

## ИСТОРИЯ РАЗВИТИЯ УГОЛОВНО-ПРАВОВЫХ НОРМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ



М.С. ЗАРКЕНОВ,  
магистр юр.н., докторант Академии  
правоохранительных органов  
при Генеральной прокуратуре  
Республики Казахстан,  
(п. Косшы, Акмолинская обл., РК),  
e-mail: zarkenov@gmail.com

Многие люди проводят большую часть своей повседневной жизни в киберпространстве, создавая и наслаждаясь новыми типами социальных отношений, которые были невозможны или финансово недоступны 30 лет назад. Однако преступники в сфере информационных технологий нашли свою нишу в этой области, поэтому риски и угрозы также возросли. В настоящее время компьютерные преступления особенно актуальны, поскольку обладают высокой степенью общественной опасности и особенностями, делающими киберпреступников опасными и неуязвимыми. *Предмет исследования* – история развития уголовно-правовых норм в сфере информационных технологий. *Цель исследования* – историко-правовой анализ уголовно-правовых норм в сфере информационных технологий, исследование процесса появления и развития компьютерных преступлений, выделение этапов эволюции информационных технологий, породивших новую сферу общественных отношений.

*Методы научного исследования:* достижение цели настоящей статьи и решение поставленных задач потребовали применения методов общего и частного характера. Так, общенаучными методами выступили: анализ, синтез, индукция, дедукция. Частно-правовыми методами, использованными в статье, являются методы юридико-догматический, историко-правовой. *Научная новизна* статьи определяется тем, что в данном историко-правовом анализе уголовного права в области информационных технологий впервые раскрываются причины, побудившие мировое сообщество принять законы о правовом регулировании в области информационных технологий. Проанализирована статистика роста персональных компьютеров, пользователей Интернета, а также ущерба, причиненного преступлениями в сфере информационных технологий. *Основные выводы:* 1) статистика роста числа персональных компьютеров, пользователей Интернета, а также ущерба, причиненного преступлениями в сфере информационных технологий, свидетельствуют о том, что они явились одними из условий и причин роста числа преступлений в сфере информационных технологий; 2) предложены этапы развития целого направления правовых норм, регулирующих сферу информационных технологий.

*Ключевые слова: история компьютерных преступлений; ЭВМ; персональный компьютер; интернет; компьютерные преступления; киберпреступность; кибербезопасность; информационные технологии; развитие правовых норм, регулирующих сферу информационных технологий; уголовные правонарушения в сфере информационных технологий.*

## **Введение**

Первоисточником, побудившим мировое сообщество принять закон о правовом регулировании в области информационных технологий, является электронная вычислительная машина (далее – ЭВМ). В первой половине XX века стремительное развитие ЭВМ привело к тому, что с ее помощью осуществлялись одни из первых взломов вычислительных машин во Вторую мировую войну. Так, расшифрованы секретные коды немецкой шифровальной машины «Энигма». В результате чего, перехватывались сообщения германского подводного флота, отслеживались перемещения подводных лодок.<sup>1</sup>

## **Основные положения**

Основными положениями данной статьи являются выявление некоторых условий и причин роста числа уголовных правонарушений в сфере информационных технологий, предлагаемые этапы развития целого направления правовых норм, регулирующих сферу информационных технологий.

## **Материалы и методы**

В целях исследования проблемы изучены и проанализированы научные источники, законодательство Республики Казахстан и зарубежных стран, статистические материалы. При проведении научного исследования использовались следующие методы: анализ и синтез, индукция и дедукция, логический, юридико-догматический, историко-правовой.

## **Результаты исследования**

### **1. Появление персонального компьютера**

По мнению А.И. Сотова, ЭВМ есть результат развития автоматических устройств, и ее отличительной особенностью является возможность не только воспринимать сигналы из внешнего мира, но и обрабатывать эту информацию.<sup>2</sup> До 70-х годов XX века ЭВМ пользовался небольшой круг людей, этому соответствовали ограниченное количество ЭВМ высокая стоимость аппарата, внушительность размера и отсутствие у людей специальных знаний по применению ЭВМ. В 1971 году изобретение микро-

---

<sup>1</sup>Lee J.A.N., Holtzman G. 50 Years after breaking the codes: interviews with two of the Bletchley Park scientists // IEEE Annals of the History of Computing, 1995. Т. 17. № 1. – P. 32–43; Eldridge J. Alan Turing. A&C Black, 2013.

<sup>2</sup>Сотов А.И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации: монография. М.: Изд-во «Русайнс», 2017. С. 128.

процессора (который вместил в себя всю мощь компьютерной системы, занимавший целую комнату) стало первым шагом к появлению персонального компьютера.<sup>3</sup> Это привело к массовому производству небольших и недорогих персональных компьютеров. В результате, к 2000 году во всем мире насчитывалось 140 миллионов персональных компьютеров (в 2008 году – свыше 1 млрд., 2010 году – свыше 1,3 млрд.).<sup>4</sup>

В свою очередь, появление персонального компьютера в руках разного рода пользователей способствовало прорыву во всех сферах общественных отношений. В том числе, стало орудием в руках преступника. С тех пор, количество уголовных правонарушений, совершаемых преступниками в данной сфере, во всем мире растет в геометрической прогрессии. Особенностями уголовных правонарушений в данной сфере является латентность, трансграничность, моментальность исполнения преступления. Все эти факторы придают сложность выявлению и раскрытию совершенных уголовных правонарушений. К примеру, в США преступления в сфере информационных технологий впервые получили публичную огласку только в середине 70-х годов XX века. В силу своей латентности большинство из выявленных в этот период времени уголовных правонарушений были совершены двадцатью годами ранее.<sup>5</sup>

Естественно, что все выявленные уголовные преступления, совершенные с использованием информационных технологий, составляют лишь малую долю всех преступлений, совершенных в этой сфере. При этом, большинство выявленных уголовных правонарушений не находят своего логического завершения и остаются нераскрытыми. Тем не менее, одно из первых раскрытых компьютерных преступлений совершил в США Альфонс Конфессоре, ущерб от которого составил 620 тысяч долларов (в 1969 г.).<sup>6</sup>

Первое преступление в сфере информационных технологий на территории бывшего СССР было совершено в городе Вильнюсе, от которого ущерб составил 78,5 тысячи рублей (в 1979 г.).<sup>7</sup> Год за годом аналогичные преступления совершались все чаще. Эти преступления стали одним из первых вызовов государственным системам, которые не были готовы противостоять им.

## 2. Появление Интернета

Вслед за массовыми продажами персональных компьютеров, которые привели к росту преступлений в сфере информационных технологий, пришел новый научно-

---

<sup>3</sup>Иванько А.Ф. Структура и архитектура микропроцессоров современных персональных электронных вычислительных машин. М.: Изд-во МГУП, 2000. С. 84; Berlin L. The man behind the microchip: Robert Noyce and the invention of Silicon Valley. Oxford University Press, 2005.

<sup>4</sup>Андронов Ю. Компьютеры: гонка преследования // Вокруг света. № 12 (2855). Москва, 2011. – С. 202-206.

<sup>5</sup>Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: Дис. ... канд. юрид. наук. М., 2002. С. 166; Мальковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: Дис. ... канд. юрид. наук. М., 2006. С. 186.

<sup>6</sup>McKnight G. Computer crime / Michael Joseph, 1973. P. 221.

<sup>7</sup>Батурин Ю.М. Проблемы компьютерного права. М.: Юрид. лит., 1991. С. 271.

технический прорыв, который вывел данный вид преступления в киберпространство. Этому способствовала необходимость обмена информацией между персональными компьютерами.

В 1961 году Агентством передовых исследований Министерства обороны США (Advanced Research Agency – ARPA) начато исследование по созданию сети «Arpanet» для изучения методов обеспечения связи между компьютерами различных типов. В результате успешных исследований, данная сеть в 1975 году превратилась в рабочую сеть для узкого круга организаций. В 1983 году из «Arpanet» отделилась сеть «Milnet» для обеспечения Министерства обороны США. В последующем протокол TCP/IP перешел в общедоступный режим, а сети «Arpanet», «Milnet» и другие сети были объединены в единую сеть «Internet». <sup>8</sup> Термин «Интернет» был закреплен в решении от 24.10.1995 года, утвержденном Федеральным сетевым советом (США). <sup>9</sup>

В данном случае ход развития интернета аналогичен с историей персональных компьютеров. Также, по мере развития глобальная сеть распространилась от узкого пользователя до широкого его круга. К примеру, в 2000 году насчитывалось 400 миллионов пользователей глобальной сети (свыше 6,5% мирового населения), 2005 году – 1 млрд. (16,8%), 2010 году – 2 млрд. (29,3%), 2015 году – 3,2 млрд. (41,5%), 2017 году – 3,5 млрд. (49%), 2018 году – 3,9 млрд. (51,4%), 2019 году – 4,1 млрд. (53,6%). <sup>10</sup>

Пользователей сети интернет в Республике Казахстан в 2000 году насчитывалось 70 тыс. человек (0,5%), <sup>11</sup> 2005 году – 608 тыс. (4%), 2006 году – 1,2 млн. (8,3%), 2007 году – 2,1 млн. (13,7%), 2008 году – 2,3 млн. (15,1%), 2009 году – 2,9 млн. (18,2%), 2010 году – 5,1 млн. (31,6%), 2011 году – 8,4 млн. (50,6%), 2012 году – 10,4 млн. (61,9%), 2013 году – 10,8 млн. (63,3%), 2014 году – 11,1 млн. (63,9%), 2015 году – 12,8 млн. (72,9%), 2016 году – 13,7 млн. (76,8%), 2017 году – 14,3 млн. (78,8%), 2018 году – 14,9 млн. (81,3%), 2019 году – 15,6 млн. (84,2%). <sup>12</sup>

Естественно, быстрому росту существенно способствовал мобильный широкополосный доступ к сети интернет, снижение тарифных планов <sup>13</sup> и доступность смартфонов. К тому же, деятельность данной сети по настоящее время дополняется разными службами и сервисами. Каждый второй человек на планете связан с электронно-вычислительными машинами, и большинство сфер занятости осуществляют свою деятельность с помощью информационных технологий. Такое развитие глобальной сети все больше привлекает киберпреступников со всего мира.

<sup>8</sup>Lawrence E. Evans, Jr. Internet Overview // ТЕР. В. J. № 63. 2000. P. 227.

<sup>9</sup>Антофеев А.Д. Об историческом и этимологическом аспектах кибер-буллинга (интернет-травли) как социально-правового явления // Безопасность: Информация, Техника, Управление. 2020. – С. 43–48.

<sup>10</sup>International Telecommunication Union statistics // International Telecommunication Union. URL: <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx> (30.06.2020).

<sup>11</sup>Statistics // Kazakhstan Internet Usage and Telecommunications Reports. Internet World Stats. URL: <https://www.internetworldstats.com/asia/kz.htm> (30.10.2019).

<sup>12</sup>Официальная статистика РК // Комитет по статистике Министерства национальной экономики Республики Казахстан URL: <https://stat.gov.kz/official/industry/29/statistic/7> (25.04.2020).

<sup>13</sup>Каррьев Б.С. Интернет, краткая история и влияние на общество // Москва: LAP LAMBERT Academic Publishing, 2015.

Убытки, понесенные от преступлений в сфере информационных технологий, колоссальны и довольно трудно поддаются оценке. Основными целями преступников являются финансовые организации. Например, в 2012 году клиентам дистанционного банковского обслуживания в Российской Федерации нанесен ущерб в размере 446 млн. долларов.<sup>14</sup> В период с августа 2015 года по февраль 2016 года преступной группой «Buhtrap» совершены компьютерные атаки на банки Российской Федерации в результате которых похищены денежные средства в размере 1,8 млрд. рублей.<sup>15</sup> Согласно подсчетам украинской киберполиции в 2019 году от совершенных преступлений в сфере информационных технологий украинцам нанесен ущерб около 1 млн. долларов.<sup>16</sup> Во второй половине 2019 года около 1 тысячи клиентов Народного банка Республики Казахстан стали жертвами хакеров.<sup>17</sup>

Только за 2014 год мировой ущерб от преступлений в сфере информационных технологий составил 445 млрд. долларов.<sup>18</sup> По подсчетам за 2017 год мировой ущерб составил около 600 млрд. долларов, который равен 0,8% мирового ВВП. За три года ущерб от преступлений в сфере информационных технологий вырос на 35%. Причинами увеличения преступности явились использование новых технологий, широкое применение черного рынка и цифровых валют.<sup>19</sup> При этом, по данным ООН ежегодный ущерб от преступлений в сфере информационных технологий составляет 1,5 трлн. долларов.<sup>20</sup> Тем временем, с 2015 по 2017 годы банки второго уровня Республики Казахстан от данного вида преступлений понесли ущерб на сумму 2 млрд. 72 млн. тенге.<sup>21</sup>

### 3. Криминализация преступлений в сфере информационных технологий

В результате развития научного прогресса новые технологии проникли во все сферы жизнедеятельности человечества в том числе, в стратегически важные объекты государств (объекты электроснабжения, водоснабжения, системы телекоммуникации и связи, атомной станции, транспортные и оборонные системы и т.д.). Так, преступления в сфере информационных технологий стали существенной угрозой для человека и государства. Вследствие чего, мировое научное сообщество

<sup>14</sup>Безопасная система ДБО // Tadviser. URL: <https://www.tadviser.ru> (11.03.2020).

<sup>15</sup>BUNTRAP. Эволюция целенаправленных атак на банки // Group-IB, 2016. – С. 27.

<sup>16</sup>Потери организаций от киберпреступности // Tadviser. URL: <https://www.tadviser.ru> (11.03.2020).

<sup>17</sup>Муканова Ж. Уже более 1 тыс. клиентов Народного банка стали жертвами хакеров // Newtimes.kz. URL: <https://newtimes.kz/proishestviya/93701-uzhe-bolee-1-tys-klientov-narodnogo-banka-stali-zhertvami-khakerov> (11.03.2020).

<sup>18</sup>Net Losses: Estimating the global cost of cybercrime. Economic impact of cybercrime II // McAfee, Centre for Strategic & International Studies, 2014. P. 24.

<sup>19</sup>Lewis J. Economic Impact of Cybercrime, No Slowing Down // McAfee, 2018. P. 28.

<sup>20</sup>В \$1,5 трлн. оценил генсек ООН ежегодный ущерб от киберпреступности // Kaztag.kz. URL: <https://kaztag.kz/ru/news/v-1-5-trln-otsenil-gensek-oon-ezhegodnyy-ushcherb-ot-kiberprestupnosti> (11.03.2020).

<sup>21</sup>Бижикеева М. Спрос рождает покушения // Kapital.kz. URL: <https://kapital.kz/finance/79373/spros-rozhdayet-pokusheniya.html> (25.04.2020).

пришло к общему мнению о криминализации общественно опасных деяний в сфере информационных технологий.

История развития законодательства в области информационных технологий началась в 1973 году в Швеции, где был принят закон «О данных», в котором требовалось, чтобы информационные системы, обрабатывающие персональные данные были лицензированы государственным органом, известным как Совет по проверке данных. С некоторыми изменениями другие скандинавские страны смоделировали свои собственные законы о защите данных по образцу шведского закона.<sup>22</sup> Вслед за ними, в том же году Риксдаг (Парламент Швеции) принял закон «О вычислительной технике». Данный закон криминализировал ряд деяний за нарушение прав личности с помощью ЭВМ.<sup>23</sup>

В 1978 году Федеративная Республика Германия стала второй страной в мире, принявшей всеобъемлющий закон о защите данных. Развитие немецкого законодательства началось еще в 1973 году, когда Бундестаг начал рассматривать необходимость юридического механизма для защиты немецких граждан от потенциальных злоупотреблений, возникающих в результате автоматической обработки персональных данных.<sup>24</sup>

Так, в 1977 году в Соединенных Штатах Америки впервые был подготовлен законопроект федерального закона «О защите федеральных компьютерных систем».<sup>25</sup> На основании, которого в 1984 году во время всеобъемлющего пересмотра уголовного кодекса США президентом США Р. Рейганом был подписан закон «О всеобъемлющем контроле над преступностью», содержащий в себе закон «О компьютерном мошенничестве». В 1986 году закон был изменен и переименован в закон «О компьютерном мошенничестве и злоупотреблениях (CFAA)».<sup>26</sup> Данный закон запрещает доступ к компьютеру без разрешения или с превышением разрешения, имеет положения касательно распространения вредоносного кода и компьютерных атак с целью «отказа в обслуживании». Помимо этого, криминализирован незаконный оборот паролей и иных вещей.<sup>27</sup>

В 1978 году впервые было введено юридическое понятие «компьютерное преступление» в законодательство штата Флориды. Однако, конкретного понятия данного вида преступления отсутствовало. Вместе с тем, объявлялось незаконным уничтоже-

---

<sup>22</sup>Madsen W. *Western European Initiatives // Handbook of Personal Data Protection*. Palgrave Macmillan, London, T. 1026. 1992. – P. 22-86; Bennett C.J. *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press, 1992. P. 63.

<sup>23</sup>Баранов А.А., Брыжко В.М., Базанов Ю.К. *Права человека и защита персональных данных // Киев: Государственный комитет связи и информатизации Украины, 2000. С. 280.*

<sup>24</sup>Madsen W. *Western European Initiatives // Handbook of Personal Data Protection*. Palgrave Macmillan, London, T. 1026. 1992. – P. 22–86.

<sup>25</sup>Волеводз А.Г. *Противодействие компьютерным преступлениям: правовые основы международного сотрудничества*. М.: Издательство «Юрлитинформ», 2002. С. 496.

<sup>26</sup>Marshall J.H. *Prosecution of Computer*. Office of Legal Education Executive Office for United States Attorneys // J.H. Marshall, M.W. Bailie. T. 207. 2010.

<sup>27</sup>Computer Fraud and Abuse Act № 1030 18 U.S., 1986 // Law.cornell.edu. URL: <https://www.law.cornell.edu/uscode/text/18/1030> (18.02.2020).

ние, модификация, несанкционированный доступ либо изъятие содержащихся в ЭВМ данных, программного обеспечения и соответствующей документации. Максимальное наказание за данное преступление предусматривалось до 5 лет лишения свободы и штраф в размере до 5 тысячи долларов либо сумма, равная двойной денежной прибыли, полученной преступником в результате правонарушения.<sup>28</sup>

В 1979 году на конференции ассоциации адвокатов в г. Далласе впервые были предложены следующие признаки преступлений в сфере информационных технологий:

- использование или попытка использования какой-либо ЭВМ или сети компьютеров с целью получения выгоды или услуг под прикрытием фиктивных предлогов;
- умышленное делинквентное поведение, направленное на изменение, повреждение, уничтожение или похищение ЭВМ, сети компьютеров или имеющихся в них информации или программного обеспечения;
- умышленное неправомерное нарушение связи между ЭВМ или сетями компьютеров.<sup>29</sup>

Кроме того, цепочка истории развития уголовно-правовых норм в области информационных технологий получила свое начало и в Великобритании, на что существенно повлиял инцидент со взломом системы «British Telecom's Prestel». Так, в период с конца 1984 года по 1985 год Р. Шифрин и С. Голд с помощью персонального компьютера и модема получили неправомерный доступ к «British Telecom's Prestel». При интернет-серфинге Р. Шифрином был обнаружен пароль от компьютера инженера «British Telecom's Prestel» (имя пользователя инженера «22222222», пароль «1234»).<sup>30</sup> С помощью этой информации ими была исследована система «British Telecom», в частности получен доступ к личному ящику принца Филиппа. Однако, взломы в систему «British Telecom» были обнаружены, и Р. Шифрину и С. Голду предъявлено обвинение в мошенничестве согласно разделу 1 закона «О подделке и подделке документов» (1981 года). По словам Р. Шифрина: «Обвинение утверждало, что ввод чьего-либо пароля в компьютер, чтобы компьютер мог проверить, верен он или нет, равносильно написанию их подписи на чеке». Судом Р. Шифрин и С. Голд признаны виновными и оштрафованы на 750 и 600 фунтов стерлингов. Данное решение было отменено Уголовной палатой Апелляционного суда. Доводами к оправданию послужили отсутствие доказательств того, что инцидент совершен в целях получения материальной выгоды и неправильное применение закона «О подделке и подделке документов». Лорд-судья Брендон заявил, что: «В результате рассмотрения этого дела мы пришли к выводу, что формулировки существующего закона не были предназначены для применения к этой ситуации. Это не уголовное преступление. Если это будет сочтено желательным, то это вопрос для законодательной власти, а не для судов».

<sup>28</sup>Florida Computer Crimes Act № 1305 Chapter 815. During its Second Regular Session April 4, 1978 through June 2, 1978 and the Special Session June 7, 1978 through June 8, 1978. – P. 139-142.

<sup>29</sup>Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия–телеком, 2002. С. 181.

<sup>30</sup>Murray A. Information technology law: the law and society / Oxford University Press, 2016. P. 653.

Решение лордов заставило многих ученых-юристов поверить в то, что взлом не был незаконным в соответствии с действующим законодательством.<sup>31</sup> Таким образом, дело выявило пробелы в законе и в 1990 году привело к принятию Закона «О неправомерном использовании компьютеров», первого закона Великобритании о взломе компьютеров. В дальнейшем криминализация преступлений в сфере информационных технологий были приняты в Германии, Канаде, Франции, Австралии и других странах.

Уголовная ответственность за преступления в сфере информационных технологий на территории Республики Казахстан появилась значительно позже, чем в западных странах. Это обусловлено невысоким уровнем компьютеризации советского общества и отсутствием рассмотрения проблем преступности в сфере информационных технологий. Ученые считали, что преступление в сфере информационных технологий – это явление, присущее только зарубежным странам, которое по причине недостаточного внедрения в производственные и общественные отношения информационных технологий не может представлять общественную опасность.<sup>32</sup>

Стремительное развитие информационных технологий не обошло стороной и Советский Союз. В 1979 году в г. Вильнюсе было совершено первое преступление в сфере информационных технологий,<sup>33</sup> которое стало отправной точкой для формирования правовых норм в сфере компьютерных технологий. В 1997 году в Республике Казахстан впервые введена уголовная ответственность за неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ (статья 165-4 УК).<sup>34</sup>

В заключение исследования нам хотелось бы привести пример нынешней ситуации в Палестине, где отсутствие сдерживающего законодательства по борьбе с преступлениями в сфере информационных технологий, а также широкое использование интернета и социальных сетей привели к росту числа этих преступлений.<sup>35</sup> Такая ситуация показывает, насколько важно своевременно принимать меры по противодействию уголовным правонарушениям в сфере информационных технологий. Поскольку эпоха цифровой революции создает новые цифровые активы, меняет представления о праве и правовых институтах, порождает не только дигитализацию права, но и цифровые формы реализации многих конституционно-правовых институтов.<sup>36</sup> Таким образом, построение успешного и эффективного механизма правопо-

---

<sup>31</sup>Leyden J. 80s hacker turned journo, IT crime ace Steve Gold logs off // The Register. URL: [https://www.theregister.com/2015/01/13/steve\\_gold\\_obit/](https://www.theregister.com/2015/01/13/steve_gold_obit/) (11.03.2020).

<sup>32</sup>Доронин А.М. Уголовная ответственность за неправомерный доступ к компьютерной информации: Дис. ... канд. юрид. наук. М., 2003. С. 154.

<sup>33</sup>Батурич Ю.М. Проблемы компьютерного права. М.: Юрид. лит., 1991. С. 271.

<sup>34</sup>Уголовный кодекс Казахской ССР от 22 июля 1959 г. // ИПС «Эдилет». URL: [http://adilet.zan.kz/rus/docs/K590002000\\_](http://adilet.zan.kz/rus/docs/K590002000_) (18.02.2020).

<sup>35</sup>Elshobake M.R.M., Laeba M. The Legal Framework of Cybercrime in Palestine // Arab Law Quarterly. 2021. Т. 1. № аор. – Р. 1–18.

<sup>36</sup>Кравец И.А. Цифровой конституционализм и будущее информационного общества (в контексте глобализации и интеграционных процессов) // Право и государство, 2020. № 3-4 (88-89). – С. 85-104.

го регулирования противодействия уголовным правонарушениям в сфере информационных технологий невозможно без должного внимания к историческим предпосылкам ее возникновения и развития.<sup>37</sup>

### Обсуждение

Основные условия и причины роста числа преступлений в сфере информационных технологий, установленные по результатам исследования, наглядно свидетельствуют о возникновении данного рода преступлений и их дальнейшем росте. Между тем, этапы развития новой для общества сферы обосновываются в статье развитием научно-технических средств, появлением компьютерных преступлений и правовых норм, регулирующих сферу информационных технологий. При этом, учитывая недостаточность исследований в рассматриваемой области, положения, предложенные в статье, имеют значительную научную и практическую значимость.

### Заключение

Подводя итоги исторического развития правовых норм, регулирующих сферу информационных технологий, следует отметить, что данная статья демонстрирует процесс развития истории новой сферы общественных отношений, возникшей в результате научно-технического прогресса. История также показывает, что появление преступлений в сфере информационных технологий, изначально недооцененных государствами, привело к разработке целого направления (блока) правовых норм, регулирующих сферу информационных технологий. Между тем, правовые меры по пресечению общественно опасных деяний в сфере информационных технологий заняли свое место в законодательстве большинства стран мира.

Проанализировав историю развития преступлений в сфере информационных технологий, мы предлагаем несколько этапов в развитии информационных технологий, которые породили новую сферу общественных отношений:

- 1 – этап развития вычислительных машин;
- 2 – этап компьютеризации и формирования информационных отношений;
- 3 – этап глобализации сети интернет;
- 4 – этап становление преступлений в сфере информационных технологий (увеличение количества преступлений и наносимого вреда, новые специализации злоумышленников, транснациональность преступлений). На данном этапе, пытались применить действующие на тот момент, традиционные правовые нормы;
- 5 – этап становления информационного пространства на национальном и международном уровнях;
- 6 – этап криминализации уголовных правонарушений в сфере информационных технологий;

---

<sup>37</sup>Apenov S.M. et al. International crime as a threat to global socio-economic security // Int. J. Electronic Security and Digital Forensics. 2021. Т. 13. №. 2. – P. 133–154.

7 – этап комплексного противодействия преступлениям в сфере информационных технологий. На этом этапе создается целый блок правовых норм, регулирующих сферу информационных технологий, как на национальном уровне, так и на международной арене.

**М.С. Заркенов, заң ғылымдарының магистрі, Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының докторанты (Қосшы к., Ақмола облысы, Қазақстан): Ақпараттық технологиялар саласындағы қылмыстық-құқықтық нормалардың даму тарихы.**

Әлеуметтік қатынастардың жаңа типтерін жасай және рахатын көре отырып, көптеген адамдар күнделікті өмірінің біршама бөлігін киберкеңістікте өткізеді, осыдан 30 жыл бұрын бұл мүмкін емес немесе қаржылық тұрғыдан қолжетімді емес болатын. Алайда, ақпараттық технологиялар саласындағы қылмыскерлер де осы салада өз орнын тапты, сондықтан тәуекелдер мен қатерлер де өсті. Қазіргі уақытта компьютерлік қылмыстар әсіресе өзекті, өйткені олар қоғамдық қауіптіліктің жоғары деңгейіне және киберқылмыскерлерді қатерлі және тіс батпайтын ететін ерекшеліктерге ие. Зерттеу *пәні* – ақпараттық технологиялар саласындағы қылмыстық-құқықтық нормалардың даму тарихы. Зерттеудің *мақсаты* ақпараттық технологиялар саласындағы қылмыстық-құқықтық нормаларды тарихи-құқықтық талдау, компьютерлік қылмыстардың пайда болуы мен дамуын зерттеу, әлеуметтік қатынастардың жаңа саласын тудырған ақпараттық технологиялардың даму кезеңдерін ұсыну болып табылады. *Ғылыми зерттеу әдістері*: осы мақаланың мақсатына қол жеткізу және оның алдындағы міндеттерді шешу жалпы және жеке сипаттағы әдістерді қолдануды талап етті. Олар: талдау, синтездеу, индукция, дедукция сияқты жалпы ғылыми әдістер. Мақалада қолданылған жеке-құқықтық әдістер құқықтық-догматикалық, тарихи-құқықтық әдістер болып табылады. Мақаланың *ғылыми жаңалығы* ақпараттық технологиялар саласындағы қылмыстық құқықты тарихи-құқықтық талдауда әлемдік қоғамдастықты ақпараттық технологиялар саласын құқықтық реттеу туралы заң қабылдауға итермелеген себептер алғаш рет ашылатындығымен анықталады. Дербес компьютерлердің, Интернетті пайдаланушылардың өсу статистикасы, сондай-ақ ақпараттық технологиялар саласындағы қылмыстармен келтірілген залал статистикасы талданады. *Негізгі тұжырымдар*: 1) дербес компьютерлер, Интернетті пайдаланушылар санының өсу статистикасы, сондай-ақ ақпараттық технологиялар саласындағы қылмыстармен келтірілген залал статистикасы олардың ақпараттық технологиялар саласындағы қылмыстар санының өсуінің шарттары мен себептерінің бірі болғандығын куәландырады; 2) ақпараттық технологиялар саласын реттейтін құқықтық нормалардың тұтас бағытының даму кезеңдері ұсынылды.

*Тірек сөздер*: компьютерлік қылмыстардың тарихы, ЭЕМ, дербес компьютер, интернет, компьютерлік қылмыстар, киберқылмыстылық, киберқауіпсіздік, ақпараттық технологиялар, ақпараттық технологиялар саласын реттейтін құқықтық нормалардың дамуы, ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтар.

**M.S. Zarkenov, Master of Law, Doctoral Student of the Academy of Law Enforcement Agencies under the Prosecutor General's Office of the Republic of Kazakhstan (Koshy town, Akmolinsk region): History of the development of criminal law standards in the field of information technology.**

Many people spend most of their daily lives in cyberspace, creating and enjoying new types of social relationships that were impossible or financially unaffordable 30 years ago. However, information technology criminals have found their niche in this area, so the risks and threats have also increased. Currently, computer crimes are particularly relevant, because they have a high degree of public danger and features making cybercriminals dangerous and invulnerable. The subject of the study consists in the history of the development of criminal law norms in the field of information technology. The research is aimed at the historical and legal analysis of criminal law standards in the field of information technology, investigation of the emergence and development of computer crimes, proposal of development stages of information technologies that gave rise to a new sphere of public relations. Methods of the scientific research: the achievement of the purpose of this article and the solution of problems within this task required the use of general and specific methods. Thus, the general scientific methods are: analysis, synthesis, induction, deduction. The specific legal methods used in the article are legal-dogmatic, historical-legal methods. The scientific novelty of the article is determined by the fact that this historical and legal analysis of criminal law in the field of information technology for the first time reveals the reasons that prompted the world community to adopt a law on legal regulation in the field of information technology. The article analyzes statistics on the growth of personal computers, Internet users, as well as statistics on the damage caused by crimes in the field of information technology. Key findings: 1) the statistics on the growth of the number of personal computers, Internet users, as well as statistics on the damage caused by crimes in the field of information technology, indicate that they were one of the conditions and reasons for the increase in the number of crimes in the field of information technology; 2) the stages of development of the entire series of legal standards regulating the sphere of information technologies are proposed.

*Keywords: history of computer crimes; computer; personal computer; Internet; computer crimes; cybercrime; cybersecurity; information technologies; development of legal standards regulating the field of information technologies; criminal offenses in the field of information technologies.*

**Список литературы:**

1. Андронов Ю. Компьютеры: гонка преследования // Вокруг света. № 12 (2855). М., 2011. – С. 202-206.
2. Антюфеев А.Д. Об историческом и этимологическом аспектах кибер-буллинга (интернет-травли) как социально-правового явления // Безопасность: Информация, Техника, Управление. 2020. – С. 43-48.
3. Баранов А.А., Брыжко В.М., Базанов Ю.К. Права человека и защита персональных данных. Киев: Государственный комитет связи и информатизации Украины, 2000.

4. Батурин Ю.М. Проблемы компьютерного права. М.: Юрид. лит., 1991.
5. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Издательство «Юрлитинформ», 2002.
6. Доронин А.М. Уголовная ответственность за неправомерный доступ к компьютерной информации: Дис. ... канд. юрид. наук. М., 2003.
7. Иванько А.Ф. Структура и архитектура микропроцессоров современных персональных электронных вычислительных машин. М.: Изд-во МГУП, 2000.
8. Каррыев Б.С. Интернет, краткая история и влияние на общество. М.: LAP LAMBERT Academic Publishing, 2015.
9. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия–телеком, 2002.
10. Кравец И.А. Цифровой конституционализм и будущее информационного общества (в контексте глобализации и интеграционных процессов) // Право и государство, 2020. № 3-4 (88-89). – С. 85-104.
11. Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: Дис. ... канд. юрид. наук. М., 2006.
12. Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: Дис. ... канд. юрид. наук. М., 2002.
13. Сотов А.И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации: монография. М.: Изд-во «Русайнс», 2017.
14. Apenov S.M. et al. International crime as a threat to global socio-economic security // *Int. J. Electronic Security and Digital Forensics*. 2021. Т. 13. № 2. – P. 133-154.
15. Bennett C.J. *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press, 1992.
16. Berlin L. *The man behind the microchip: Robert Noyce and the invention of Silicon Valley*. Oxford University Press, 2005.
17. Eldridge J. *Alan Turing*. A&C Black, 2019.
18. Elshobake M.R.M., Laeba M. The Legal Framework of Cybercrime in Palestine // *Arab Law Quarterly*. 2021. Т. 1. № аор. – С. 1-18.
19. Lawrence E. Evans, Jr. *Internet Overview* // *TEX. B.J.*, № 63. 2000.
20. Lee J.A.N., Holtzman G. 50 Years after breaking the codes: interviews with two of the Bletchley Park scientists // *IEEE Annals of the History of Computing*, 1995. Т. 17. № 1. – P. 32-43.
21. Madsen W. *Western European Initiatives* // *Handbook of Personal Data Protection*. Palgrave Macmillan, London, Т. 1026. 1992. – P. 22-86.
22. Marshall J.H. *Prosecution of Computer*. Office of Legal Education Executive Office for United States Attorneys / J.H. Marshall, M. W. Bailie. Т. 207. 2017.
23. McKnight G. *Computer crime* / Michael Joseph, 1973.
24. Murray A. *Information technology law: the law and society*. Oxford University Press, 2016.

**References (transliterated):**

1. Andronov Yu. Komp'yutery: gonka presledovaniya // *Vokrug sveta*. № 12 (2855). М., 2011. – S. 202-206.
2. Antyufeev A.D. Ob istoricheskom i etimologicheskom aspektah kiber-bullinga (internet-travli) kak social'no-pravovogo yavleniya // *Bezopasnost': Informaciya, Tekhnika, Upravlenie*. 2020. – S. 43-48.
3. Baranov A.A., Bryzhko V.M., Bazanov Yu.K. Prava cheloveka i zashchita personal'nyh dannyh. Kiev: Gosudarstvennyj komitet svyazi i informatizacii Ukrainy, 2000.
4. Baturin Yu.M. Problemy komp'yuternogo prava. М.: Yurid. lit., 1991.
5. Volevodz A.G. Protivodejstvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva. М.: Izdatel'stvo «Yurilitinform», 2002.
6. Doronin A.M. Ugolovnaya otvetstvennost' za nepravomernyj dostup k komp'yuternoj informacii: Dis. ... kand. jurid. nauk. М., 2003.
7. Ivan'ko A.F. Struktura i arhitektura mikroprocessorov sovremennyh personal'nyh elektronnyh vychislitel'nyh mashin. М.: Izd-vo MGUP, 2000.
8. Karryev B.S. Internet, kratkaya istoriya i vliyanie na obshchestvo. М.: LAP LAMBERT Academic Publishing, 2015.
9. Kozlov V.E. Teoriya i praktika bor'by s komp'yuternoj prestupnost'yu. М.: Goryachaya liniya–telekom, 2002.
10. Kravec I.A. Cifrovoj konstitucionalizm i budushchee informacionnogo obshchestva (v kontekste globalizacii i integracionnyh processov) // *Pravo i gosudarstvo*, 2020. № 3-4 (88-89). – S. 85-104.
11. Malykovcev M.M. Ugolovnaya otvetstvennost' za sozдание, ispol'zovanie i rasprostranenie vredonosnyh programm dlya EVM: Dis. ... kand. jurid. nauk. М., 2006.
12. Malyshenko D.G. Ugolovnaya otvetstvennost' za nepravomernyj dostup k komp'yuternoj informacii: Dis. ... kand. jurid. nauk. М., 2002.
13. Sotov A.I. Komp'yuternaya informaciya pod zashchitoy. Pravovoe i kriminalisticheskoe obespechenie bezopasnosti komp'yuternoj informacii: monografiya. М.: Izd-vo «Rusajns», 2017.
14. Apenov S.M. et al. International crime as a threat to global socio-economic security // *Int. J. Electronic Security and Digital Forensics*. 2021. T. 13. № 2. – P. 133-154.
15. Bennett C.J. *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press, 1992.
16. Berlin L. *The man behind the microchip: Robert Noyce and the invention of Silicon Valley*. Oxford University Press, 2005.
17. Eldridge J. *Alan Turing*. A&C Black, 2019.
18. Elshobake M.R.M., Laeba M. The Legal Framework of Cybercrime in Palestine // *Arab Law Quarterly*. 2021. T. 1. № aop. – S. 1-18.
19. Lawrence E. Evans, Jr. Internet Overview // *TEX. B.J.*, № 63. 2000.
20. Lee J.A.N., Holtzman G. 50 Years after breaking the codes: interviews with two of the Bletchley Park scientists // *IEEE Annals of the History of Computing*, 1995. T. 17. № 1. – P. 32-43.

21. Madsen W. Western European Initiatives. // Handbook of Personal Data Protection. Palgrave Macmillan, London, T. 1026. 1992. – P. 22-86.

22. Marshall J.H. Prosecution of Computer. Office of Legal Education Executive Office for United States Attorneys / J.H. Marshall, M. W. Bailie. T. 207. 2017.

23. McKnight G. Computer crime / Michael Joseph, 1973.

24. Murray A. Information technology law: the law and society. Oxford University Press, 2016.

Для цитирования и библиографии: Заркенов М.С. История развития уголовно-правовых норм в сфере информационных технологий // Право и государство. 2021. № 2(91). – С. 124-137. DOI: 10.51634/23075201\_2021\_2\_124

Материал поступил в редакцию 04.03.2021



### НОВЫЕ КНИГИ

**Оробинский В.В. Чему все еще не учат на юрфаке. Как думает юрист. Стратегии мышления.** Ростов-на-Дону: Феникс, 2019. – 277 с.

ISBN: 978-5-222-32045-7

Пять прошедших изданий книги помогли многим юристам – как начинающим, так и опытным. Поможет и вам, даже если вы прочтете вторую часть без первой. А помощь будет кстати, так как на юрфаках, увы, до сих пор прилежно учат право, но не учат, как применять это право в реальной жизни. Как знанием права зарабатывать на кусок хлеба. Как ладить с клиентами. Как строить отношения с коллегами. И много чему еще... Но самое страшное: на юрфаке – как и вообще в вузах – все еще не

учат думать. Основная цель книги: научить думать, как успешный юрист. Автор, в прошлом руководитель судебной практики крупной фирмы, разработчик собственных мастер-классов, ведет читателя сквозь лабиринт мышления по принципу «от простого – к сложному». От критического мышления и умения применять право в реальной жизни – к дедукции и индукции, а там и к более сложным стратегиям: продвинутая индукция, системный метод, внезапное озарение, созидательное мышление. Ссылки на практику, просветляющие упражнения и примеры из жизни – все это поможет вам перейти к работе над собой, не откладывая чтение. К каждой теме приложена «линейка» – вы сможете измерить, как у вас развит тот или иной профессиональный навык. Книга адресована прежде всего студентам, выпускникам и молодым специалистам. Но и опытный юрист сможет почерпнуть здесь нечто новое и полезное: редкие стратегии мышления, эффективные инструменты аналитики и поиска информации, умение толковать закон в нужную вам сторону с помощью теории и практики.