РАЗДЕЛ IV.
УГОЛОВНОЕ ПРАВО И КРИМИНОЛОГИЯ; УГОЛОВНО-ИСПОЛНИТЕЛЬНОЕ ПРАВО

УДК: 343
DOI: 10.18384/2310-6794-2018-4-144-152

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Ахмедханова С.Т., Ахмедханова С.Т., Кахбулаева Э.Х.
Всероссийский государственный университет юстиции (РПА Минитерства юстиции РФ), Северо-Кавказский институт (филиал)
367008, Республика Дагестан, г. Махачкала, ул. Агасиева, д. 87, Российская Федерация

Аннотация. На современном этапе развития и постоянного совершенствования информационных отношений в различных сферах общества наблюдаются тенденции роста осуществления неправомерного доступа к компьютерной информации. В связи с этим возникает необходимость достаточно серьёзного реформирования со стороны законодателя и усиления регулирования со стороны государства информационной базы с целью обеспечения информационной безопасности и целостности общегосударственных интересов. С этой целью в данной статье предложены меры по предупреждению и профилактике преступлений в сфере компьютерной информации.

Ключевые слова: криминология, информационная безопасность, компьютерные преступления, профилактика, предупреждение.

CRIMINOLOGICAL CHARACTERISTICS OF COMPUTER CRIMES

Akhmedkhanova S.T., Akhmedkhanova S.T., Kahbulayeva E.H.
North Caucasus Institute (branch) of the All-Russian State University of Justice (Russian Legal Academy of the Ministry of Justice of Russia)
87, Agasieva st., Makhachkala, Republic of Dagestan, 367008, Russian Federation

Abstract. Along with continuous improvement of information relations in various spheres of society there are tendencies to the growth of illegal access to computer information. In this regard, there is a need for serious reform on the part of the legislator and the strengthening of state regulation of the information base in order to ensure information security and integrity of national interests. To attain this goal the authors of the article suggest some measures to prevent cybercrimes.

Key words: criminology, information security, computer crime, prevention.

Рассматривая и изучая историю последних десятилетий, можно сделать вывод, что происходит постоянный, прогрессирующий рост преступлений, совершаемых с использованием ПК (персонального компьютера), усложняются и изменяются способы совершения данных преступлений и тем самым затрудняется возможность для правоохранительных структур обнаружить признаки данных преступлений, выявить и привлечь к уголовной ответственности лиц, совершающих данные преступления, а также установить количество жертв и суммы ущербов.

Во-первых, преступления данной категории приносят лицам огромные, колоссальные прибыли, осуществляются данные действия сравнительно лёгким способом, посредством доступа к финансовым средствам определённых физических лиц либо организаций. Во-вторых, если говорить о преступно заинтересованных и действующих группах, получение информации, относящейся к категории конфиденциальной для ряда государственных органов и значимых на мировом рынке коммерческих структур, является для преступной группировки мощным инструментом оказания воздействия на данные структуры с целью реализации своих преступных замыслов и обеспечения собственной безопасности, а также для выдвижения определённых требований, создавая при этом угрозу причинения вреда общественным интересам. В-третьих, преступления, направленные на создание, распространение и последующее использование вредоносных компьютерных программ, создают существенную угрозу национальной безопасности, имеют огромное социально-правовое значение, т. к. все системы жизнеобеспечения страны закреплены именно в электронных носителях и возможность вмешательства со стороны может причинить колоссальный вред. В условиях современной глобализации информационное поле становится ареной, на которой возникают различные соглашения международного характера, и вмешательство в данный процесс со стороны различных преступных группировок будет способствовать росту международного терроризма. В подтверждение можно привести исследованные статистические данные, полученные с официального сайта Совета безопасности РФ, согласно которым в 2017 г. было выявлено 900 тыс. попыток проникнуть в секретные данные служб государственной власти, и 79 тыс. из них раскрыты как попытки проникнуть на официальный сайт Президента РФ [1].

Российской информационной сфере присуще несовершенство правовых отношений, и поэтому пользователи не всегда располагают точными юри-

дическими ориентирами нормального правомерного поведения при пользовании информационными носителями. Это, в свою очередь, порождает и повышает степень криминологической уязвимости основных центров компьютерной секретной информации для участников недобросовестных информационных отношений.

Но есть и другая сторона, связанная с тем, что информационная сфера не имеет возможности развиваться сбалансировано, поскольку технические меры безопасности и организационно-правовые структуры развиты достаточно слабо, что ухудшает и делает пассивной работу предупредительных организаций, чья деятельность направлена на создание устойчивой и сильной базы для информационного обмена. На сегодняшний день существует угроза криминальных посягательств на государство, общество, коммерческие организации со стороны преступных хакерских группировок, и поэтому необходимость разработки эффективной предупредительной и профилактической программы, направленной на защиту и обеспечение информационной безопасности, является приоритетной программой Российского государства [2]. При разработке данных программ необходимо постоянно и целенаправленно изучать криминологические особенности компьютерных преступлений, необходимо работать с лицами, совершающими данные преступления, изучать их личностные характеристики, основные детерминанты их преступного поведения с целью постоянного совершенствования системы информационной безопасности, создания прочной и устойчивой базы, не подвергающейся хакерским атакам со стороны преступных группировок, формирования прочной и недоступной государственной системы внутреннего и внешнего управления. Компьютерные технологии всё чаще выступают орудиями совершения преступлений, о чём свидетельствует изученная мною статистика ущерба, нанесённого бюджету Российской Федерации за последний год, оценивающегося в 6 млрд. долларов, тогда как в США ущерб от данной категории преступлений составляет 4 млрд. долларов, во Франции 1 млрд. евро, в Германии 2 млрд. евро; при этом наблюдается, по данным статистического исследования, постоянное увеличение и рост преступлений данной направленности [3].

Увеличение числа преступлений с использованием компьютерных технологий обусловлено также тем, что данный вид преступления всё чаще совершается интеллектуально предприимчивой категорией лиц, использующей определённые изощрённые методы проникновения в засекреченную базу данных государственных структур и коммерческих организаций. Возраст и стаж преступников весьма различны: от молодых до взрослых, от малообразованных до высококвалифицированных специалистов.

В качестве детерминанты выступают также трудности, возникающие в процессе применения уголовно-правовых диспозиций судебными и следственными органами, вызванные казуистичной формулировкой норм, регулирующих преступления в области компьютерных программ, а также влиянием других норм при применении указанных правоохранительными органами. Причиной распростране-

ния преступлений данной диспозиции также является недостаточное исследование всех аспектов, касающихся привлечения лиц к уголовной ответственности, не достаточно точное определение понятия компьютерных преступлений и постоянно возникающая необходимость совершенствования института ответственности за преступления данной направленности с использованием опыта зарубежных стран [4].

Основными тенденциями, причинами и условиями роста и развития компьютерных преступлений являются: увеличение количества преступлений в области компьютерных программ с использованием постоянно совершенствующихся хакерских программ, рост профессионализма, респектабельности, интеллекта компьютерных преступников, усложнение процесса изучения личности преступника в связи с постоянным омоложением состава преступников и увеличения количества лиц, раннее не привлекавшихся к уголовной ответственности, колоссальные суммы причинённого материального ущерба государственному бюджету, явно превалирующего над суммами других видов преступлений, активный процесс перерастания компьютерной преступности в разряд международной, а также достаточно высокий уровень латентности подобных преступлений. Это усложняет возможности разработки и применения программ, направленных на предупреждение компьютерных преступлений. Латентность данного вида преступления связана прежде всего с небрежностью совершения пользователем-правонарушителем в силу его неопытности и неосведомлённости о преступном характере совершаемых им действий. Часто потерпевшая сторона умалчивает в силу незаинтересованности о противоправном деянии либо не сообщает вовремя об имевшем место факте готовящегося преступления. Количество нераскрытых и неучтённых преступлений в области компьютерной информации правоохранительными структурами также влияет на уровень латентности преступления [5].

Криминологическая характеристика личности преступника показала, что система его ценностей выражена искажением нравственных приоритетов. Чаще всего личностные качества характеризуются ярко выраженными чертами эгоизма и свойственными этому стремлениями к материальному благополучию. Данные лица создают для себя наиболее комфортные условия, закрываясь от всего общества, но в то же время создавая узкую группу по эгоистическим интересам, так называемые объединения хакеров, для удобства совершения преступлений с использованием компьютерной информации и новейших компьютерных технологий. Им свойственно обычно деформированное, ослабленное сознание, и их нравственные приоритеты искажены призмой своих представлений об окружающем мире, что является причиной выбора преступной линии поведения [6].

Основными мотивами противоправного поведения преступников данной области, как справедливо отмечал В.Б. Вехов, являются:

1) присутствие корыстных соображений при совершении преступлений в сфере компьютерной информации;

2) цели политического характера, связанные со шпионажем, направленные на подрыв финансово-экономической и денежно-кредитной политики государства как внутри страны, так на международной арене;

3) совершение студентами и профессиональными программистами в целях исследовательской мотивации различных современных технологий и программ.

4) хулиганские побуждения и озорство, а также личная вражда и месть.

При изучении структуры личности можно выделить следующие подструктуры: физиологические, социально-демографические, психологические, нравственно-моральные, уголовно-правовые [7].

С криминологической точки зрения можно составить портрет преступника, совершающего преступления в сфере компьютерной информации, примерно такой: лицо в возрасте от 20 до 40 лет, имеющее достаточный опыт работы в данной сфере, к уголовной ответственности ранее не привлекавшееся, являющееся достаточно мыслящей личностью, способной принимать ответственные решения, работник, добросовестно исполняющий свои обязанности, нетерпимый к насмешливому отношению, имеющий устойчивый статус в глазах окружающих людей, любящий работать в уединённой атмосфере, для решения рабочих вопросов до конца часто задерживающийся и редко использующий отпуск.

При тщательном изучении характеристики лиц, совершающих преступления в сфере компьютерной информации, можно прийти к выводу, что это лица, чертами которых являются аутизация и интравертированность, т. е. данным лицам свойственно уходить в себя, отгораживаться от всех проблем и от окружающих, направлять свои интересы только на удовлетворение своих собственных потребностей и нужд, а связано это в основном с нарушением социального общения и отгороженностью от нормальных контактов.

В целях избегания неправомерного доступа к компьютерной информации и сохранения секретности государственной информации необходимо применить правовые, социальные и организационно-технические меры [8].

В качестве организационно-технических можно рассматривать разработку специальных защитных программ, направленных на исключение возможности доступа к секретной информации, составляющей государственную тайну. Посредством использования защитных программ можно постепенно прийти к сокращению количества преступлений в области неправомерного доступа к компьютерной информации, осуществить совершенствование социально-экономических, функциональных проблем, возникающих в информационной сфере, путём изменения системы ценностей и формирования определённых морально-этических, основанных на диспозициях уголовно-правовых норм, правил при осуществлении работы с компьютерными технологиями.

Если говорить о социальной направленности, меры предупреждения и профилактики должны быть в первую очередь сориентированы на достаточно широкую социальную превенцию, основной целью которой

является минимизация компьютерных преступлений, снижение зависимости у индивида, начиная с детского возраста, от видеоигр и Интернета. Возникает необходимость создания дополнительных субъектов, осуществляющих постоянную борьбу с данными видами преступлений. Негосударственные общественные объединения и структуры, объединения молодёжи, основными задачами которых являются обогащение духовно-нравственной сферы современного индивида, воспитание чувства ответственности и формирование этико-правовых приоритетов, вовлечение современного поколения в научные и спортивные мероприятия, а также привитие с детского возраста чувства любви к Родине.

Если касаться правовых мер предупреждения, тут возникает необходимость совершенствования законодательной сферы, регулирующей данную область, путём изложения ч. 1 ст. 273 УК РФ в следующей редакции: «Создание программ для персонального компьютера путём внесения изменений в существующие программы, целью которого является несанкционированное уничтожение, блокирование, изменение и модификация любых нарушений работы персонального компьютера, системы, сети, а равно использование, распространение таких программ и машинных носителей» [9].

Возникает вопрос о целесообразности включения в качестве квалифицирующего обстоятельства в ст. 272 в чч. 2, 3 ещё одного непосредственного объекта – отношения собственности, где потерпевший рассматривается как главный обязательный элемент данного объекта посредством дополнения ч. 2 ст. 272 УК РФ новым квалифицирующим признаком «сопряженное с применением значительного материального ущерба потерпевшему».

Для дифференциации и усиления ответственности за осуществление неправомерного доступа к компьютерной информации, учитывая признаки, раскрывающие субъективную сторону данного преступления, можно выделить некоторые дополнительные мотивы и цели совершения преступления, рассматривая их в качестве новых квалифицирующих признаков: «То же деяние, совершенное лицом:

– из корыстных побуждений с целью извлечения определённой выгоды для себя либо по найму;

– из хулиганских побуждений, нарушая установленные в обществе нормы;

– с целью скрыть факт совершения другого преступления либо облегчить его совершение».

На наш взгляд, необходимо дополнить гл. 28 УК РФ новым нормативно-правовым актом – ст. 272.1 УК РФ «Незаконное завладение персональным компьютером с целью осуществления доступа к охраняемым законом компьютерным информациям» и квалифицирующими признаками.

В составы большей части преступлений можно включить в качестве квалифицирующего дополнения «совершение преступления с использованием компьютерной информации, персонального компьютера и сети ЭВМ» [10].

Рассмотренный в данной статье материал может быть использован в научных исследованиях по данной тематике, а предложенные меры социального характера, а также меры, направленные на совершенствование

существующего законодательства, способствуют дальнейшему улучшению программ предупреждения и профилактики преступлений в области компьютерных программ и дополняют диспозицию ст. 273 УК РФ нововведениями.

ЛИТЕРАТУРА

1. Вехов В.Б., Голубев В.А. Расследование компьютерных преступлений в странах СНГ: монография / под ред. Б.П. Смагоринского. Волгоград: ВА МВД России, 2014. 304 с.
2. Грунин О., Грунин С. Экономическая безопасность организации. СПб.: Питер, 2002. 160 с.
3. Егоров В.С. Понятие состава преступления в уголовном праве: учебное пособие. М.: Московский психолого-социальный институт, 2001. 80 с.
4. Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук. М., 2002. 166 с.
5. Приговор Басманного районного суда г. Москвы от 06.05.2011 [Электронный ресурс] // Правосудие: [сайт]. URL: http://basmanny.msk.sudrf.ru/modules.php?name=bsr&op=show_text&srv_num=1&id=77600021105121427202311000128572 (дата обращения: 07.10.2018).
6. Постановление Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс] // Российская газета: [сайт]. URL: https://rg.ru/2008/01/12/sud-voprosy-dok.html (дата обращения: 30.11.2018).
7. Старичков М.В. Уголовная ответственность за неправомерный доступ к компьютерной информации, повлекший её копирование // Деятельность правоохранительных органов и государственной противопожарной службы в современных условиях: проблемы и перспективы развития: сб. науч. тр. / отв. ред. А.В. Чернов. Иркутск: ВСИ МВД России, 2013. С. 202–204.
8. Спирина С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации: дис. ... канд. юрид. наук. Краснодар, 2014. 216 с.
9. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» // Собрание законодательства РФ. 2014. № 30 (ч. 1). Ст. 4223.
10. Шмонин А.В. Формирование понятия «преступления, сопряженные с банковскими технологиями» // Банковское право. 2005. № 6. С. 28–32.

REFERENCES

1. Vekhov V.B., Golubev V.A. *Rassledovaniye komp'yuternykh prestupleniy v stranakh SNG: monografiya* [Investigation of Computer Crimes in the CIS Countries: a Monograph]. Volgograd, *VA MIA* of Russia Publ., 2014. 304 p.
2. Grunin O., Grunin S. *Ekonomicheskaya bezopasnost' organizatsii* [Economic Security Organization]. St. Petersburg, *Peter* Publ., 2002. 160 p.
3. Egorov B.C. *Ponyatiye sostava prestupleniya v ugolovnom prave* [The Concept of Crime in Criminal Law]. Moscow, Psychological and Social Institute Publ., 2001. 80 p.
4. Malyshenko D.G. *Ugolovnaya otvetstvennost' za nepravomernyy dostup k komp'yuternoy informatsii: dis. ... kand. yurid. nauk* [Criminal liability for illegal access to computer information: PhD thesis in Law]. Moscow, 2002. 166 p.
5. [The Verdict of the Basmanny District Court of Moscow dated 06.05.2011]. In: *Pravosudiye* [Justice]. Available at:http://basmanny.msk.sudrf.ru/modules.php?name=bsr&op=show_

text&srv_num=1&id=77600021105121427202311000128572 (accessed: 10.07.2015).
6. [Resolution of the Plenum of the Supreme Court of the Russian Federation dated 27.12.2007 no. 51 "On Judicial Practice in Cases of Fraud and Embezzlement"]. In: *Rossiiskaya gazeta.* Available at:https://rg.ru/2008/01/12/sud-voprosy-dok.html (accessed: 30.11.2018).
7. Starichkov M.V. [Criminal Liability For Unauthorized Access to Computer Information That Caused Its Copying]. In*: Deyatel'nost' pravookhranitel'nykh organov i gosudarstvennoy protivopozharnoy sluzhby v sovremennykh usloviyakh: problemy i perspektivy razvitiya: sb. nauch. tr.* [Activities of Law Enforcement Agencies and the State Fire Service in Modern Conditions: Problems and Development Prospects: Collection of Scientific Works]. Irkutsk, *VSI MIA* of Russia, 2013. Pp. 202–204.
8. Spirin S.G. *Kriminologicheskiye i ugolovno-pravovyye problemy prestupleniy v sfere komp'yuternoy informatsii: dis. ... kand. yurid. nauk* [Criminological and Criminal Problems of Crimes in the Field of Computer Information: PhD Thesis in Law]. Krasnodar, 2014. 216 p.
9. [Federal Law dated 07.27.2006 "On Information, Information Technologies and Protection of Information" no. 149-FZ]. In: *Sobraniye zakonodatel'stva RF* [Collection of the Legislation of the Russian Federation], 2006, no. 31 (part 1). Art. 3448; 2010, no. 31. Art. 4196; 2011, no. 15. Art. 2038; 2011, no. 30 (part 1). Art. 4600; 2012, no. 31. Art. 4328; 2013, no. 14, art. 1658; 2013, no. 23. Art. 2870; 2013, no. 27. Art. 3479; 2013, no. 52 (part 1). Art. 6961; 2013, no. 52 (part 1). Art. 6963; 2014, no. 19. Art. 2302; 2014, no. 30 (part 1). *Territoriya nauki* [The Territory of Science], 2015, no. 6 (142). Art. 4223.
10. Shmonin A.V. [Building the Concept of "Crimes Associated with Banking Technologies"]. In: *Bankovskoye pravo* [Banking Law], 2005, no. 6, pp. 28–32.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Ахмедханова Самира Телхатовна – кандидат юридических наук, доцент кафедры уголовного права Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России);
e-mail: cabinaken@mail.ru

Ахмедханова Сабина Телхатовна – кандидат экономических наук, доцент Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России);
e-mail: cabinaken@mail.ru

Кахбулаева Эльмира Хасулбековна – кандидат юридических наук, доцент кафедры уголовного права Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России);
e-mail: cabinaken@mail.ru

INFORMATION ABOUT THE AUTHORS

Samira T. Akhmedkhanova– PhD in Law, associate professor at the Department of Criminal Law, North Caucasus Institute (branch) of the All-Russian State University of Justice (Russian Legal Academy of the Ministry of Justice of Russia);
e-mail: cabinaken@mail.ru

Sabina T. Akhmedkhanova – PhD in Economics, associate professor at North Caucasus Institute (branch) of the All-Russian State University of Justice (Russian Legal Academy of the Ministry of Justice of Russia);
e-mail: cabinaken@mail.ru

Almira K. Kakhbulayeva – PhD in Law, associate professor at North Caucasus Institute (branch) of the All-Russian State University of Justice (Russian Legal Academy of the Ministry of Justice of Russia);
e-mail: cabinaken@mail.ru

ПРАВИЛЬНАЯ ССЫЛКА НА СТАТЬЮ

Ахмедханова С.Т., Ахмедханова С.Т., Кахбулаева Э.Х. Криминологическая характеристика преступлений в сфере информационных технологий // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2018. № 4. С. 144–152.
DOI: 10.18384/2310-6794-2018-4-144-152

FOR CITATION

Akhmedkhanova S.T., Akhmedkhanova S.T., Kahbulayeva E.H. Criminological Characteristics of Computer Crimes. In: *Bulletin of Moscow Region State University. Series: Jurisprudence,* 2018, no. 4, pp. 144–152.
DOI: 10.18384/2310-6794-2018-4-144-152