Научная статья
Original article
УДК 004.056

КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА СОВРЕМЕННОМУ ИНФОРМАЦИОННОМУ ОБЩЕСТВУ

CYBERCRIME AS A THREAT TO THE MODERN INFORMATION SOCIETY

Идрисов Идрис Керимович, преподаватель кафедры профессиональной подготовки Уфимского юридического института МВД России, г. Уфа

Вердиев Мурад Агаджанович старший преподавал кафедры криминалистики Казанского юридического института МВД России, г. Казань

Idrisov Idris Kerimovich, e-mail: idrisov05@gmail.com

Verdiev Murad Agadzhanovich e-mail: mister.verdiew2013@yandex.ru

Аннотация

По мере появления компьютера жизнь в обществе претерпела большие изменения. В частности, виртуальное пространство, как таковое стало неотъемлемой частью жизни человека. Наряду с этим эволюционировала также и преступность, обусловленная появлением такого специфического вида, как киберпреступность.

Нами рассмотрены особенности киберпреступности и ее виды. Проанализированы преступные деяния, связанные с данным феноменом и его последующим развитием.

В настоящее время в науке не выработано четкое определение данного понятия. Киберпреступность характеризуются определенно-специфичными

признаками. Данное обстоятельство предполагает рассматривать данное явление в рамках нестандартных преступлений. Рассмотрена классификация и реальные угрозы, порождаемые киберпреступностью.

Исследовано законодательство РФ, некоторых стран Европы и США. Как в РФ, так и в некоторых странах зарубежья, главный упор делается на закреплении соответствующих норм в Уголовном кодексе. В данном контексте необходимо отметить, что практически все страны достаточно быстро реагируют на явления, связанные с киберпреступностью, стараясь оперативно и законодательно отреагировать на появление возможных угроз. В статье выявлены и обоснованы актуальные проблемы раскрытия киберпреступлений.

В целом киберпреступность, как явление представляет собой угрозу мирового масштаба, подрывает основы международной безопасности.

Annotation

With the advent of the computer, life in society has undergone great changes. In particular, virtual space, as such, has become an integral part of human life. Along with this, crime has also evolved, due to the emergence of such a specific type as cybercrime.

We have considered the features of cybercrime and its types. Analyzed criminal acts associated with this phenomenon and its subsequent development.

Currently, science has not developed a clear definition of this concept. Cybercrime is characterized by certain specific features. This circumstance suggests considering this phenomenon in the framework of non-standard crimes. The classification and real threats generated by cybercrime are considered.

The legislation of the Russian Federation, some countries of Europe and the USA has been studied. Both in the Russian Federation and in some foreign countries, the main emphasis is on fixing the relevant norms in the Criminal Code. In this context, it should be noted that almost all countries quickly respond to the phenomena associated with cybercrime, trying to quickly and legally respond to the

emergence of possible threats. The article identifies and substantiates the actual problems of disclosing cybercrime.

In general, cybercrime, as a phenomenon, is a global threat that undermines the foundations of international security.

Ключевые слова: преступление; киберпреступность; Интернет пространство; кибертерроризм; компьютерная безопасность; виртуальное пространство; компьютерные сети; глобальные сети; уголовное преследование

Keywords: crime; cybercrime; Internet space; cyberterrorism; computer security; virtual space; computer networks; global networks; criminal prosecution.

В настоящее время в науке не выработано четкое определение понятия «киберпреступность». Данное понятие характеризуются определенно-специфичными признаками. Все это предполагает рассматривать это явление в рамках нестандартных преступлений.

Задуманное Говардом Эйкеном в 1941 году Устройство «Марк 1», стало основой создания современного компьютера. Устройство стоило полмиллиона долларов. Оно применялась в целях разработки оборудования для военно-морских сил США [3].

Начало разработки архитектуры компьютера пришлось на 1943 год. Именно в этом году по заказу лаборатории баллистических исследований для расчётов таблиц стрельбы были задействованы сотрудники Пенсильванского университета, Джон Преспер Эккерт и Джон Уильям Мокли [4].

Современные персональные компьютеры значительно отличаются от объемных, неуклюжих устройств, произведенных в период Второй мировой войны. В современном мире представить жизнь без вхождения в виртуальное пространство не представляется возможным. Тотальные процессы, связанные с глобализацией на фоне бурного развития различного рода компьютерных технологий, а также общемировая социально=экономическая интеграция стали основой перехода из постиндустриального в информационный этап развития общества.

Тем не менее, виртуальный мир сопровождается рядом непредсказуемых «сюрпризов». На фоне тотальной информатизации и глобальной компьютеризации стали наблюдаться изменения практически во всех сферах бытия общества. Этот процесс изменения отразился и на преступную среду: стала проявляться совершенно новая форма преступлений, в частности преступления в области информационных технологий.

Понятие «Киберпреступление» впервые начала проявляться в середине 70-х гг. прошлого века в Америке, именно в эти годы были отмечены первые преступления посредством применения информационных технологий. Например, в 1973 г. (Нью-Йорк) некий кассир местного банка применил компьютер, для хищения более 2 млн. долларов, путем элементарного перевода данной суммы на свой персональный счет. Конкретное понятие равно, как и главные признаки киберпреступления были явно сформулированы только лишь в 1974 г. и утверждены в Американской ассоциации адвокатов. Несколько позднее, а именно в 1986 г., был утвержден первый нормативно-правовой акт относительно противодействия киберпреступлениям под названием «Закон о мошенничестве с применением компьютеров» [1].

Однако четкого определенного понятия, характеризующего это преступление, до сих пор нет. Тем не менее, обобщенно, данное киберпреступление можно воспринимать в качестве преступления совершенного непосредственно в виртуальном пространстве.

К киберпрступлениям относятся преступления, совершаемые посредством использования компьютерной системы, равно, как и /или/ Сети (Интернет), или же преступления, определяющиеся деяниями против самой компьютерной структуры или Сети (Интернет). Данный вид преступлений представляет собой достаточно широкое понятие. К нему можно отнести такие виды преступления, при которых компьютер, в качестве информационной сети (Интернет), представляется в виде предмета преступления, где компьютеры играют роль средств и орудия одновременно.

По мнению некоторых исследователей, к киберпреступлениям можно отнести также и деяния, связанные с информационным пространством, представленным поддержкой деяний преступной общности, группы, к примеру применение электронной почты в качестве коммуникации, обмена тем или иным криминальным опытом, либо обменом определенными познаниями.

Такие преступления характеризуются анонимностью, наибольшей скрытностью преступника. В информационном пространстве достаточно сложно вычислить конкретное лицо, совершившее то или иное противоправное деяние.

Киберпреступления отличаются своей мобильностью, например такое преступление можно совершить практически из любой точки планеты. Для этого нужен, всего на всего компьютер и Интернет. При этом преступник и жертва преступления могут пребывать в разных странах планеты на довольно внушительных расстояниях. Кроме того, довольно сложно, а в некоторых случаях и невозможно определить дальнейшие действия киберпреступника из-за крайней сложности мошеннических виртуальных схем [1].

Существующая возможность автоматизма киберпреступлений является в некотором роде «ноу-хау» в преступных действиях. К примеру, хакер создает ту или иную вредоносную программу, которая уже сама продолжает совершать киберпреступления, т.е. реально проникает в другие компьютеры и выдает личную информацию без какого-либо участия разработчика в строго автономном режиме.

Такие преступления в современном мире считаются достаточно перспективным вектором диалектики преступного мира. Подобные противоправные деяния могут применяться практически на всех областях общественной жизни.

Виды и масштабы распространения киберпреступности постоянно растут. На сегодняшний день четкого деления на те, или иные, виды

киберпреступлений не существует. Тем не менее киберпреступления вполне можно подвергнуть дифференциации.

К преступлениям, направленным непосредственно против компьютерных систем и в частности баз данных можно отнести, так называемые хакерские атаки, определяющиеся заражением вирусами, а также специальными вредоносными программами и т.д. Примером такого преступления могут стать частые взломы баз данных определенных мобильных операторов для доступа к той или иной информации с целью приобретения интересующих для хакеров данных, для их применения в мошеннических и иных целях [5].

К киберпреступлениям, определяющимся получением той или иной экономической выгоды, является, так называемый «фишинг», который на сегодняшний день считается самой распространенной формой мошенничества в Интернет сети. Основной целью данного преступления является желание завладеть логином и паролем какой-либо виртуальной учетной записи конкретного пользователя с дальнейшим их использованием в своих преступных целях.

В большинстве своем, подобное преступление совершается посредством рассылок интернет писем (сообщений) в той или иной социальной сети, причем с прямой ссылкой на фальшивый сайт. Преступники, используя все возможные способы вынудить интернет-пользователя ввести реальные данные личной учетной записи. Некоторые аналитики утверждают, что примерно 70 % фишинговых атак заканчиваются успешно.

К киберпреступлениям, связанным со свободой личности можно отнести, так называемый, кибербуллинг, интернет-груминг равно, как и секстинг. Главными жертвами данных преступлений являются лица не достигшие совершеннолетия. При этом кибербуллинг, или же по-другому интернет-травля является осознанным и продуманным оскорблением, угрозой, выражающейся в виде компроматов, длящихся на протяжении довольно длительного времени.

Такая травля производится путем рассылок электронных писем или же посредством социальных сетей, видео порталов. Подобное преступное деяние вполне можно воспринимать как реальное вмешательство в личное виртуальное пространство и ущемление личных свобод и достоинств человека. Статистика указывает на достаточно большое распространение жертв данного преступления среди подростков 12-17 лет.

Понятие Интернет-груминг, считается своеобразным подходом со стороны взрослого лица к несовершеннолетним с определенными сексуальными целями с применением Интернета. Считается, что именно груминг в условиях сегодняшнего дня является идеальным средством для педофилов.

Термин секстинг понимается, как реальная пересылка информации определенно-интимного содержания путем использования тех или иных информационных технологий, например фотографий, видеосообщений и пр. Это понятие появилось в последние годы в Новой Зеландии. Стартовым началом секстинга послужил поступок девочки тринадцати лет, которая выставила свои откровенные фото на сайте знакомств. Секстинг в некоторых странах попадает под уголовную статью и рассматривается в качестве детской порнографии.

Другим видом киберпреступления считается нарушение авторских прав, например распространение кинофильмов, музыки и иной информации под другими названиями или авторством.

Понятие кибертерроризм возникло по причине тесного взаимодействия виртуального пространства непосредственно с государством равно, как и главными областями жизни общества. Данное понятие вбирает в себя преступные действия, определяющиеся дезорганизацией той или иной электронной информационной системы с причинением в перспективе огромного вреда человеческому сообществу и стране в целом. Особенностью этой формы киберпреступления является его масштабность. Ярким примером этого понятия является взлом системы NASA совершенным в 2015 г.,

вследствие которого произошла реальная утечка важной информации, являющейся государственной тайной.

Из основных угроз, исходящих из киберпреступлений можно выделить:

1.Вредоносную рекламу, называющуюся «спамом», которая или уже содержит в себе некую «рекламную информацию», определяющуюся шпионским ПО, или же реально переводит пользователей на непосредственный сайт зараженной вредоносной программой [6].

2.Целенаправленную деятельность злоумышленников, обусловленную взломом (Интернет атака) компьютеров с последующей кражей данных хранящихся в сети Интернет. В данном контексте необходимо отметить, что в последние годы стали проявляться, такие популярные действия, как PDF-атаки. Такая популярность напрямую связана с довольно низкой защищенностью PDF-фалов.

3.Огромная популярность социальных сетей является благодатной почвой для реализации киберпреступлений. В виртуальных просторах социальных сетей, где имеет место распространение большого числа различного рода вредоносных программ.

4.Киберпреступление в системе Веб-приложения, является довольно новым направлением интернет угроз, при котором злоумышленники реально похищают целые базы личных данных пользователей посредством «поддельных» приложений.

5.Довольно популярным вариантом преступлений является Интернет-мошенничество. В интернет пространстве, имеется большое количество различных схем, начиная от банальных и кончая достаточно сложными, к которым можно отнести, такие схемы, как «лотереи», «подружка», «мнимые приглашения на работу» и так далее. Творчество киберпреступников не имеет границ, - буквально ежедневно в пределы Интернет пространства выходят иные, все новые мошеннические схемы.

Скорость роста киберпреступлений довольно высока. Согласно статистике, буквально каждую секунду на планете «Земля» совершается

примерно 18 киберпреступлений, что в пересчете на количество преступлений, совершенных в течение одного дня, составляет 1,5 миллиона. Кроме того, около 70% пользователей Интернета минимум один раз становились реальными жертвами киберпреступников.

С годами число киберпреступлений растет. В РФ в течение 2010 г. было отмечено 7974 киберпреступлений, в 2012 году их количество составило 10227 случаев. За период 2013-2016 годов число данных преступлений повысилось с 10 до 66 тысяч. В 2017 году данный показатель определился 90688 преступлениями.

В целостном объеме преступлений совершенных в 2020 году доля киберпреступлений составила 21,7%, в 2021 году этот показатель представился 26,8%, что составляет порядка 27 от их общего числа преступлений [7].

В этой связи необходимо отметить, что общий объем ущерба от киберпреступлений в мире составляет порядка 110 млрд. долларов за один год. Вышеприведенный анализ данных указывает на реальную угрозу реально-стабильной безопасности, как в РФ, так и во всем мире.

В США еще в 1986 году к данной проблеме отнеслись со всей серьезностью [2]. В 2017 году Киберпреступление нашло свое отражение непосредственно в основном документе США «Стратегии национальной безопасности», равно как и в федеральных законах, данный аспект также были отражен в законах отдельных штатов. Кроме того, в 2018 г. была частично обновлена сама Стратегия кибербезопасности США.

В Европе, принят нормативно-правовой акт, относительно киберпреступности, всецело поддержанный 46 странами мира. Данная Конвенция Совета Европы, касательно киберпреступности, вступила в действие 1 ноября 2004 г. Она представлена набором принципов применительно для любой страны. Эта Конвенция являет собой некий шаблон для законодательства других стран в информационной системе.

В Англии принят свой национальный нормативно-правовой акт касательно компьютерных злоупотреблений, который был утвержден в 1990 г., в который периодически вносились небольшие изменения, на фоне развития общественных отношений в области компьютерных и Интернет – технологий. При этом размеры наказания за Киберпреступление, в этой стране представляются штрафами, или же лишением свободы сроком, определяющимся от полугода до 5 лет.

Меры борьбы с киберпреступностью в Голландии определились посредством введения новых статей непосредственно в Уголовный кодекс. Более того, был создан специальный государственный орган по формированию законодательной базы относительно противодействия киберпреступлениям.

В ФРГ основное законодательное противодействие киберпреступности реализуется посредством Уголовного кодекса.

Стратегией, связанной с Национальной Безопасностью РФ, считается информационная безопасность РФ, утвержденная 5 декабря 2016 г. Эта доктрина необходима для создания государственной политики, определяющейся выработкой совершенствования мер по обеспечению информационной безопасности

В УК РФ киберпреступления выражены отдельной главой 28, статьями:

- 272 УК РФ, - неправомерный доступ к той или иной компьютерной информации;

- 273 УК РФ создание вредоносных программ;

- 274.1 УК РФ воздействие на ту или иную критическую информационную инфраструктуру РФ [8].

Итак, киберпреступность, как явление с каждым годом все больше актуализируется, представляя реальную угрозу, как в масштабе РФ, так и всего мира. Киберпреступность, появившись относительно недавно, ускоренным темпом набирает популярность, практически во всем

виртуальном Интернет пространстве, открывая все новые возможности для преступных кругов.

Литература

1. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М.: Мир, 1999. 351 с
2. Фролов М.Д. Уголовная ответственность за мошенничество в сфере компьютерной информации по законодательству стран Северной и Южной Америки, Океании, Азии и Африки // Административное и муниципальное право. 2015. № 11 (95). С. 1164-1168.
3. Самый первый компьютер в мире [Электронный ресурс]. URL: https://basetop.ru
4. Юридический интернет-журнал «Первый юрист» [Электронный ресурс]. URL: https://urist.one

Literature

1. Aikov D., Seiger K., Fonstorkh U. Computer crimes. Manual on combating computer crimes. Moscow: Mir, 1999. 351 p.
2. Frolov M.D. Criminal liability for fraud in the field of computer information under the legislation of the countries of North and South America, Oceania, Asia and Africa // Administrative and municipal law. 2015. No. 11 (95). pp. 1164-1168.
3. The very first computer in the world [Electronic resource]. URL: https://basetop.ru
4. Legal online magazine "First Lawyer" [Electronic resource]. URL: https://urist.one

© Идрисов И.К., Вердиев М.А., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №3/2022.

Для цитирования: ИДРИСОВ И.К., ВЕРДИЕВ М.А., КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА СОВРЕМЕННОМУ ИНФОРМАЦИОННОМУ ОБЩЕСТВУ// Научно-образовательный журнал для студентов и преподавателей «StudNet» № 3/2022.