранительных мер противодействия.

Основная часть. «Как отмечают исследователи, структура киберпреступности в России включает две группы преступлений: преступления в сфере компьютерной информации, а также преступления с применением информационно-телекоммуникационных технологий» [1. С. 114].

«Также одним из оснований типологии киберпреступников в научной литературе предлагается способ совершения преступлений. В зависимости от способа выделяют обычных киберпреступников, которые занимаются незаконными действиями в рамках отдельных видов преступной деятельности, например наркоторговля через Интернет. А также выделяют преступников, действующих в области компьютерной информации и технологий, чья противоправная деятельность возможна исключительно в киберпространстве, например, использование вредоносных компьютерных программ» [3. С. 105].

В настоящем исследовании предлагается рассмотреть криминологическую характеристику лиц, совершающих преступления в сфере компьютерной информации.

В бытовом обывательском представлении киберпреступник чаще всего ассоциируется с компьютерным хакером, одиноким асоциальным молодым человеком, способным «хакнуть», то есть взломать любую компьютерную систему. Подобное представление о киберпреступнике можно встретить и в научной литературе, исследователи характеризуют его как человека, не обладающего привлекательными внешними данными или имеющими трудности общения со сверстниками, противоположным полом, который ищет самореализации в виртуальном мире, самоутверждается, совершая неправомерный доступ к компьютерной информации или создавая компьютерный вирус [4. С. 86].

Подобное представление о киберпреступниках уже не соответствует реальной картине, киберпреступность стала коммерчески успешным явлением, что как следствие привлекло в эту сферу людей с предпринимательскими качествами и авантюрным духом [8. С. 258].

В современном мире характеристика киберпреступника может быть крайне разнообразна, преступления часто совершаются группой лиц с четким распределением ролей по специализации.

Современные киберпреступники могут отличаться различным уровнем образования, владения информационными технологиями, возрастом, мотивом, социальным положением, что подтверждается в отечественных [1; 3; 5; 8; 9] и зарубежных исследованиях [11. С. 102–103].

Характеризуя особенности лиц, совершающих преступления в сфере компьютерной информации в научной литературе, выделяют следующие типы в зависимости:

1. От способа совершения преступления.

Согласно имеющимся исследованиям [9] рассматриваемую категорию киберпреступников, можно классифицировать в зависимости от способа совершения преступления следующим образом:

– **Применение вредоносных компьютерных программ для неправомерного доступа к мобильным устройствам, компьютерам, ноутбукам и т. д.**

Преступники данной группы могут действовать как одни, так и в группе с четким распределением ролей и функций при реализации более сложного проекта, такие роли можно разделить на создателей, распространителей, и пользователей вредоносных программ. В зависимости от роли будут отличаться и средний возраст преступников, их уровень образования, а также наличие навыков в сфере информационных технологий (далее – ИТ). Однако обычно это мужчины 18–40 лет, с высшим или средним специальным образованием, действующие из корыстных мотивов [9. С. 26–27].

Наличие ролей у киберпреступников обусловлено не только техническими аспектами их деятельности, но и использованием методов социальной инженерии.

В большинстве случаев при киберпреступлениях средства защиты информации работают эффективно, однако слабым звеном часто оказывается сам пользователь из-за своей некомпетентности. Компьютерная система, подвергающаяся взлому, никогда не функционирует изолированно – всегда присутствует человеческий фактор [10. С. 134]. Проблема в том, что как специалисты по информационной безопасности, так и обычные пользователи компьютеров зачастую недостаточно осведомлены о рисках, связанных с применением технологий социальной инженерии [2. С. 31].

Социальная инженерия, направленная на манипуляцию человеческими эмоциями и поведением, позволяет киберпреступникам эффективно распределять задачи и роли внутри своих групп. Например, один участник может специализироваться на фишинге – искусстве обмана для получения конфиденциальной информации, тогда как другой – на технической поддержке атак, например, создании вредоносных компьютерных программ. Такое разделение ролей повышает эффективность операций, поскольку каждый участник группы концентрируется на своей задаче.

– **Неправомерный доступ к учетным записям в социальных сетях и электронным почтовым ящикам.**

Такие преступники чаще всего действуют самостоятельно из корыстных мотивов или с целью проверки своих умений, пол мужской, разброс по возрасту большой 16–40 лет, но четкого разграничения по уровню образования и социальному статусу не имеется, по характеру зажатые и стеснительные, реальному общению предпочитают виртуальное [9. С. 27–28].

– **DDoS-атака** (от англ. Denial of Service – отказ в обслуживании) – атака на систему, например сайт, в виде большого количества фиктивных запросов, что должно привести к отказу в доступе к системе обычным пользователям.

Преступники данной группы также действуют самостоятельно из корыстных мотивов, чаще всего это мужчины 20–40 лет, безработные, без высшего и

специального образования в сфере ИТ, в браке не состоят, не общительные и замкнутые, то есть виртуальный мир для них ближе реального [9. С. 28–29].

2. От уровня навыков киберпреступника в ИТ сфере.

В научной литературе существуют исследования посвященные классификации киберпреступников в зависимости от их уровня владения компьютерной техникой и навыков программирования.

Так М. В. Жижина и Д. В. Завьялова предлагают выделить три группы субъектов преступлений в сфере компьютерной информации:

– **Лица с различным уровнем навыков в ИТ сфере, которые не ведут систематической преступной деятельности.**

Как указывают авторы это преступники, действующие в силу обстоятельств. Обычно такие лица ранее не были замечены в преступной деятельности и не связаны с криминальным миром [5. С. 154].

– **Лица с низким или средним уровнем навыков в ИТ сфере, которые ведут систематическую преступную деятельность.**

Такие лица обладают низкими или средними навыками в ИТ сфере, и как следствие плохо понимают работу программного кода. В связи с этим в своей преступной деятельности используют уже готовые технические решения, а не разрабатывают программное обеспечение специально под определенную жертву [5. С. 154].

– **Лица с высоким уровнем навыков в ИТ сфере, которые ведут систематическую преступную деятельность.**

Участники данной группы обладают профессиональными знаниями и навыками, чаще всего имеют узкую специализацию [5. С. 155–156].

Исследования в области киберпреступности показывают, что мотивация киберпреступников может быть весьма разнообразной и сложной [8. С. 258]. Одной из ключевых причин, способствующих вовлечению в киберпреступную деятельность, является финансовая выгода, экономические стимулы играют решающую роль в выборе пути киберпреступления. Преступники, желая получить быстрый доход, могут использовать различные методы, такие как фишинг, кража личных данных и проведение атак с целью вымогательства. Корыстные мотивы чаще характерны для представителей второй и третьей группы вышеперечисленной классификации, то есть для преступников ведущих систематическую преступную деятельность, для которых она является основным источником дохода. В то же время, некоторые киберпреступники могут быть мотивированы местью, хулиганскими, идеологическими или политическими целями, такими как протест против системной несправедливости или стремление подорвать политические режимы [5. С. 154–156].

3. От демографических признаков.

Согласно данным отчета Судебного департамента при Верховном Суде РФ о демографических признаках осужденных за преступления в сфере компьютерной информации (статьи 272–274.2 УК РФ) за 2023 г. соотношение киберпреступников распределено следующим образом:

– *по половому признаку:*

– мужчины – 71,5 %;

– женщины – 28,5 %.
– *по возрасту:*
– в возрасте от 18 до 24 лет – 42,3 %;
– в возрасте 25–29 лет – 18,0 %;
– в возрасте 30–49 лет – 35,7 %;
– в возрасте 50 лет и старше – 3,9 %.
– *по уровню образования:*
– обладатели высшего профессионального образования – 32,7 %;
– среднего профессионального образования – 41,4 %;
– среднего общего образования – 20,7 %;
– с основным общим, начальным, либо без образования – 5,1 %.
– *по месту жительства:*
– постоянные жители данной местности – 96,1 %;
– другие жители иной местности – 3,9 %;
– *по роду занятий (социальному положению):*
– рабочие – 25,8 %;
– государственные и муниципальные служащие – 2,7 %;
– служащие коммерческой или иной организации – 35,1 %;
– лица, осуществляющие предпринимательскую деятельность или участвующие в предпринимательской деятельности – 3,3 %;
– учащиеся и студенты – 1,5 %;
– нетрудоспособные (неработающие) – 1,2 %;
– трудоспособные лица без постоянного источника дохода – 16,8 %;
– иные сотрудники правоохранительных органов, в том числе органов прокуратуры – 3,0 %;
– лица прочих занятий – 10,5 %.

Проанализировав данные официальной статистики можно сделать вывод, что киберпреступником преступлений в сфере компьютерной информации чаще всего выступают местные жители мужчины в возрасте от 18 до 24 лет либо от 30 до 49 лет, обладающие средним профессиональным либо высшим профессиональным образованием, по роду занятий служащие коммерческой или иной организации либо рабочие [7].

Думаем верным согласиться с М. В. Жижиной и Д. В. Завьяловой в том, что по причине высокой латентности данных категорий преступлений официальная статистика не в полной мере отражает реальную картину [5. С. 153–154]. Это связано как с высоким уровнем профессионализма киберпреступников, их осторожностью и скрытностью при совершении преступлений, возможностью сохранения анонимности в сети, так и с тем, что часто потерпевшие от киберпреступлений не заявляют о преступлениях либо по причине стыда, что были обмануты, либо по причине неуверенности в положительном исходе расследования [6. С. 150].

Заключение. Одним из важных выводов является возможность выделения различных типов лиц, совершающих преступления в сфере компьютерной информации, в зависимости от ряда факторов. Во-первых, типология может быть основана на способах совершения преступления. Во-вторых, важным критерием является уровень ИТ-компетенций преступников, варьирующийся от низких

навыков у новичков до профессионалов, обладающих глубокими техническими знаниями и умениями. В-третьих, демографические признаки, такие как возраст, пол, образование и социальное положение, также оказывают влияние на криминальное поведение в цифровой среде.

Таким образом, более глубокое понимание характеристик преступников в сфере компьютерной информации открывает возможности для разработки целенаправленных профилактических и правоприменительных мер. Создание эффективных программ профилактики, повышение уровня киберграмотности населения и укрепление законодательной базы станут важными шагами в противодействии этой форме преступности.

Список литературы

1. Бабурин В. В., Карабеков К. О. Криминологическая характеристика личности киберпреступника в Российской Федерации и Республике Казахстан // Психопедагогика в правоохранительных органах. – 2024. – Т. 29, № 1(96). – С. 113–119. DOI: 10. 24412/1999-6241-2024-196-113-119

2. Бегишев И. Р., Берсей Д. Д. Генезис криминальной социальной инженерии // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 6. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – С. 23–34. EDN: IDLEUI. DOI: http://dx.doi.org/10.21202/978-5-8399-978-5-8399-0819-2_476

3. Григорян С. А. Особенности личности современного «киберпреступника» // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2022. № 8(147). С.103–106.

4. Евдокимов К. Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) // Сибирский юридический вестник. – 2011. – № 1(52). – С. 86–90.

5. Жижина М. В., Завьялова Д. В. Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников) // Актуальные проблемы российского права. – 2022. – Т. 17, № 5(138). – С. 149–158. DOI: 10.17803/1994-1471.2022.138.5.149-158

6. Майоров А. В. Влияет ли цифровизации на виктимизацию в современном обществе? // Виктимология. – 2022. – Т. 9, № 2. – С. 148–156. DOI: 10.47475/2411-0590-2022-19202

7. Отчет о демографических признаках осужденных по всем составам преступлений Уголовного кодекса Российской Федерации // URL: http://www.cdep.ru/userimages/sudebnaya_statistika/2023/k5_1-svod_vse_sudy-2023.xls

8. Поляков В. В., Попов Л. А. Особенности личности компьютерных преступников // Известия АлтГУ. – 2018. – № 6(104). – С. 256–259. DOI: 10.14258/izvasu(2018)6-49

9. Родивилин И. П. Типологизация лиц, совершающих преступления в сфере компьютерной информации, по способу преступного деяния // Научный вестник Омской академии МВД России. – 2017. – № 4(67). – С. 25–29.

10. Янгаева М. О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. – 2021. – № 1(42). – С. 133–138.

11. Holt T. J., Bossler A. M., Seigfried-Spellar K. C. Cybercrime and Digital Forensics. Introduction. Second Edition. – Abingdon, Oxon : Routledge, 2018.

А. С. Фартушнова,
сотрудник ООО «Отель»

ПРАВОВЫЕ АСПЕКТЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ: РЕАЛИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Аннотация. Сегодня и уже немало лет вопросы правового оснащения кибербезопасности не просто сохраняют свою актуальность, но и в отдельных аспектах своей сферы продолжают отставать от реальных темпов развития цифровых систем. Вместе с тем «цифра» сегодня максимально внедрена во все среды жизни человека. Оцифровываются изображения, текстовая информация о человеке, голосовые тонкости, детали движений и практически все, что связано с человеком и в полной мере идентифицирует его. Все эти возможности ограничиваются во всех случаях, прежде всего, техническими средствами и, как следствие, не ограничены в потенциальном риске, в лучшем случае, утраты, а в худшем – несанкционированной передачи и/или распространения и невосполнимых злоупотреблений с данными.

Ключевые слова: безопасность, право, цифра, цифровые решения, технологии, киберпространство, возможности, перспективы

LEGAL ASPECTS OF DIGITAL SECURITY: REALITIES AND DEVELOPMENT PROSPECTS

Abstract. Today and for many years now, the issues of legal framework for cybersecurity not only remain relevant, but also in certain aspects of their sphere continue to lag behind the actual pace of development of digital systems. At the same time, "digital" today is maximally implemented in all environments of human life. Images, text information about a person, voice subtleties, details of movements and almost everything that is associated with a person and fully identifies him are digitized. All these possibilities are limited in all cases, first of all, by technical means and, as a result, are not limited in potential risk, at best, of loss, and at worst – unauthorized transfer and/or distribution and irreparable abuse of data.

Keywords: security, law, digital, digital solutions, technologies, cyberspace, opportunities, prospects