УДК 343.92

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Лев ЛЕФТЕРОВ,
адъюнкт кафедры уголовного права и криминологии
Одесского государственного университета внутренних дел

АННОТАЦИЯ

В статье рассматриваются актуальные вопросы противодействия киберпреступлениям. Особое внимание уделено незаконным операциям по завладению имуществом путем обмана или злоупотреблением доверия, механизм совершения которых невозможен без использование электронно-вычислительных машин. В частности, проводится комплексное криминологическое исследование мошенничества, совершенного с использованием электронно-вычислительной техники. Приведены некоторые данные статистики совершения компьютерных мошенничеств как на территории Украины, так и в мире.

Ключевые слова: компьютерное мошенничество, криминологическая характеристика, электронно-вычислительная техника, злоупотребление доверием, киберпреступления.

CRIMINOLOGICAL CHARACTERISTICS OF FRAUD, DONE BY THE USE OF ELECTRONIC COMPUTER ENGINEERING

Lev LEFTEROV,
Adjunct at of the Department of Criminal Law and Criminology
of Odessa State University of Internal Affairs

SUMMARY

The article raises topical issues of countering cybercrime. Particular attention is paid to illegal operations to seize property through deception or abuse of trust, the mechanism of which is impossible without the use of electronic computers. In particular, a comprehensive criminological study of fraud committed using electronic computers is conducted. There are some data on the statistics of computer fraud, both in Ukraine and in the world.

Key words: computer fraud, criminological characteristics, computer technology, abuse of trust, cybercrime.

Постановка проблемы. В июне 2017 года на территории Украины было зафиксировано распространение новой модификации вредоносного программного обеспечения, в результате чего была нарушена деятельность ряда государственных учреждений, а также предприятий частного сектора. По информации Департамента киберполиции Национальной полиции Украины, за немногочисленное время работы указанного компьютерного вируса в органы Национальной полиции Украины поступило более 1000 обращений о несанкционированном вмешательстве в работу электронно-вычислительных машин, которые привели к блокированию информации и сбоям в работе компьютерной сети [6].

Указанные события спровоцировали активные действия в изучении проблем компьютерной преступности, рассмотрения стратегий и концепций обеспечения кибербезопасности на государственном уровне. Основы национальной безопасности, а также бесперебойная работа объектов критической инфраструктуры безусловно является главным направлением государства. Однако следует отметить, что

Интернет-мошенничества, совершенные с использованием электронно-вычислительной техники и электронных платежных систем несут в себе угрозу не только для физических лиц, но и для государственных предприятий, а ущерб от них сопоставим с национальными масштабами.

Актуальность темы исследования. По данным украинской межбанковской ассоциации членов платежных систем ЕМА, только во втором квартале 2016 года от Интернет-мошенничеств пострадал каждый сотый держатель платежных карт в Украине, «доход» от незаконных действий составил почти 340 миллионов гривен (11,2 миллионов Евро) [7]. Данная статистика отображает как результат недостаточного изучение криминологических особенностей указанной категории преступлений, так и недостатки украинского законодательства, которое все еще находится на этапе адаптации к современным тенденциям информационно-технического развития государства. Данный факт подтверждает актуальность рассматриваемой темы. Научные исследования отдельных аспектов борьбы с Интернет мошенничеством и киберпреступностью в общем проводились И. Г. Богатыревым, А. А. Комаровым, А. К. Лебедевым, А. Е. Корыстиным, А. А. Жмиховым, А. С. Малаховым, А. С. Дубиным, однако на современном этапе изучения криминологических особенностей мошенничества, совершенного с использованием электронно-вычислительной техники, существует ряд ранее неисследованных вопросов, в том числе анализ факторов и переменных, влияющих на динамику развития указанного вида преступлений в условиях современного развития борьбы с киберпреступностью.

Целью статьи является осуществление криминологической характеристики мошенничеств, совершенных с использованием электронно-вычислительной техники, анализ данного вида преступности, ее территориальные особенности и региональные структуры.

Изложение основного материала. Как известно, мошенничество, совершенное с использованием электронно-вычислительной техники, является не только видом киберпреступления, но и весомой частью общей преступности. Информационно-аналитическое обеспечение деятельности по борьбе с преступностью – исходный, необходимый ее элемент. Соответственно общими задачами анализа преступности в криминологии является выявление ее закономерностей с тем, чтобы перейти к анализу закономерностей ее детерминации, причинности, определить закономерности ее подверженности различным воздействиям и соответственно правильно построить борьбу с преступностью в конкретных условиях территории (государства, региона) и времени.

При криминологическом изучении преступности выявляются:

– степень ее общей распространенности и общественной опасности в конкретных условиях места и времени в целях оценки ее состояния и тенденций, определения направлений борьбы с преступностью;

– социальные характеристики преступности, указывающие на особенности ее порождения и функционирования (мотивация, социальная направленность, социально-групповая, социально-отраслевая, социально-территориальная распространенность), в целях разработки конкретных предупредительных мер;

– собственные, внутренние характеристики преступности (устойчивость, активность, организованность) в целях совершенствования правоохранительной деятельности и мер предупреждения рецидива преступлений, усиления организованных начал в преступности [4, с. 91].

Согласно части 3 статьи 190 Уголовного Кодекса Украины – мошенничество, совершенное путем незаконных операций с использованием электронно-вычислительной техники, предусматривает наказание в виде лишения свободы на срок от трех до восьми лет [1, ст. 190]. Указанная норма в полной мере дает уголовно-правовое понятие действиям, которые относятся к киберпреступности.

Прежде всего необходимо рассмотреть абсолютные показатели количества мошенничеств, которые относятся к категории киберпреступлений, а именно, преступления, которые предусмотрены ч. 3, ст. 190 УК Украины [1, ст. 190]. Анализ информации проводился согласно официальным данным статистики Генеральной прокуратуры в виде единого отчета по уголовным правонарушениям, зарегистрированным в Единый реестр досудебных расследований на территории Украины в период времени с 2013 по 2018 года [8].

Согласно отчету, в период времени с января 2013 до июня 2018 года на территории Украины, зафиксировано и внесено в Единый реестр досудебных расследований 19 654 фактов мошенничества, совершенных с использованием электронно-вычислительной техники (предусмотренные ч. 3 ст. 190 УК Украины). Новизна данного вида преступности, а также методы совершения указанной категории мошенничеств влияют на отсутствие статистических данных за более длительный период времени, что в свою очередь исключает возможность качественного отслеживания динамики преступности по годам. Однако если детально изучить изменение показателей можно установить научно объяснимые закономерности. Так в 2013 году на территории Украины зафиксировано и внесено в Единый реестр досудебных расследований 3320 факта, из которых установлены лица и объявлено о подозрении по 1047 уголовным производствам. В 2014 году зафиксировано и внесено в Единый реестр досудебных расследований 2740 факта, из которых установлены лица и объявлено о подозрении по 1241 уголовным производствам. В 2015 году зарегистрировано 3633 уголовных производства, из которых раскрыты 1318. В 2016 и 2017 году на территории Украины открыто 3578 и 4808 уголовных производств, из которых объявлено о подозрении по 878 фактам в 2016 году и 2103 делам в 2017 году соответственно. По состоянию на 1 июня 2018 года, за 5 месяцев на территории Украины выявлено и зарегистрировано 1575 уголовных производств и раскрыто 557 преступлений [8].

Как видно из выше представленных показателей, количество раскрытых преступлений на порядок ниже количества зарегистрированных. Данный факт, не является аномальным, так как преступность в большинстве случаев находится «на шаг впереди» от правоохранительных органов. Однако, главной особенностью динамики ком-

пьютерного мошенничества в Украине является его постепенное увеличение, но не по прямой, а по кривой линии. Что означает увеличение количества фактов, зарегистрированных в Едином реестре досудебных расследований в 2018, по сравнению с 2013 годом. Но увеличение происходило пропорционально временным снижениям преступности в 2014, 2016 годах. Чем обуславливаются данные изменения?

Как известно киберпреступления являются одним из самых сложных деяний в подготовке, совершении, а также в методах и тактике документирования их правоохранительными органами. Если объединить указанные сложности с механизмами обмана и злоупотребления доверием, предусмотренные мошенничеством, в арсенал киберпреступников поступает несчетное количество способов для совершения незаконных действий, с использованием компьютерной техники, специальных технических инструментов для работы с платежными данными, а также Интернета (как виртуальной среды для совершения преступлений).

Как было упомянуто ранее, хоть правоохранительная система не успевает за динамикой развития и совершения мошенничеств с использованием компьютерной техники, на месте она тоже не стоит.

В ходе проведенного нами изучения и анализа данных из открытых источников можно выявить основные переменные и факторы, которые влияют на снижение уровня преступности (на основании статистики 2013-2018 года):

1. Правовые и законодательные. Так на стороне противодействия киберпреступности находится целая государственная система в виде Законодательной и Исполнительной ветвей власти, со своими нормами права (направленными на противодействие и оказание содействия в борьбе с данной категорией кибепреступлений). Влияние на преступность оказывают даже малые изменения в правовых нормах, или процессах реформирования государственных органов (в частности, образование в 2015 году подразделения киберполиции Национальной полиции Украины).

2. Частный сектор и банковская система также оказывают поддержку и борьбу с кибермошенничествами в рамках своих прав. Контролирование финансовых потоков играет не маловажную роль, особенно в мошенничествах, которые совершены с использованием систем удаленного банковского обслуживания. Так Государственная служба финансового мониторинга Украины, которая является центральным органом исполнительной власти и тесно связана с банковскими учреждениями: реализует государственную политику в сфере предотвращения и противодействия легализации (отмыванию) доходов, полученных преступным путем; собирает, обрабатывает и анализирует информацию о финансовых операциях, подлежащих финансовому мониторингу и другие финансовые операции; создает и обеспечивает функционирование единой государственной информационной системы в сфере предотвращения и противодействия легализации (отмыванию) доходов, полученных преступным путем, или финансированию терроризма [2]. Украинская межбанковская ассоциация членов платежных систем «ЕМА», которая была зарегистрирована еще в 1999 году, свою активную деятельность, направленную на предупреждение интернет-мошенничеств, ведет путем усовершенствования взаимодействия негосударственного и государственного секторов по вопросам противодействия платежным и другим финансовым правонарушениям, разработка, внедрение и эксплуатация программных продуктов, проектов для совместного использования и реализации подразделениями Национальной полиции, членами Ассоциации и другими участниками платежных систем, платежными учреждениями, платежными системами, системами перевода средств, другими участниками рынка платежей и кредитования, Государственной службой финансового мониторинга Украины, Национальным банком Украины и других [3, с. 2].

3. Профилактика и опыт. Основным, фактором, который исключает возможность компьютерных мошенников долгое время использовать одни и те же способы совершения преступлений, является профилактика, приобретенный опыт, проведение бесед, освещение в СМИ и так далее. Также не малую роль играют процессуальные и правовые прецеденты, которые используются во время расследования и документирования уголовных правонарушений органами досудебного расследования, прокуратуры и оперативными подразделениями по борьбе с кибепреступностью.

Другими словами, особенностями преступности в сфере мошенничества с использованием электронно-вычислительной техники, является ее развитие, связанное на прямую с повышением уровня противодействия.

Еще одним статистическим показателем является количество преступлений, совершенных в составе групп. В 2013 году предъявлено подозрение по 145 уголовным производствам, которые были совершены в составе группы (по предварительному сговору лиц, в составе организованной преступной группы или организации). В 2014 году – предъявлено подозрение по 57 уголовным производствам (низкий уровень связан с политическим кризисом в государстве в этот период времени), в 2015 – по 182, в 2016 – по 130, в 2017 – по 246 уголовным производствам. Как видно, данный показатель также, как и предыдущие статистические данные, имеет динамику, которая на прямую зависит от влияния переменных. Кроме того, объяснить факт увеличения совершенных преступлений указанной категории в составе группы можно криминологическими особенностями. Иными словами, для совершения определенных категорий мошенничеств с использованием высоких информационных технологий также необходимы силы в виде человеческого ресурса и уникальных знаний (в сфере информационных технологий, социальной инженерии, психологии, экономики, а в некоторых случаях: знания юриспруденции, методов и тактики работы правоохранительных органов). Именно поэтому мошенники все чаще объединяются в группы, в которых происходит распределения обязанностей и ролей в ходе подготовки и совершении уголовных правонарушений.

Для выявления региональных показателей была проанализирована статистика зарегистрированных дел в Едином реестре досудебных

расследований в 2017 году, каждой отдельно взятой административно-территориальной единицы (кроме регионов, временно не подконтрольных центральной власти). Из показателей видно, что основная доля преступности приходится на территорию города Киева (650 уголовных производств, зарегистрированных за отчетный период) и Одесской области (638 уголовных производств). Кроме того, не малое количество мошенничеств с использованием электронно-вычислительной техники зафиксировано на территориях оперативного обслуживания: Запорожской области (368 уголовных производства), Николаевской области (337 уголовных производства), Харьковской (207 уголовных производства) Днепропетровской (204 уголовных производства) и Львовской областей (148 уголовных производства). Различие в уровне структуре и динамике преступности неслучайны. Они связаны с демографическими, экономическими, социальными, культурными, организационными, национальными, экологическими, правовыми, регистрационными и другими особенностями той или иной местности (этнический состав населения, проживание большинства населения региона в городах или селах и т.д.). Поэтому изучение географии преступности имеет исключительное значение для сравнительной криминологии при анализе причин преступности и ее изменений, при выработке эффективных мер ее предупреждения [5, с. 108].

Так, принимая во внимание демографический фактор можно сделать вывод, что на динамику преступности данной категории влияет в первую очередь количество и плотность населения отдельно взятого региона. Согласно данным государственной службы статистики, средняя численность населения в г. Киеве в 2017 году составила 2 930 141 человек без учета миграций и временно посетивших столицу Украины. В Одесской области в 2017 году постоянная численность населения составила 2 384 796 человек (а также более 2,2 миллиона человек, которые посетили регион в курортный период и межсезонье). Кроме того, в данных регионах обусловлен повышенный уровень проникновения Интернета во многие сферы экономической и повседневной деятельности.

Если говорить о других факторах, которые главным образом влияют на киберпреступность в Украине, необходимо изучить другие дополнительные статистические данные. Принимая во внимание тот факт, что самым основным орудием компьютерного мошенничества является Интернет, целесообразно проанализировать показатели развития и проникновения Интернета в Украине. Так в 2018 году Интернет ассоциацией Украины (ИнАУ) совместно с холдингом Factum Group Ukraine проведено исследование репрезентативное населению Украины в возрасте от 15 лет и старше [9]. По результатам проведенных исследований установлено, что динамика проникновения Интернета, начиная с 2010 года, имеет следующие показатели:

– 2010 год – 28 % населения страны;
– 2011 год – 39 %;
– 2012 год – 50%;
– 2013 год – 53%;
– 2014 год – 57%;
– 2015 год – 58%;
– 2016 год – 63%;
– 2017 год – 63%;
– 2018 год – 65 %.

При этом 65% населения (21,35 миллионов) являются регулярными пользователями, 67% населения (21,9 миллиона) имеют подключение домашнего Интернета.

Социально-демографическая структура «регулярных» Интернет-пользователей выглядит таким образом:

– пользователи Интернета мужчины 48%;
– женщины – 52%, от общего количества.

Возрастная категория пользователей:

– 15-24 лет – 18%;
– 25-34 лет – 28%;
– 35-44 лет – 23%;
– 45-54 лет – 16%;
– 55-64 лет – 11%;
от 65 лет – 4%.

Если взять за основу индивидуальные характеристики киберпреступности, то можно сделать выводы о среднем возрасте потерпевших от мошенничеств с использованием электронной вычислительной техники. В основном это категория самых активных пользователей возрасте от 25 до 50 лет. Также немалая доля потерпевших приходится на возрастную категорию выше 50 лет, в связи с низким уровнем знаний в той или иной технической сфере (пенсионеры, взрослые люди, не имеющие достаточного уровня осведомленности о высоких информационных технологиях и методах защиты в сети Интернет).

Территориальные показатели сопоставимы и с уровнем киберпреступности, а именно уровень проникновения Интернета в крупных городах с население больше 100 тысяч, составляет 44%. В городах с населением менее 100 тысяч человек – 28%, а в селах и поселках городского типа – 27%.

Уровень дохода пользователей, обусловлен неоднозначными показателями:

– высокий уровень дохода – 1% пользователей;
– выше среднего – 10%;
– средний уровень – 40%;
– ниже среднего – 38%;
– низкий уровень дохода – 7%.

Как правило, пользователи, которые имеют доход низкий и ниже среднего, являются категорией, которую можно расценивать финансово зависимой. Пользователи данной категории часто являются потенциальными мошенниками, которые ищут в Интернете легкий способ незаконного обогащения путем обмана и злоупотребления доверием других законных пользователей.

Также следует отметить, что немалую долю пользователей составляют лица, не получившие высшего образования. К этим лицам можно отнести студентов, которые имеют специальные технические знания в сфере высоких информационных технологий, что позволяет им использовать уже полученные в ВУЗе знание при совершении незаконных действий в сети Интернет.

Следующим фактором, который влияет на преступность рассматриваемой категории является мобильность доступа в сеть. Так 57% Интернет пользователей используют в качестве типа доступа – мобильный телефон или смартфон; 45% – домашний переносной персональный компьютер; 39% – стационарный персональный компьютер; 15% – планшетный персональный компьютер; 10% – рабочий компьютер [9].

Все приведенные статистические данные в статье не являются точными и отображают лишь общую картину криминогенной обстановки в Украине. Кроме того, не учтены данные о преступлениях, про которые позже не были проинформированы правоохранительные органы. Есть ряд причин, по которым потерпевшие могут не заявлять в органы правопорядка о совершенных в отношении них мошенничествах с использованием электронно-вычислительной техники.

Выводы. Мошенничество, совершенное с использованием электронно-вычислительной техники, действительно оказывает высокое влияние на экономику государства в целом, отображает уровень экономической безопасности частного сектора, крупной предпринимательской деятельности, банковской и финансовой системы в целом. Вышеуказанные показатели статистики дают возможность оценить значительную динамику развития данного вида преступности. Развитие киберпреступности и ее криминологические особенности очень сильно отличаются от преступности общекриминальной направленности. Рост мошенничеств с использование электронно-вычислительной техники на прямую зависит от увеличения степени проникновения высоких информационно-программных технологий в повседневную жизнь населения Украины. Кроме того, повышение квалификации правоохранительными органами (специальными подразделениями по борьбе с киберпреступностью), их методы противодействия, опыт, профилактика порождают необходимость изобретения преступниками все новых видов кибермошенничеств.

Конечно, быстрое решение данных проблем в принципе невозможно, однако оптимизирование работы по борьбе как с данным видом мошенничества, так и с киберпреступностью в целом является первоочередной необходимостью государства. Речь идет об изменениях в законодательстве (конституционной, административной, уголовной, гражданской и хозяйственной отраслях права), а также окончательная реорганизация и создание дополнительных органов по контролю, обеспечению безопасности и противодействию правонарушениям в сфере высоких информационных технологий.

Список использованной литературы:

1. Кримінальний кодекс України: Закон від 05.04.2001 № 2341-III (Редакція станом на 14.06.2018). Відомості Верховної Ради України (ВВР). 2001, № 25-26, ст. 131.

2. Про затвердження Положення про Державну службу фінансового моніторингу України: постанова кабінету міністрів України від 29 липня 2015 р. № 537. Офіційний вісник України від 14.08.2015. 2015 р., № 62, с. 109, ст. 2028.

3. Статут Української міжбанківської Асоціації членів платіжних систем «ЄМА», затверджений рішенням конференції – 2006 р., с. 21, м. Київ.

4. Долгова А. И. Криминология: учебник для ВУЗов. Москва, 2005. 894 с. (Норма).

5. Криминология: учебник / Под ред. В. Н. Кудрявцева, В. Е. Эминова. М.: Юрист, 2004. 734 с;

6. Официальный сайт Департамента киберполиции Национальной полиции Украины «У поліції відкрито 23 кримінальних провадження за фактами втручання в роботу комп'ютерних мереж». URL: https://cyberpolice.gov.ua/news/u-policziyi-vidkryto--kryminalnyx-provadzhennya-za-faktamy-vtruchannya-v-robotu-kompyuternyx-merezh-video-5296;

7. Официальная статистика Украинской межбанковской ассоциации членов платежных систем EMA. URL: https://ema.com.ua/payment-fraud-actual-infographics-results-2-q-2016;

8. Статистична інформація «Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування» Генеральна прокуратура України. URL: https://www.gp.gov.ua/ua/stat.html;

9. Проникновение Интернета в Украине: материалы исследования Интернет Ассоциации Украины, 2018 год. URL: http://www.inau.org.ua/sites/default/files/file/1806/ui_factum_group_ii_kvartal_2018.pdf

ИНФОРМАЦИЯ ОБ АВТОРЕ

Лефтеров Лев Васильевич – адъюнкт кафедры уголовного права и криминологии Одесского государственного университета внутренних дел

INFORMATION ABOUT THE AUTHOR

Lefterov Lev Vasilyevich – Adjunct at the Department of Criminal Law and Criminology of Odessa State University of Internal Affairs

lev.lefterov@cybercrime.gov.ua