Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2019. – Т. 5 (71). № 4. – С. 139-145.

УДК 303.6

ФАКТОРЫ ПРЕСТУПНОСТИ В СФЕРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Бугаев В. А., Чайка А. В.

Крымский федеральный университет им. В. И. Вернадского

В статье рассмотрен криминологический аспект преступлений в сфере компьютерных технологий. Дан анализ круга причин и условий (факторов), способствующих совершению преступлений в сфере компьютерных технологий. Проведено криминологическое исследование личности киберпреступника. Обобщены и проанализированы мнения ученых по данной тематике, сделаны соответствующие теоретические выводы.

Ключевые слова: компьютерные технологии, факторы, способствующие совершению преступлений, их причины и условия, интернет, интернет-преступления, личность преступника.

Уровень развития инновационных технологий, сети Интернет, компьютерных и беспроводных сетей растет из года в год. Все большее количество людей начинает использовать различные платформы, электронные средства и даже криптовалюты, размещает персональные данные в социальных сетях. Компании ведут свою деятельность за счет полностью автоматизированного производства и управляемых человеком синхронизированных систем, которые производят обработку и хранение информации на серверах. Развитие уровня потребления различных компьютерных услуг приводит к активизации злоумышленников, специализирующихся на проникновениях в компьютерные сети, хищениях информации и денежных средств с электронных счетов. У преступников растет интерес к киберпространству, увеличивается количество взломов целых платформ и личных аккаунтов, а также утечек данных со стороны крупных IT-компаний.

Согласно отчету, опубликованному Генпрокуратурой в 2017 г., число преступлений в сфере информационно-телекоммуникационных технологий увеличилось на 37%. При этом доля таких преступлений от числа всех зарегистрированных в России составляет 4,4%: это почти каждое 20-е преступление [1], а латентность – шести-семикратная.

По мнению криминологов, количество совершаемых преступлений в сфере компьютерных технологий неуклонно растет. Однако этот процесс не находит отражения в официальной статистике в силу самых разных причин. Необходимо отметить, что несовершенство статистического учета позволяет проследить динамику лишь части преступлений в сфере компьютерных технологий, причем не самой значимой, и не дает объективной картины состояния преступности в этой сфере (табл.1).

Таблица 1
Динамика преступлений в сфере компьютерных технологий в РФ в 2015-2017 гг.

Преступления, предусмотренные	Годы		
	2015	**2016**	**2017**
ст. 272 УК РФ	1395	1443	1079
ст. 273 УК РФ	970	1124	802
ст. 274 УК РФ	13	3	2

Раскрываемость даже этой малой части выявленных преступлений в сфере компьютерных технологий не превышает 5% [2, с. 41].

Чтобы противостоять преступности в сфере компьютерных технологий, необходимо четко представлять причины и условия, способствующие совершению этой категории преступлений.

Вопрос о причинах и условиях преступности вообще и преступности в сфере компьютерных технологий в частности, относится к одному из самых сложных и противоречиво разрешаемых в мировой и отечественной науке.

Преступность в сфере компьютерных технологий, с одной стороны, порождается теми же причинами и условиями, что и преступность вообще. С другой стороны, она имеет свои сугубо специфические причины и условия вследствие ее особенностей. Однако в криминологии при наличии общепринятых подходов к концепции причин преступности вообще и компьютерной в частности, имеется ряд проблем, не позволяющих эффективно осуществлять предупреждение такого рода преступлений.

Каковы же причины и условия, т.е. факторы преступности в сфере компьютерных технологий?

Представляется, что все факторы преступности в сфере компьютерных технологий можно подразделить на три категории.

1. Факторы преступности в сфере компьютерных технологий, в информационных сетях, информационной среде и ее инфраструктуре.

В мире и стране наблюдается рост информационного обмена, однако этот рост не обеспечивается соответствующим уровнем защиты информации, что создает благоприятные возможности для совершения преступлений в сфере компьютерных технологий путем как «внешнего», так и «внутреннего» воздействия. Не всегда надлежаще осуществляется защита информации в зависимости от ее категории и общественной значимости. При обработке компьютерной информации можно наблюдать отступление от технологических режимов обработки информации. Нарушаются правила работы с охраняемой законом компьютерной информацией.

К факторам преступности в сфере компьютерных технологий, относительно информационной среды, можно выделить:

-повсеместность использования соответствующей инфраструктуры, сетей, программ, оборудования, а также растущее во всем мире и в России количество пользователей программно-технических средств;

-доступность компьютерных технологий;

-возрастающую зависимость современных технологий от компьютерных систем и средств телесвязи;

-широкое использование зарубежного программно-технического обеспечения, операционных систем, а также технических компонентов.

Информационная инфраструктура — это совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории РФ, а также на территориях, находящихся под юрисдикцией РФ или используемых на основании международных договоров РФ.

К факторам преступности в сфере компьютерных технологий, касающимся информационной инфраструктуры, следует отнести: отсутствие должного контроля со стороны администрации за деятельностью работников, задействованных в обработке компьютерной информации; отсутствие должного контроля со стороны государства за СМИ и российским сегментом сети «Интернет»; наличие закрытых анонимных информационно-телекоммуникационных сетей, посредством которых совершаются самые разнообразные преступления.

2. Факторы, относящиеся к особенностям преступности в сфере компьютерных технологий имеют: организованный и профессиональный характер значительной части преступности; весьма скрытный характер преступлений, в совокупности составляющих преступность в сфере компьютерных технологий, в силу их анонимности, удаленности и сложности инфраструктуры, неосведомленности потерпевших; глобальный и трансграничный характер преступности в сфере компьютерных технологий.

Так, среди этих факторов:

- преступник может находиться в одной стране, преступление совершать в другой, а последствия преступления могут наступать в третьей, что затрудняет противодействие преступности в рамках одного государства и даже совокупности государств;

- возможность при совершении преступлений в сфере компьютерных технологий одновременно атаковать сотни и тысячи компьютеров, находящихся как в одной, так и в разных странах;

- многообразие способов совершения преступлений в сфере компьютерных технологий, возможность совершения преступлений в автоматических режимах и объединения ресурсов пользователей помимо их желания и воли;

- невозможность предотвращения и пресечения преступлений в сфере компьютерных технологий традиционными способами;

- отсутствие какой-либо достоверной статистики преступности в сфере компьютерных технологий, ее состояния, структуры и динамики;

- чрезвычайно широкая распространенность преступлений в сфере компьютерных технологий и высоколатентный характер данных преступлений, обусловленный самыми разными причинами;

- неустоявшаяся судебно-следственная и прокурорская практика, отсутствие научно обоснованных методических рекомендаций по раскрытию, расследованию и квалификации такого рода преступлений;

- чрезвычайно высокая скорость совершения преступного воздействия на среду влияния и практическое отсутствие материальных следов;

- отсутствие восприятия последствий обществом как последствий криминального деяния.

3. Факторы преступности в сфере компьютерных технологий, относящиеся к субъектам общественных отношений, возникающих по поводу обеспечения информационной безопасности:

-несоответствие системы международных стандартов в области компьютерной техники, связи и информационной безопасности требованиям времени;

-отсутствие должного международно-правового сотрудничества в сфере противодействия преступности в сфере компьютерных технологий;

-отсутствие комплексных государственных мер, направленных на противодействие преступлениям в указанной сфере;

-недостатки действующего информационного законодательства, страдающего отсутствием системности и планомерности развития и законодательного регулирования;

-несоответствие уголовного законодательства существующим общественно опасным явлениям в информационной сфере;

-несовершенство действующего уголовного законодательства;

-несовершенство социальных, юридических и политических структур, уровень развития которых значительно отстает от уровня развития компьютерных и телекоммуникационных технологий;

-недостаточное правовое, научное, организационно-техническое и правоприменительное противодействие преступности в сфере компьютерных технологий;

-недостаточная осведомленность общества об уязвимости компьютерных систем и необходимость осуществления действенных мер безопасности;

-неадекватное отношение общества к преступности в сфере компьютерных технологий в целом и компьютерным преступникам в частности;

-недостаточное правовое воспитание населения, особенно подрастающего поколения;

-участие в ряде стран специальных государственных структур, в незаконном проникновении в компьютерные сети, в геополитических и военно-стратегических целях этих государств;

-высочайшая степень свободы, ввиду отсутствия эффективных предохранителей на каналах общения в киберпространстве.

Для успешного устранения этих факторов, а также выявления, раскрытия и предупреждения преступлений в сфере компьютерных технологий необходимым элементом является криминологическое исследование личности преступника.

Анализируя труды российских ученых в области изучения личности компьютерного преступника (например, Попова А. Б., Макушева Д. И., Дьякова В. В.), можно отметить тот факт, что среди социально-демографических характеристик личности, наиболее свойственных для киберпреступников, выделяют: пол, возраст, образование, материальное положение, род занятий. Рассмотрим каждое из них отдельно и попытаемся сформировать социально-демографический портрет киберпреступника.

В криминологической науке имеется единое мнение о том, что киберпреступления совершаются преимущественно мужчинами, что подтверждает в своем исследовании Макушев Д. И. [3, с. 23]. Появляющиеся в СМИ случаи совершения дан-

ной группы преступлений женщинами скорее являются исключительными случаями, однако последнее время прослеживается тенденция роста доли женщин, в структуре преступности указанного вида.

Дьяков В. В. считает, что положительная динамика роста женской киберпреступности состоит в профессиональной ориентации некоторых специальностей (секретарь, бухгалтер, контролер, делопроизводитель, кассир и другие) по использованию в работе средств компьютерной техники [4, с. 130]. Это может быть обусловлено тем, что среди женщин чаще встречаются так называемые «белые» хакеры, не причиняющие значительный вред обществу.

В криминологической науке существует мнение о том, что компьютерные преступления в основном совершаются двумя возрастными категориями: от 16 до 25 лет, и от 18 до 24 лет [4, с. 130]. Однако практика показывает, что компьютерные преступления могут совершаться лицами любого возраста. Это же подтверждается и некоторыми авторами в своих исследованиях [5, с. 99].

Следует отметить тенденцию понижения возраста киберпреступников. Получаемые в школе базовые знания информатики, любопытство, развитие сети Интернет, появление множества обучающих и вспомогательных материалов в открытом доступе, относительно доступная стоимость компьютера, выводит совершение киберпреступлений на новый, более доступный уровень.

Однако для этой возрастной группы речь идет о совершении невысокоинтеллектуальных преступлений, для учинения которых требуются специальные знания и навыки (языки программирования, особенности передачи информации, протоколы взаимодействия, уязвимости сетей и программного обеспечения).

В то же время встречаются исключения из этой тенденции. Юные хакеры сегодня могут получить доступ на просторах Рунета ко множеству пошаговых инструкций для мелких кибердеяний, начиная от DDOS-атак и взломов устройств (например, джейлбрейк продукции компании Apple) до более серьезных преступлений. Хакеры зачастую представляют собой единое коммьюнити, которое охотно делится своими успехами и путями их достижения. Совершив мелкую шалость и получив положительный результат, хакеры зачастую повышают планку совершаемого правонарушения, выбирая в качестве объектов своих атак более квалифицированные компании с большим уровнем защиты. Как правило, именно такая схема генезиса личности киберпреступника наблюдается в последнее время.

Учитывая все вышесказанное, можно сделать вывод о том, что сейчас и в дальнейшем будет происходить снижение возраста киберпреступников и лица в возрасте от 16 до 25 лет будут наиболее активной группой, совершающей данные преступления. Эту тенденцию отразил в своем исследовании Попов А. Б., разделивший компьютерных преступников на 3 возрастные группы: начинающие – 15-25 лет; закрепившиеся – 20-25 лет; профессионалы – 25-45 лет [6, с. 411].

Образование киберпреступника существенно отличается, в зависимости от категории совершаемых ими правонарушений. Для незначительных деяний достаточно среднего образования, и не требуется серьезных технических знаний. Совершение незаконных крупных финансовых операций, вторжение в чужие компьютерные сети, создание и внедрение вредоносного программного обеспечения требует высокого уровня подготовки.

Практически все авторы сходятся во мнении о том, что уровень материального обеспечения киберпреступников или их семей в России выше среднего. Такая тенденция наблюдается в последние 15 лет в связи со стремительным падением цен на персональные компьютеры и повсеместным внедрением широкополосного вещания. Ранее к числу хакеров могли относиться лишь обеспеченные лица или лица из богатых семей, поскольку высокопроизводительный компьютер являлся роскошью, а Интернет и вовсе отсутствовал в большинстве домов. Но научно-технический прогресс меняет эту ситуацию для «начинающих» хакеров практически кардинально.

В целом, род занятия не имеет принципиального значения для киберпреступников, поскольку они совершают эти деяния, как в рабочее, так и нерабочее время. Как показывает практика, это либо безработные, добывающие средства к существованию за счет работы на фрилансе или за счет хищения чужих денежных средств с банковских счетов, либо лица, которые трудятся в сфере информационных технологий (зачастую это системные администраторы локальной вычислительной сети). Подобную позицию поддерживает и Дьяков В. В. [4, с. 130].

Семейный статус киберпреступников не оказывает существенного влияния на совершаемые ими преступления. Соотношение киберпреступников составляет 60% к 40% в пользу тех, кто не состоит в зарегистрированном браке [3, с. 23]. Этот факт может быть обусловлен тем, что зачастую киберпреступники сами по себе отстраненные личности, предпочитающие общение с представителями своего коммьюнити и не находящие собеседников среди рядовых граждан. Также стоит отметить, что киберпреступники чаще всего молодые люди, о чем уже было указано, что несомненно влияет на их семейное положение. Чаще заключение брака может быть зафиксировано у хакеров-профессионалов старше 25 лет. Причем, зачастую, такие браки могут быть заключены с представителями того же рода деятельности ввиду понимания их жизненных устоев и принципов (женщины-хакеры чаще встречаются именно в группе «профессионалов»).

Иные признаки (социальное положение, специальность, наличие постоянного места жительства, гражданство) не имеют ключевого значения для формирования социально-демографического портрета личности преступника, поскольку для них не представляется возможным определить тенденцию, свойственную для данной группы преступников.

Исходя из проанализированных выше положений можно сделать вывод о том, что киберпреступник – это преимущественно неженатый мужчина в возрасте от 16 до 25 лет, материально обеспеченный (с достатком на уровне среднего или выше среднего), обладающий специальными знаниями и навыками в сфере информационно-коммуникационных технологий и занятый в сфере информационных технологий.

Таким образом, рост совершения преступлений в сфере компьютерных технологий связан с развитием, доступностью и популярностью цифровых технологий. Только лишь воздействуя на весь комплекс факторов преступности в указанной сфере, можно значительно снизить ее уровень. Приоритет в этой деятельности должен отдаваться воспитанию человека, формированию его личности, привитию ему чувства коллективизма и ответственности, нейтрализации негативных свойств его личности.

Список литературы

1. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий. URL: http://genproc.gov.ru/smi/news/genproc/news-1431104 (дата обращения 01.10.2019). – Текст электронный.
2. Гилинский Я. Криминология: теория, история, эмпирическая база, социальный контроль. Авторский курс / Я. Гилинский. – СПб. : ООО Издательский Дом «Алеф-Пресс», 2018. – 352 с.
3. Макушев Д. И. Криминологическая характеристика личности киберпреступника / Д. И. Макушев // Актуальные проблемы гуманитарных и естественных наук. – 2016. – № 1-3. – С.23-29.
4. Дьяков В. В. О личности преступника, как компоненте системы криминалистической характеристики преступления в сфере компьютерной информации / В. В. Дьяков // Бизнес в законе: экономико-юридический журнал. – 2008. – № 2. – С. 129-131.
5. Мещеряков В. А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ / В. А. Мещеряков. – Воронеж: ВГУ, 2001. – 176 с.
6. Попов А. Б. Криминологическая характеристика личности преступника, совершающего преступление, предусмотренное ст. 272 УК РФ / А. Б. Попов // Вестник ТУ. – 2009. – № 8. – С.411-413.

Bugaev V. A., Chaika A.V. Computer crime: the criminological aspect / V. A. Bugaev, A. V. Chaika // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2019. – T. 4 (72). № 4. – P. 139-145.

In the article the criminological aspect of crimes is considered in the field of computer technology. The analysis of the range of reasons and conditions (factors) contributing to the commission of crimes in the field of computer technology is given. The criminological research of the identity of the cybercriminal is conducted. The opinions of scientists are generalized and analyzed on this subjects, the corresponding theoretical conclusions are done.

Keywords: the factors promoting committing of crimes in the field of computer technologies, personality of criminal.

Spisok literatury

1. O prestupleniyah, sovershaemyh s ispol'zovaniem sovremennyh informacionno-kommunikacionnyh tekhnologij. URL: http://genproc.gov.ru/smi/news/genproc/news-1431104 (data obrashcheniya 01.10.2019). – Tekst elektronnyj.
2. Gilinskij YA. Kriminologiya: teoriya, istoriya, empiricheskaya baza, social'nyj kontrol'. Avtorskij kurs / YA. Gilinskij. – SPb. : OOO Izdatel'skij Dom «Alef-Press», 2018. – 352 s.
3. Makushev D. I. Kriminologicheskaya harakteristika lichnosti kiberprestupnika / D. I. Makushev // Aktual'nye problemy gumanitarnyh i estestvennyh nauk. – 2016. – № 1-3. – S.23-29.
4. D'yakov V. V. O lichnosti prestupnika, kak komponente sistemy kriminalisticheskoj harakteristiki prestupleniya v sfere komp'yuternoj informacii / V. V. D'yakov // Biznes v zakone: ekonomiko-yuridicheskij zhurnal. – 2008. – № 2. – C. 129-131.
5. Meshcheryakov V. A. Prestupleniya v sfere komp'yuternoj informacii: pravovoj i kriminalisticheskij analiz / V. A. Meshcheryakov. – Voronezh: VGU, 2001. – 176 s.
6. Popov A. B. Kriminologicheskaya harakteristika lichnosti prestupnika, sovershayushchego prestuplenie, predusmotrennoe st. 272 UK RF / A. B. Popov // Vestnik TU. – 2009. – № 8. – C.411-413.