Сыздыков Алмаз Жаксыбекович
Академия правоохранительных органов при Генеральной прокуратуре
Республики Казахстан, главный научный сотрудник
доктор PhD, младший советник юстиции

Имангалиев Нуртай Конысбаевич
Академия правоохранительных органов при Генеральной прокуратуре
Республики Казахстан, главный научный сотрудник
к.ю.н., старший советник юстиции

КРИМИНОЛОГИЧЕСКИЙ ПОРТРЕТ КИБЕРПРЕСТУПНИКА

Резюме. *В статье рассмотрены отдельные вопросы совершения киберпреступлений в зарубежных странах и в Казахстане. Охарактеризован криминологический портрет киберпреступника на основе зарубежного и отечественного опыта.*

Ключевые слова*: киберпреступление, киберхищение, киберпреступник, криминологический портрет, информационные технологии.*

Түйін. *Мақалада шетмемлекеттерде және Қазақстанда киберқылмыс жасалудың кейбір сұрақтары қарастырылған. Сонымен қатар шетел және отандық тәжірибе негізінде киберқылмыскердің криминологиялық портреті көрсетілген.*

Кілт сөздер: *киберқылмыс, кибержымқыру, киберқылмыскер, криминологиялық портрет, ақпараттық технологиялар.*

Summary. *The article discusses certain issues of cybercrime in foreign countries and Kazakhstan. The authors made criminological portrait of the cybercriminal based on foreign countries and domestic experience.*

Key words: *cybercrime, cyber theft, criminological portrait, cybercriminal, informational technologies.*

Развитие научно-технического прогресса захватывает практически все сферы жизнедеятельности современного общества. Одним из достижений научно-технического прогресса является всемирная сеть Интернет, которая получила распространение в экономической, научной, педагогической, управленческой, производственной, медицинской, финансовой сферах общества. Интернет в значительной степени способствовал улучшению жизнедеятельности человека, стиранию границ, форсированию интеграционных, глобализационных процессов.

Для пользователей Интернета, так и для информационной безопасности государства вместе с положительными сторонами, возникла серьезная угроза от «глобальной паутины». Достижения науки и техники позволяют преступникам без прямого контакта с жертвой совершать противоправные действия на всем информационном пространстве.

Учитывая, что научно-технический процесс не стоит на месте, борьба с данным видом преступности еще долгое время будет одной из наиболее актуальных проблем.

К отличительным особенностям киберпреступлений можно отнести то, что при наличии доступа к Интернету совершение и подготовка преступления может проводиться с любой точки мира.

Доходы от киберпреступлений значительно превысили доходы от других преступлений, включая торговлю наркотиками. По последним данным, приведенным в июле 2013 г. в совместном анализе американского Центра стратегических и международных исследований и компании McAfee, ежегодные потери мировой экономики от киберпреступлений достигли уже 500 миллиардов долларов [1].

Приведем примеры причиненного ущерба от киберпреступлений в некоторых зарубежных странах.

По сведениям Group-IB, картина киберхищений в России выглядит следующим образом.

Хищений в интернет-банкинге у физических лиц с использованием вредоносных программ совершено в 2015 году на сумму 6 424 200 рублей, в 2016 году – 15 687 000 рублей, рост составил 144%.

Хищений в интернет-банкинге у юридических лиц с использованием вредоносных программ совершено в 2015 году на сумму 956 160 000 рублей, в 2016 году – 622 500 000 рублей, снижение составило 35%.

Хищений у физических лиц с Андроид-троянами совершено в 2015 году на сумму 348 600 000 рублей, в 2016 году – 821 700 000 рублей, рост составил 136%.

Целевые атаки на банки в 2015 году были совершены на сумму 25 000 000 000 рублей, в 2016 году – 1 630 000 000 рублей, снижение на 35% [2].

Таким образом, в России в результате киберпреступлений похищается ежедневно 6 813 000 рублей.

По данным немецкой полиции, в Германии в 2016 году совершено 82649 киберпреступлений, что на 80,5 % выше по сравнению с 2015 годом. Общий ущерб составил 51, 6 млн. евро. Совершено 253290 случаев

фишинга, из которых в рамках интернет-банка, снижение на 51,4 %. В 972 случаях использован вирус вымогатель, рост на 94%. Следует отметить, что при этом имеется колоссальное теневое пространство – более чем 90%. По оценкам организации по оценке ущерба, сведения разнятся. По оценке DIW – 14,7 млрд. евро в год, по оценке BITKOM – 22,4 млрд. евро [3].

Аналогичные преступления совершаются и в Казахстане.

За последние 5 лет (с 2012 по 2017 гг.) в Казахстане число зарегистрированных преступлений с использованием IT-технологий выросло в более чем 22 раза.

Согласно статистическим данным, за 6 месяцев т.г. зарегистрировано 1013 киберпреступлений (за 2012 г. - 54, 2013 г. - 75, 2014 г. - 95, 2015 г. - 357, 2016 г. - 1234). Приведенные данные свидетельствуют о тенденции неуклонного роста числа преступлений данного вида.

При этом в стране не сформирована практика расследования дел данной категории. Так, за 2,5 года (с 2015-и 6 месяцев 2017гг.) было прекращено 274 уголовных дела, возбужденных по ст.ст.205 - 208 и 210 Уголовного Кодекса Республики Казахстан. Из них более 90% на основании п.п.1 (за отсутствием события уголовного правонарушения) и 2 (за отсутствием в деянии состава уголовного правонарушения) ч.1 ст.35 Уголовно-процессуального кодекса Республики Казахстан.

Средний удельный вес киберпреступлений в структуре общей преступности в стране по результатам проведенного анализа составил всего 0,33%. Взятие за основу указанного периода связано с тем, что соответствующие квалифицирующие признаки были введены с 1 января 2015 года.

Так, за анализируемый период органами уголовного преследования зарегистрировано 3305 киберпреступлений (2015 г. – 180, 2016 г. – 1078, 9 мес. 2017 г. – 2047), в суд направлено лишь 6%, или 201 уголовное дело (2015 г. – 103, 2016 г. – 6, 2017 г. – 92).

В связи с неустановлением лиц, совершивших такие преступления, прерваны сроки по 2773 уголовным делам (2015 г. – 58, 2016 г. – 941, 9 мес. 2017 г. – 1774).

Таблица 1 – Удельный вес киберпреступлений в общей преступности

Вид киберпреступлений	период	Количество		Коэффициент преступности на 10 000 экономически активного населения	Неустановление лица, совершившего уголовное правонарушение, %
		уровень, ед.	удельный вес, %		
киберкража	2015 г.	135	0,05	0,16	25,2
	2016 г.	31	0,01	0,04	87,1
	2017 г.	113	0,08	0,10	72,6
кибермошенничество	2015 г.	45	0,01	0,05	53,3
	2016 г.	1047	0,29	1,22	87,3
	2017 г.	2215	0,62	1,78	69,8

В качестве примера совершения киберхищения в особо крупном размере можно привести преступление, совершенное казахстанскими киберпреступниками в г. Алматы.

Так, в 2015 году два программиста для совершения киберпреступлений создали организованную преступную группу, состоящую из 20 человек. На протяжении длительного периода преступная группа занималась покупкой и модернизацией программных продуктов для несанкционированного подключения к системе удаленного пользователя и получения неправомерного доступа к информации. Для хищения денежных средств с использованием добытой информации координировали и привлекали к участию в организованной преступной группе лиц, по своим личностным и профессиональным качествам способных совершать активные действия, направленные на совершение планируемых преступлений.

Осуществляя подготовку преступлений, для скрытия следов своей незаконной деятельности посредством глобальной сети Интернет преступники арендовали сервера с IP-адресами в Соединенном Королевстве Великобритании, Северной Ирландии, Федеративной Республике Германия, Французской Республике, Королевстве Нидерландов, Соединенных Штатах Америки.

Затем, используя программы для шифрования, в алгоритм программного продукта «NanoCore» внесли изменения, позволившие исключить обнаружение системами защиты компьютеров. Модифицированный программный продукт предоставил преступникам возможность скрытой установки и обеспечил удаленный доступ к зараженным компьютерам.

Таким образом, преступниками был создан вредоносный компьютерный программный продукт для не-

правомерного использования информации, хранящейся на электронных носителях.

Далее преступники разослали электронные письма от имени государственных надзорных и контролирующих органов. Бухгалтера и сотрудники финансовых служб различных учреждений и коммерческих фирм, установившие и активировавшие вредоносный программный продукт «NanoCore», способствовали получению преступниками неправомерного удаленного доступа к хранящимся на электронных носителях данным, возможности контроля и управления зараженными компьютерами.

В ходе предварительного следствия было установлено более 40 фактов совершения преступниками аналогичных преступлений и похищения путем удаленного перечисления денежных средств на счета и платежные карты, заранее оформленные на членов ОПГ, на общую сумму более 500 млн. тенге.

В данной организованной преступной группе киберпреступников два программиста, имеющие опыт работы в сфере информационных технологий, бухгалтерского учета и онлайн платежей, взяли на себя роль одновременно руководителей преступной группы, разработчиков, распространителей вредоносных программных продуктов и заливщиков.

Семь членов ОПГ подбирали лиц, на которых оформлялись счета и платежные карты для легализации похищенных денежных средств, координируя их деятельность. Остальные члены ОПГ осуществляли снятие денежных средств в отделениях банков и банкоматов со своих счетов и получали в качестве вознаграждения 10-20% от суммы похищенных денег.

Приговором районного суда № 2 Бостандыкского района города Алматы от 24 января 2017 года члены и руководители организованной группы киберпреступников за совершение преступлений, предусмотренных п. 1,3, ч.4 ст. 188, 24 ч.3, п.1,2, ч.3 ст. 208, п.1,2, ч.3 ст. 210, ч.1 ст. 262 УК РК осуждены к различным срокам лишения свободы от 5 до 8 лет, с отбыванием наказания в колонии общего режима [4].

Таким образом, мы видим, что киберпреступления наносят колоссальный ущерб, как бюджету отдельного лица и организации, так и для государства в целом.

Как показывает статистика, количество киберпреступлений, из года в год в Казахстане увеличивается. В этой связи одним из немаловажных вопросов остается установление криминологического портрета киберпреступника.

Рассмотрим мнения ученых по данному вопросу.

Традиционно криминологи выделяют следующие мониторинговые показатели, без которых невозможно изучение личности преступника: социально-демографические, нравственно-психологические и правовые [5].

Рассматривая криминологический портрет киберпреступника, мы разделяем мнение М.И. Еникеева, согласно которому личность преступника - это «совокупность типологических психологических качеств индивида, обусловивших совершенное им преступное деяние» [6].

Профессор В.Д. Малков под личностью преступника предлагает понимать «лицо, совершившее преступление, в котором проявилась его антиобщественная направленность, отражающая совокупность негативных социально значимых свойств, влияющих в сочетании с внешними условиями и обстоятельствами на характер преступного поведения» [7].

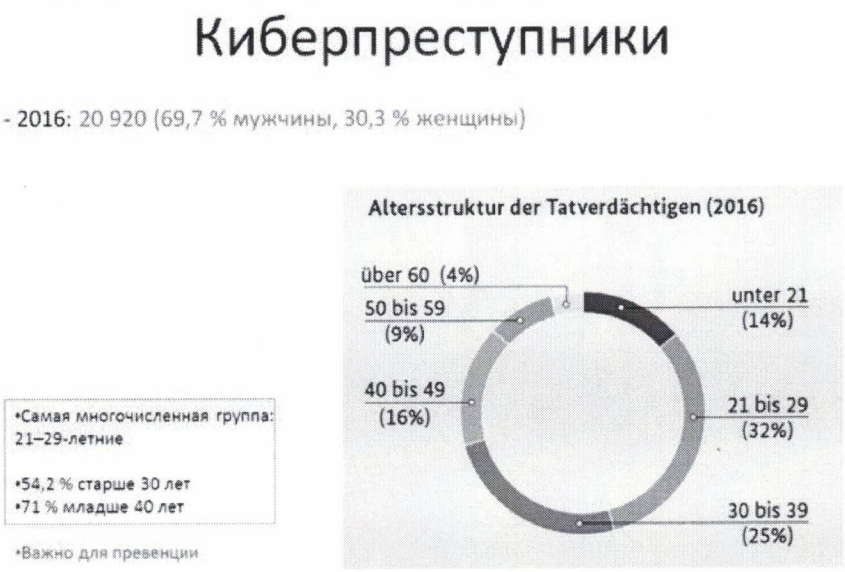
Проведенное исследование личности киберпреступника, по статистическим данным о лицах, привлеченных к уголовной ответственности за совершение преступлений в сфере информационных технологий, указывает на то, что образ киберпреступника в последние годы претерпевает значительные изменения.

В конце XX в. Экспертно-криминалистическим центром МВД РФ был составлен портрет российского хакера. Это был мужчина в возрасте от 15 до 45 лет, имеющий многолетний опыт работы на компьютере либо почти не обладающий таким опытом; является мыслящей личностью, способной принимать ответственные решения; добросовестный работник, по характеру нетерпимый к насмешкам; любит уединенную работу; часто задерживается на работе [8].

В качестве примера можно также привести криминологический портрет немецкого киберпреступника. В 2016 году совершено 20920 преступлений, из которых 69,7 % совершено мужчинами и 30,3 % женщинами [3].

Согласно научному исследованию, проведенному в 2016 году немецкими учеными, криминологический портрет киберпреступника в Германии выглядит следующим образом.

Диаграмма 1 – Характеристика киберпреступников по возрасту в Германии.



При исследовании учитывались такие критерии личности преступника, как: возраст, образование, социальное положение (трудоустройство), пол, судимость.

В результате обобщенный криминологический портрет киберпреступника выглядит следующими образом. Значительная часть киберпреступлений совершена мужчинами (64 из 85, т.е. 75,3 %), женщинами – +21 преступление, или 24,7%. 42 человека (49, 4 %) – это лица в возрасте от 21 до 29 лет, 27 человек (31, 7 %) – от 29 до 39 и 8 человек (9, 4 %) в возрасте до 21 года.

Среди киберпреступников наблюдается преобладание представителей молодого поколения, так как навыки владения компьютером формируется в более раннем, дошкольном возрасте.

По мнению зарубежных ученых, главной особенностью является их юный возраст, непрофессиональные хакерские способности, наличие свободного времени, упорство в достижении поставленной цели, использование уже готовых кодов, разработанных специалистами [9].

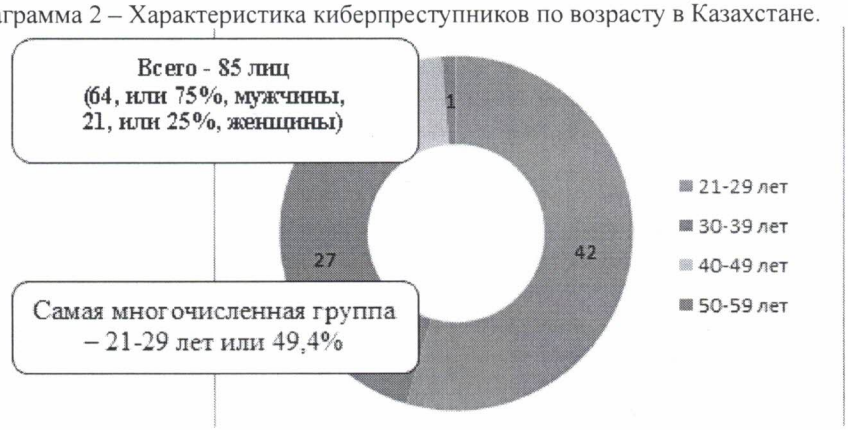
Также немаловажное значение в формировании личности хакера имеет уровень образования и социальное положение. Так, среди киберпреступников доля лиц со средним и средним специальным образованием составляет 76,4 % (65 человек), с высшим образованием – 20 % (17 человека).

На долю безработных приходится 82,3 % (70 человек), что позволяет судить о том, что преступления в основном совершаются лицами, имеющими низкий уровень доходов либо не имеющими его вовсе.

Ранее привлекавшимися к уголовной ответственности лицами совершено 36,4 % преступлений (31 человек). Преступления данной категории носят индивидуализированный характер, поэтому формы соучастия либо совершение киберпреступлений в составе организованной преступной группы слабо выражены.

Жертвами киберпреступника, согласно статистическим данным, в 50,4% случаях киберхищений являются женщины, граждане РК (99,3%) в возрасте 21-29 лет (36,1%), и только в 10 случаях жертвами являются юридические лица.

Диаграмма 2 – Характеристика киберпреступников по возрасту в Казахстане.



Список использованной литературы:

1. The Economic impact of cybercrime and cyberspionage. Center for Strategic and International Studies July 2013 Report.

2 . Ограбление по-хакерски: 2,2 млрд. рублей украли в 2016 году из российских банков / /www.kommersant.ru/doc/3235006.

3. Юрген Маурер, вице-председатель Федерального ведомства уголовной полиции в отставке. «Состояние киберпреступности в Германии». Материалы круглого стола с представителями ГП РК Астана, 2–3 ноября 2017 года.

4. Уголовное дело № 157500121001309 СУ ДВД г. Алматы.

5. Глухова А. А. Основные черты криминологической характеристики личности преступника / А. А. Глухова // Криминология: курс лекций. — Нижний Новгород: Нижегородская академия МВД России, 2013.

6. Еникеев М.И. Энциклопедия. Общая и социальная психология. М., 2002. С. 198–199.

7. Криминология [Текст]: учебник для вузов / под ред. проф. В. Д. Малкова; 27 - е изд., перераб. и доп. – М.: ЗАО «Юстицинформ», 2006. – 528с.

7. Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук. – М., 2002. – 154с.

8. Джеймс Л. Фишинг. Техника компьютерных преступлений / пер. с англ. Р. В. Гадицкого. - М.: НТ Пресс, 2008. - 320с.