

ПРАВОВЫЕ СИСТЕМЫ СТРАН АЗИИ

УДК 343.72, 343.85
ББК 67.408

ОСОБЕННОСТИ ДИНАМИКИ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН И ЕЕ ВЛИЯНИЕ НА ВОПРОСЫ ЕЁ ПРЕДУПРЕЖДЕНИЯ

А. Д. Мухамеджанова

Карагандинская академия Министерства внутренних дел Республики Казахстан имени Б. Бейсенова (Караганда, Казахстан)

В статье проведен анализ статистических данных, раскрывающих состояние преступности в сфере информатизации и связи в Республике Казахстан в период с 2018 по 2021 г. Особое внимание уделено правонарушениям, связанным с интернет-мошенничеством. Проанализированы основные показатели, формирующие представление о состоянии киберпреступности в стране. Наряду с количеством зарегистрированных правонарушений в сфере кибернетической преступности также проведен анализ количества уголовных дел, находящихся в производстве; уголовных дел, направленных в суд; прекращённых досудебных расследований. На основе анализа полученных данных сделан вывод об эффективности деятельности по профилактике отдельных видов преступлений в данной сфере, но выявлена отрицательная тенденция в предупреждении и пресечении интернет-мошенничества. В этой связи предлагается усилить меры по совершенствованию деятельности правоохранительных органов и судебной системы в вопросах противодействия преступности в сфере информатизации и связи.

Ключевые слова: киберпреступность, предупреждение преступлений, интернет-мошенничество, регистрация уголовных правонарушений, досудебное расследование, прекращение уголовного дела.

FEATURES OF THE DYNAMICS OF CYBERCRIME IN THE REPUBLIC OF KAZAKHSTAN AND ITS IMPACT ON PREVENTION ISSUES

A. D. Mukhamedzhanova

Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after B. Beisenov (Karaganda, Kazakhstan)

The article analyzes statistical data revealing the state of crime in the field of informatization and communications in the Republic of Kazakhstan in the period from 2018 to 2021. Special attention is paid to offenses related to Internet fraud. The main indicators forming an idea of the state of cybercrime in the country are analyzed. Along with the number of registered offenses in the field of cybercrime, an analysis was also carried out of the number of criminal cases under investigation; the number of criminal cases sent to court; the number of discontinued pre-trial investigations. Based on the analysis of the data obtained, a conclusion was made about the effectiveness of activities for the prevention of certain types of crimes in this area, but a negative trend in the prevention and suppression of Internet fraud was revealed. In this regard,

it is proposed to strengthen measures to improve the activities of law enforcement agencies and the judicial system in combating crime in the field of informatization and communications.

Keywords: cybercrime, crime prevention, Internet fraud, registration of criminal offenses, pre-trial investigation, termination of a criminal case.

DOI: [https://doi.org/10.14258/ralj\(2022\)2.9](https://doi.org/10.14258/ralj(2022)2.9)

Содержание практической деятельности органов внутренних дел определяется действующей криминальной обстановкой, которая влияет как на принятие конкретных управленческих решений, так и на распределение и координацию имеющихся сил и средств. В этой связи для органов внутренних дел всегда является актуальным анализ текущего состояния преступности и динамики её изменений.

В современных условиях набирает обороты преступная деятельность в сфере информационных технологий, так называемая киберпреступность. Сегодня интернет представляет собой ежедневно нарастающее пространство, в котором пользователям предоставлено гораздо больше возможностей, чем просто поиск информации. Не упускают своего случая и криминальные элементы, используя интернет-ресурсы для реализации своих преступных замыслов, они совершают запрещённые уголовным законом деяния. Многие киберпреступники используют компьютерные и смарт-технологии для проникновения не только в пользовательскую среду, но также в банковскую и платёжную системы. Хакеры взламывают защиту смартфонов, гаджетов и различных информативных баз с целью сбора персональных данных, инсайдерской информации, коммерческой тайны и других сведений, охраняемых законом. В этой связи важным элементом профилактической и предупредительной деятельности является обеспечение информационной безопасности. На данный аспект указывают как казахстанские, так и зарубежные авторы [1, с. 60; 2, с. 40; 3, с. 67; 4, с. 26; 5, с. 399; 6, с. 645]. Однако затронутая проблема требует отдельного исследования и выходит за рамки предмета представленной статьи.

Наша задача — определить значение понятия «киберпреступность» и проанализировать динамику её основных видов.

Существует много различных определений такого уголовного правонарушения, как киберпреступность. Не претендуя на оригинальность дефиниции, обобщая имеющиеся точки зрения, изложенные в исследованиях отдельных авторов [7–10], мы сформулировали свое видение данного вопроса. Так, по нашему мнению, под киберпреступностью следует понимать совокупность уголовных правонарушений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству в рамках компьютерных систем или сетей, а также против компьютерных систем, компьютерных сетей или компьютерных данных.

Следует констатировать, что киберпреступность — это глобальная проблема, не имеющая границ и требующая своего разрешения, в том числе и посредством применения уголовно-правовых мер, предусматривающих в своей основе наряду с карательными санкциями предупредительный и профилактический аспект.

Оценивая мировой масштаб киберпреступности, следует сказать, что в разных регионах мира работают около 40 миллионов киберпреступников, ущерб от действий которых оценивается миллиардами долларов [11].

Названные обстоятельства обуславливают актуальность избранной тематики, поскольку исследование изменения количества киберпреступлений позволяет оценить эффективность реализации мер по их противодействию и сделать заключение о состоянии киберпреступности в стране и определить дальнейшие направления совершенствования борьбы с киберпреступностью.

В статье представлена динамика киберпреступности в Республике Казахстан (РК) в период с 2018 по 2021 г. Наряду с анализом уголовных правонарушений, предусмотренных главой 7 Уголовного кодекса (ст. 205, 206, 207, 208 УК РК и т. д.), исследованию подвергнуто и деяние, предусмотренное п. 4 ч. 2 ст. 190 УК РК. Такой подход обусловлен тем, что способ совершения преступления с исполь-

зованием пользователя информационной системы, напрямую связан с вопросами кибербезопасности [12; 13; 14].

Анализ статистических данных показывает, что всего за период с 2018 по 2021 г. в Республике Казахстан было совершено 364 уголовных правонарушения в сфере информатизации и связи и 43911 интернет-мошенничеств [15] (табл. 1).

Таблица 1

**Информация о зарегистрированных киберпреступлениях
в период с 2018 по 2021 г.**

Вид уголовного правонарушения	Всего зарегистрировано в ЕРДР				Всего
	2018	2019	2020	2021	
п. 4 ч. 2 ст. 190 УК РК «Мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы»	517	7769	14220	21405	43911
Неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть (ст. 205)	28	59	71	46	204
Неправомерное уничтожение или модификация информации (ст. 206)	13	6	12	9	40
Нарушение работы информационной системы или информационно-коммуникационной сети (ст. 207)	5	6	4		15
Неправомерное завладение информацией (ст. 208)	11	16	8	9	44
Принуждение к передаче информации (ст. 209)	1				1
Создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210)	4	4	4	4	16
Неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211)	7	8	8	5	28
Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212)	1	2			3
Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213)	2	7	2	1	12
Всего	589	7877	14325	21479	44274

Из представленных выше данных следует, что наибольшая регистрация уголовных правонарушений наблюдается по делам, связанным с интернет-мошенничеством. В целом, по уголовным правонарушениям, предусмотренным гл. 7 УК РК, ежегодно регистрируется значительно меньше фактов, чем по делам об интернет-мошенничестве (табл. 1). Для более детального исследования, а также ввиду достаточно большого разрыва в количественном соотношении зарегистрированных уголовных дел, целесообразно анализировать уголовные правонарушения, предусмотренные главой 7 УК РК, отдельно от интернет-мошенничеств.

Итак, исследуя динамику киберпреступности, следует отметить, что в тройку наиболее распространённых уголовных правонарушений, предусмотренных гл. 7 УК РК, входят:

1) неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть (ст. 205 УК РК), процент регистрации которого составляет 56% от общего процента рассматриваемых уголовных правонарушений;

2) неправомерное завладение информацией (ст. 208 УК РК), процент регистрации которого составляет 12%;

3) неправомерные уничтожение или модификация информации, на которые приходится (ст. 206 УК РК), процент регистрации которого составляет 10%.

К наименее распространённым преступлениям следует отнести все остальные уголовные правонарушения, поскольку процент их регистрации колеблется от 1 до 8% (рис. 1.)

При этом, несмотря на наблюдающийся рост общей регистрации рассматриваемых деяний в 2019–2020 гг. (на 50%), в 2021 г. показатель регистрации уголовных правонарушений, предусмотренных главой 7 УК РК, вернулся к отметкам 2018 г.

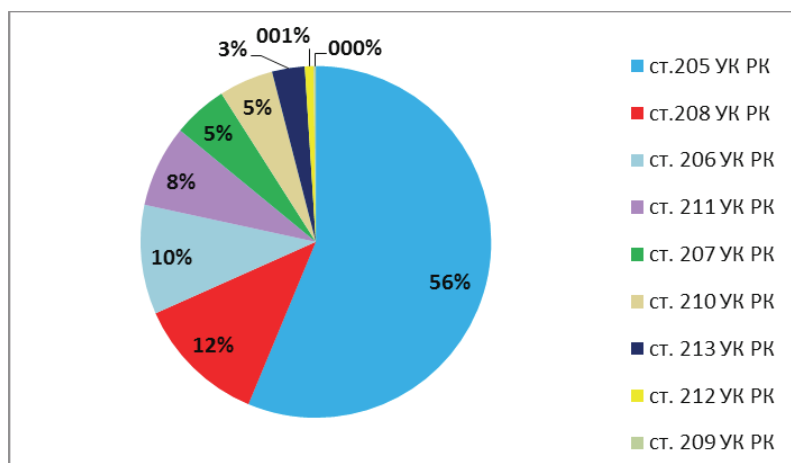


Рис. 1. Процентные значения регистрации уголовных правонарушений, предусмотренных главой 7 УК РК, за период с 2018 по 2021 г.

По всем рассматриваемым уголовным правонарушениям наблюдается как рост (2019 и 2020 гг.), так и последующее снижение (2021 г.) регистрации, что, на наш взгляд, объясняется мерами по предупреждению и профилактике преступлений, проводимыми после очередного скачка регистрации.

Что касается интернет-мошенничеств, то их регистрация в несколько раз превышает общее количество уголовных правонарушений, предусмотренных гл. 7 УК РК. При этом, сравнивая показатели 2018 и 2021 гг., мы наблюдаем колоссальный рост преступлений — более чем в 40 раз (рис. 2) [16].

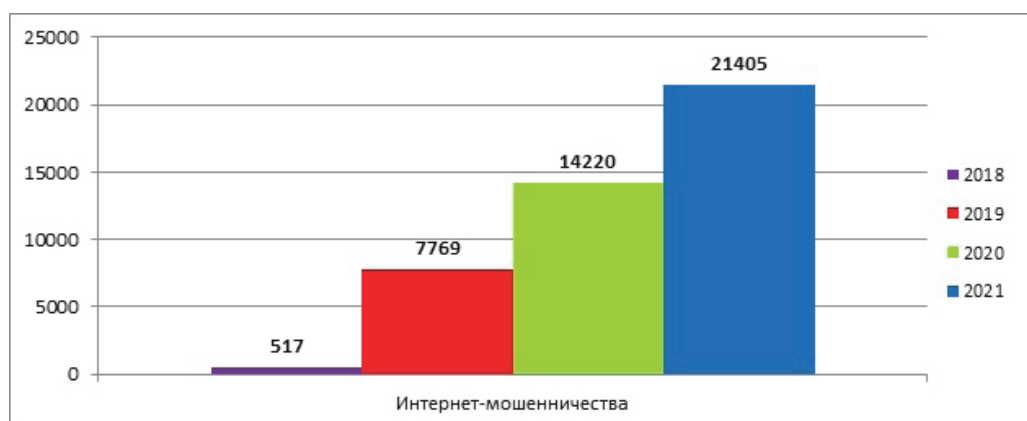


Рис. 2. Рост фактов регистрации интернет-мошенничеств в период с 2018 по 2021 г.

Наблюдая рост регистрации интернет мошенничеств, можно сделать вывод, с одной стороны, о недостаточности и малоэффективности проводимых мер по предупреждению и профилактике данных деяний; с другой стороны, о доверчивости и правовой неграмотности граждан, бесконтрольном распространении мошеннических мобильных приложений, об открытой рекламе финансовых интернет-пирамид, малоэффективности существующих мер киберзащиты платёжных интернет-платформ, нехватке специалистов по кибербезопасности и др.

Наряду с показателями регистрации всех рассматриваемых деяний, ещё одним элементом, характеризующим динамику киберпреступности, является коэффициент раскрываемости.

В Республике Казахстан данный показатель составляет 31,65% по делам об интернет-мошенничествах и 72,7% по всем уголовным делам, начатым по фактам совершения уголовных правонарушений, предусмотренных гл. 7 УК РК. Складывается данный показатель из процента уголовных дел, направленных в суд, и уголовных дел, производство по которым прекращено. Следует отметить, что при анализе данных и подсчёте процентного соотношения было учтено не количество уголовных дел, зарегистрированных в ЕРДР за тот или иной период, а количество уголовных дел, находящихся в производстве, в том числе — уголовных дел прошлых лет, что отражает более точную динамику.

Таблица 2

Количество уголовных дел, находящихся в производстве, направленных в суд и прекращённых в 2018–2021 гг., начатых по фактам интернет-мошенничества, и процентный показатель раскрываемости

Интернет-мошенничество	2018			2019			2020			2021		
	Всего в про-извод	На-прав-лено в суд	прекр.	Всего в про-извод	На-прав-лено в суд	прекр.	Всего в про-извод	На-прав-лено в суд	прекр.	Всего в произ-вод	На-прав-лено в суд	прекр.
	535	127	142	8210	669	1581	15058	1683	1950	23351	3054	2858
	Процент раскрываемо-сти =50,2%			Процент раскрывае-мости =27,4%			Процент раскрываемо-сти =24%			Процент раскрываемо-сти =25%		
	Общий процент раскрываемости=31,65%											

Таблица 3

Количество уголовных дел, по фактам уголовных правонарушений, предусмотренных главой 7 УК РК, находящихся в производстве, направленных в суд и прекращённых в 2018–2019 гг., и процентный показатель их раскрываемости

Уголовное правонарушение	2018				2019			
	Всего в про-извод	Направлено в суд	прекр.	% раскры-ваемости	Всего в про-извод	Направлено в суд	прекр.	% раскры-ваемости
Всего	168	6	83	52,9%	147	11	92	70%
Ст. 205 УК РК	89	1	29	33,7%	77	0	42	54,5%
Ст. 206 УК РК	31	3	18	67,7%	14	1	13	100%
Ст. 207 УК РК	7	0	7	100%	8	2	2	50%
Ст. 208 УК РК	15	1	5	40%	22	7	13	91%
Ст. 209 УК РК	1	0	0	0%	1	0	1	100%
Ст. 210 УК РК	7	0	7	100%	4	1	3	100%
Ст. 211 УК РК	14	1	13	100%	13	0	10	77%
Ст. 212 УК РК	1	0	0	0%	2	0	1	50%
Ст. 213 УК РК	3	0	3	100%	7	0	7	100%

Таблица 4

Количество уголовных дел, по фактам уголовных правонарушений, предусмотренных главой 7 УК РК, находящихся в производстве, направленных в суд и прекращённых в 2020–2021 гг., и процентный показатель их раскрываемости

Уголовное правонарушение	2020				2021			
	Всего в про-извод	Направлено в суд	прекр.	% раскры-ваемости	Всего в про-извод	Направлено в суд	прекр.	% раскры-ваемости
Всего	110	3	95	89%	120	15	80	79%
Ст. 205 УК РК	71	1	57	81,6%	75	2	52	72%
Ст. 206 УК РК	12	0	6	50%	16	4	10	87,5%
Ст. 207 УК РК	4	1	2	75%	2	2	0	100%
Ст. 208 УК РК	12		12	100%	11	3	7	91%
Ст. 209 УК РК	0	0	0	100%	0	0		100%
Ст. 210 УК РК	5		1	20%	6	3	2	83%
Ст. 211 УК РК	12	1	11	100%	8		8	100%
Ст. 212 УК РК			1	0%	1		0	0%
Ст. 213 УК РК	4		4	100%	1	1	0	100%

Анализ представленных в таблицах данных позволяет констатировать следующее:

1) наивысший процент раскрываемости уголовных дел (от 75 до 100%), расследуемых по фактам правонарушений, совершённых в сфере информатизации и связи, приходится на деяния, предусмотренные статьями:

- 207, 210, 211 и 213 УК РК в 2018 г.;
- 206, 209, 210, 213 УК РК в 2019 г.;
- 205, 207, 208, 211, 213 УК РК в 2020 г.;
- по всем уголовным правонарушениям, кроме статьи 212 УК РК в 2021 г.;

2) наименьший процент раскрываемости уголовных дел (до 75%), расследуемых по фактам правонарушений, совершённых в сфере информатизации и связи, приходится на деяния, предусмотренные статьями:

- 205, 206, 208, 209 УК РК в 2018 г.;
- 205, 207, 212 УК РК в 2019 г.;
- 206, 210 УК РК в 2020 г.;
- 212 УК РК в 2021 г.;
- нулевой процент раскрываемости наблюдается только по статьям 209 и 212 в 2018 г., опять же по статье 212 УК РК в 2020 и 2021 гг.;
- по уголовным правонарушениям, связанным с интернет-мошенничествами, наивысший процент раскрываемости наблюдается только в 2018 г. На протяжении последующих трёх лет (2019–2021 гг.) процент раскрываемости не превышает отметки в 25%. Наименьший процент раскрываемости приходится на 2020 г. (24%).

Указанные выводы свидетельствуют о том, что в целом, по фактам совершения уголовных правонарушений, ответственность за которые предусмотрена в статьях гл. 7 УК РК, проводится достаточно эффективная работа по предупреждению и профилактике, результатами которых является высокий процент раскрываемости уголовных правонарушений и сокращение фактов их совершения.

Вместе с тем, не следует оставлять без внимания следующие уголовные правонарушения:

- создание и использование вредоносных компьютерных программ (ст. 210 УК РК). Регистрация данного правонарушения стабильна на протяжении всего анализируемого периода, что указывает на недостаточную работу по предупреждению данных уголовных правонарушений;
- предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212 УК РК), процент раскрываемости которого имеет нулевой показатель.

В этой связи следует активизировать работу по выявлению и предупреждению выше указанных уголовных правонарушений.

Соответственно, результаты проведенного исследования указывают на определенную положительную динамику в части уголовных правонарушений, предусмотренных главой 7 УК РК, однако ситуация с регистрацией и раскрытием интернет-мошенничеств оставляет желать лучшего.

Несмотря на то, что подавляющее большинство причин, как было отмечено выше, носит объективный характер, выявленная отрицательная тенденция ещё раз доказывает необходимость совершенствования мер по борьбе с интернет-мошенничествами, повышения эффективности деятельности органов расследования и проведения результативной работы по предупреждению и профилактике данных деяний.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Баширов А. В Вопросы информационной безопасности в Республике Казахстан // Актуальные проблемы современности. 2015. № 4 (10). С. 59–61.
2. Ханов Т. А., Жиенбеков Ж. Е. Система обеспечения информационной безопасности // Актуальные проблемы современности. 2016. № 2 (12). С. 37–43.
3. Жетпісов А. Ж. О необходимости защиты информации в сфере деятельности, связанной с выявлением и раскрытием преступлений // Актуальные проблемы современности. 2018. № 3 (21). С. 68–72.

4. Новичков В. Е., Пыхтин И. Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Психопедагогика в правоохранительных органах. 2018. № 2 (73). С. 25–29.
5. Шабуров А. С., Зонова В. Э., Рыжук Н. С. Защита критической информационной инфраструктуры в соответствии с требованиями по обеспечению безопасности информации // Инновационные технологии: теория, инструменты, практика. 2018. Т. 1. С. 397–403.
6. Курбатов Н. М. О формировании правовых и научных основ обеспечения безопасности критической информационной инфраструктуры Российской Федерации // Вестник Удмуртского университета. Серия: Экономика и право. 2019. Т. 29. № 5. С. 644–654.
7. Герке Марко. Понимание киберпреступности: явление, задачи и законодательный ответ. URL: [https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime 2014_R.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime%2014_R.pdf) (дата обращения: 08.02.2022);
8. Михайлов Б. П., Хазов Е. Н., Богданов А. В. и др. Особенности противодействия киберпреступности подразделениями уголовного розыска : учебное пособие. М. : Юнити-Дана, 2016. 151 с.
9. Кюютин В. Г., Новиков А. П. Правовое регулирование борьбы с киберпреступностью, кибертерроризмом и трафиком людей: опыт Европейского Союза. Бишкек; Москва : Кыргызско-Российский Славянский университет, 2010. 240 с.
10. Ханов Т. А., Нуркеев А. Ж. Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений // Известия Алтайского государственного университета. 2017. № 6 (98). С. 105–111.
11. Российская Ассоциация Электронных Коммуникаций (РАЭК). Глобальные киберугрозы: возможно ли безопасное развитие цифровой инфраструктуры? URL: (<http://raec.ru/live/raec-news/9471/>) (дата обращения: 09.02.2022).
12. Информационный портал «Zakon.kz» Как интернет-мошенники обманывают казахстанцев. URL: <https://www.zakon.kz/4927774-kak-internet-moshenniki-obmanyvayut.html> (дата обращения: 09.02.2022).
13. Новостной портал «Tengrinews». Количество интернет-мошенничеств резко возросло в Казахстане (от 22.01.2021). URL: <https://tengrinews.kz/crime/kolichestvo-internet-moshennichestv-rezko-vozroslo-454633/> (дата обращения: 09.02.2022).
14. Горбунова А. В МВД рассказали о самых популярных видах интернет-мошенничества в Казахстане // ForbesKazakhstan. URL: https://forbes.kz/process/probing/samyie_populyarnyie_vidyi_internet-moshennichestva_v_kazahstane_nazvali_v_mvd (дата обращения: 09.02.2022).
15. Статистические данные — сведения об уголовных правонарушениях за 2018–2021 год. URL: <https://qamqor.gov.kz> (дата обращения 09.02.2022).
16. Алмазқызы А. Киберқылмыстылық — Қазақстан республикасының қауіпсіздігіне жаңа қылмыстық қауіптерінде // Вестник Казахского национального университета. Серия юридическая. 2018. Т. 88, № 4. С. 142–151.