УДК 343.2/.7

Киберпреступность в России. Юридическая ответственность за нарушения прав в сфере информационных технологий

А. Н. Прикмета
Липецкий государственный технический университет, г. Липецк
parapan58@gmail.com

Прикмета А. Н. Киберпреступность в России. Юридическая ответственность за нарушения прав в сфере информационных технологий. *Статья посвящена рассмотрению вопросов* ***к****иберпреступности в России. Дается анализ понятий «киберпреступность», «киберкриминальный рынок», оцениваются причины и особенности киберпреступлений. Особое внимание уделяется юридической ответственности за нарушения прав в сфере информационных технологий.*

Ключевые слова: *киберпреступность, киберкриминальный рынок, киберинциденты, ответственность за киберпреступления.*

Введение

В наше время не осталось сфер, где в той или иной мере не применялись бы информационные технологии и программное обеспечение. С развитием современных технологий сформировались условия появления нового вида преступлений, совершаемых в киберпространстве. Современный мир – сфера компьютерных технологий, в котором кибервойны и киберпреступления стали реальностью.

По определению экспертов ООН термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде [1].

По исследованиям The Wall Street Journal:

- ✓ 29 стран имеют специализированные военные киберподразделения, занимающиеся противодействием угрозам информационной безопасности, в частности Россия, Австралия, Бразилия и Египет;
- ✓ 49 стран закупают специализированное хакерское программное обеспечение, в том числе Россия, Австралия, Бразилия и Египет;
- ✓ 63 страны используют инструменты сплошного наблюдения как внутри страны, так и глобально (Чехия, Италия, Мексика и др.).

Согласно информации о взломах, наиболее развитым кибероружием обладают Россия, США, Великобритания, Китай, Индия, Иран и Северная Корея.

Отчет консалтинговой компании PricewaterhouseCoopers (PwC) показывает, что стратегию по кибербезопасности имеют 60% российских и американских компаний. В Германии только 45%, во Франции 51%, в Италии 55%. Наиболее защищенными от кибератак странами являются Малайзия (74%), Япония (72%) и Индонезия (70%)[2].

Для создание и использование кибервооружений не требует колоссальных вложений в обогатительные заводы, разработку средств доставки и строительство пусковых установок. Достаточно обладать сравнительно небольшими финансовыми ресурсами, средними компьютерными системами и доступом к глобальным сетям. Кибератаки сложно остановить и зачастую невозможно отследить. Благодаря этому инструменты хакерских атак стали доступны не только правительствам, но и агрессивным политическим группировкам и террористическим организациям.

На расширенном заседании Совета безопасности 26.10.2017, президент России В.В.Путин обозначил основные направления развития информационной безопасности в Российской Федерации, среди которых выделил увеличение интенсивности кибератак. По его словам, все острее встает проблема вторжения в ИТ-системы в сфере гособороны и управления, а также финансов. Кроме того, значительную угрозу представляет утечка электронных документов.

«*Следует повысить безопасность и устойчивость работы инфраструктуры российского сегмента Интернета. Как и в других демократических странах, мы должны бороться с теми, кто использует информационное пространство для пропаганды радикальных идей, оправдания терроризма, экстремизма, решительно пресекать попытки размещения материалов, угрожающих безопасности нашего государства, общества в целом и отдельных граждан...*» [3].

Исследования

Классификация киберпреступлений. Поскольку киберпреступления охватывают широчайший пласт общественных отношений, предполагают использование различного оборудования и имеют целый спектр способов совершения, логично провести их классификацию.

Согласно классификации установленной Конвенцией Совета Европы виды киберпреступлений объединены в пять групп:

1. Компьютерные преступления, направленные против компьютерных данных и систем (например, взлом базы данных мобильного оператора с целью получения паспортных данных пользователей). Классифицируются как *незаконный доступ.*

2. Противоправные деяния, связанные с использованием технологий (подлог, извлечение, блокировка или изменение данных, мошенничество, получение экономической выгоды иными способами), так называемый *незаконный перехват*.

3. Противоправные деяния, связанные с содержанием данных или контентом. Самый распространённый и жёстко наказуемый практически во всех странах вид этих киберпреступлений – преступные деяния, связанные с детской порнографией.

4. Нарушение авторских и смежных прав, определяемое как *вмешательство в данные.* При этом установление таких правонарушений Конвенцией отнесено к компетенции национальных законодательств государств.

5. Кибертерроризм и использование виртуального пространства для совершения актов насилия, а также другие деяния, посягающие на общественную безопасность. Так называют *особо серьезные преступления*, связанные с жестокостью и совершением актов насилия по средствам высоких технологий. Также к этому виду относят деяния, которые ставят под угрозу общественную безопасность, а также акты расизма и ксенофобии, совершённые с использованием компьютерных сетей[4].

При этом в Конвенции вредоносное программное обеспечение понимается как средство, способствующее совершению компьютерных преступлений, а его использование не является отдельным правонарушением.

Количество киберпреступлений неуклонно растет. По данным испанского сайта Informática Forense (Компьютерная криминалистика) [5] только на 2017г. прогнозируется более 26500 кибератак против государственного сектора и стратегических компаний, что на 26.5% больше, чем в 2016г. (см. рис.1).

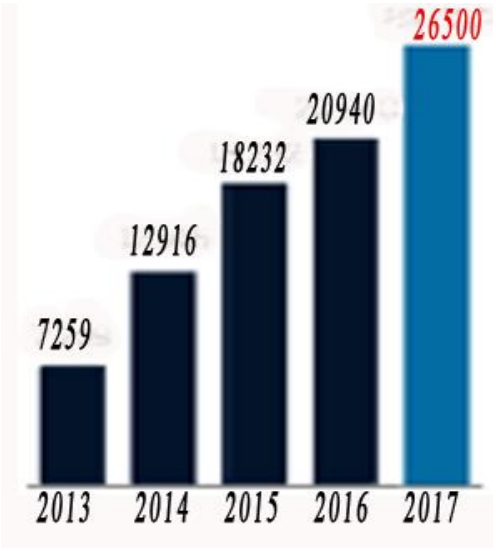

Рисунок 1 – Тенденции изменения числа кибератак

Более 70 кибератак было зафиксировано в октябре 2017г., что связывают с проведением референдума в Каталонии. Их целью были сайты правительственных организаций, Конституционный суд, Национальный разведывательный центр и др.

Как видим, кроме экономической составляющей, в данный момент причиной киберпреступлений может быть и составляющая политическая[6].

Исследования «Лаборатории Касперского» показали, что за год каждая вторая промышленная компания в мире пережила от одного до пяти киберинцидентов, которые затронули важные инфраструктуры или автоматизированные системы управления технологическими процессами, см. рис 2.

Опрос, проводимый более, чем в 350 организациях по всему миру, показал, что три четверти компаний допускают вероятность пострадать от кибератак [7].

Особенностями данного вида преступлений являются:

- чрезвычайная скрытность деяний, которая достигается применением механизмов анонимности и шифрования;
- трансграничность: преступник и жертва могут быть разделены тысячами километров, границами нескольких государств;
- нестандартность способов совершения;
- автоматизированный режим.

Самым разрушительным образцом американского кибероружия стал червь Stuxnet, который вывел из строя центрифуги на иранском заводе по обогащению урана.

Успешность применения кибероружия можно проиллюстрировать на примере конфликта в Сирии. По данным компании в области

компьютерной безопасности FireEye, сирийское правительство совершило атаку на компьютерные системы командования повстанцев и получило важную тактическую информацию, что вылилось в значительные потери для повстанцев.

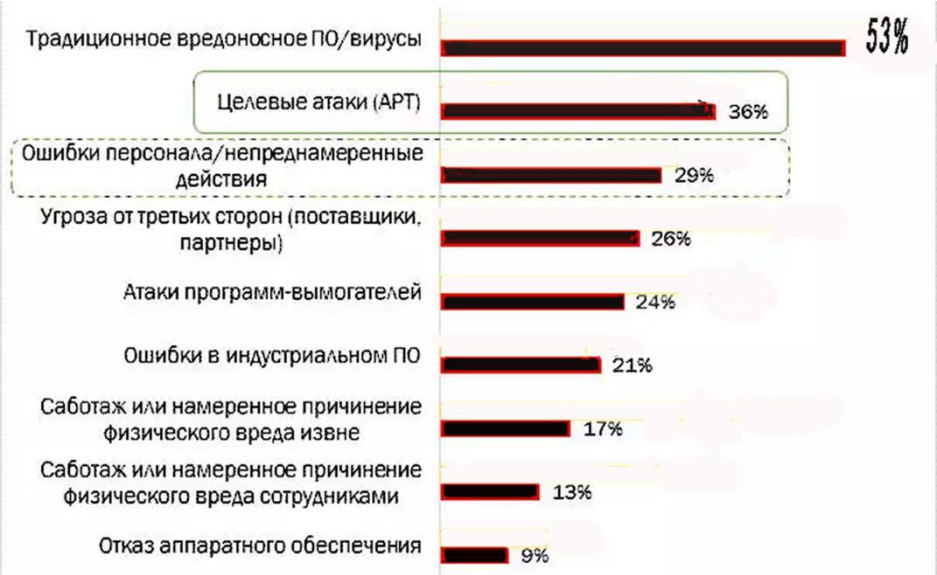

Рисунок 2 – Причины киберинцидентов

Киберкриминальный рынок. Киберкриминальный рынок рассматривается как совокупность «услуг» и «продуктов», используемых для совершения противоправных действий в киберпространстве.

Продукты:

✓ программное обеспечение, предназначенное для получения несанкционированного доступа к компьютеру или мобильному устройству, кражи данных с зараженного устройства и/или денежных средств со счета жертвы (троянцы);

✓ программное обеспечение, предназначенное для эксплуатации уязвимостей в установленном на компьютере ПО (эксплойты).

Услуги:

✓ рассылка спама;

✓ организация DDoS-атак (перегруз сайтов запросами с целью сделать их недоступными для легитимных пользователей);

✓ «перекриптовка» вредоносного ПО (изменение вредоносного ПО таким образом, чтобы его не детектировали антивирусы);

✓ VPN (предоставление анонимного доступа к веб-ресурсам);

✓ передача в аренду ботнетов;

✓ проверка ценности краденных данных платежных карт;

✓ услуги по подтверждению данных (фальшивые звонки, фальшивые сканы документов);

✓ продвижение вредоносных и рекламных сайтов в поисковой выдаче;

✓ посредничество при сделках по приобретению «продуктов» и «услуг»;

✓ вывод и обналичивание средств.

По наблюдениям экспертов «Лаборатории Касперского», преступления, связанные с кражей денег, наиболее распространены в последние годы.

По данным аналитического центра Zecurion веб-сервисы являются самым популярным в мире каналом утечек информации (26,7%), на втором месте – неэлектронные носители. В России 53% компаний сталкиваются с утечкой информации через электронную почту, 32% - через интернет-сервисы, см. рис.3 [8].

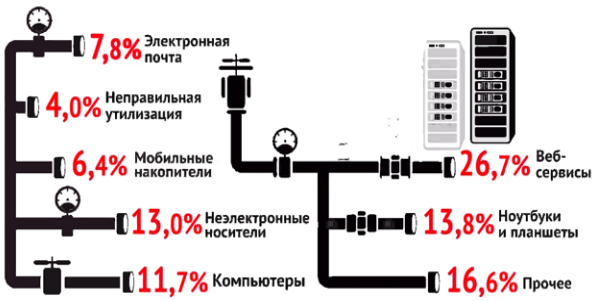

Рисунок 3 –Каналы утечек информации

Ответственность за киберпреступления в законодательстве РФ.

Актуальность темы киберпреступлений придает тот факт, что размер причиняемого этим видом преступлений, ущерба неуклонно растет и по мнению ряда экспертов доходы теневого бизнеса сети Интернет могут сравниться с прибылью от незаконной торговли наркотиками.

В Росси совершается в среднем ежедневно 44 хищения из систем дистанционно – банковского обслуживания.

Согласно статистическим данным Европола большинство хакеров и киберпреступников – граждане России и СНГ.

В настоящее время не существует ни релевантной статистики, отражающей реальную картину состояния рынка киберпреступлений, ни методов сбора данных такого вида.

Поэтому столь важна разработка методов анализа, сбора информации, а также уровень ее классификации.

Киберпреступность представляет собой не только техническую и правовую, но и социальную проблему, эффективное решение которой требует системного подхода.

По данным Global CIO доля привлеченных к ответственности за киберпреступления менее 0,1% .

Основная проблема – отсутствие реальной ответственности киберпреступников за преступления.

Лишь 3% из поданных заявлений доходят до возбуждения уголовных дел. Следует учитывать, что данные по компьютерному преступлению собрать весьма сложно, электронные улики остаются, но их легко уничтожить и сложно обеспечить их юридическую значимость.

Ответственность за свои действия несут в среднем лишь 5-7 преступников.

Причин этому несколько.

1. Очень часто преступные группировки находятся в разных городах, нередко – в разных странах.

Последние несколько лет в связи с появлением и распространением ботнетов[1] ситуация усложнилась еще более. Деньги крадутся у компании, находящейся в одном регионе, через банк в другом, переводятся через несколько счетов в разных банках и платежных системах и обналичиваются в третьем.

Возникает вопрос, какой территориальный орган должен возбуждать дело? По действующему законодательству дело возбуждает тот орган, на территории которого произошло преступление. Другой пример. Сервер атаки находится в Германии, а цель – предприятие/банк в Москве. Эти вопросы, связанные с местоположением преступников и целью киберпреступлений, законодательно не решены, что служит основанием в отказе в возбуждении дела.

2. SMS-мошейничество вообще не попадает под действующие нормы, поскольку сумма конкретного ущерба очень мала и на этом основании органы могут отказать в возбуждении дела. Отметим, что, по мнению экспертов, оборот SMS-мошейничества оценивается в 100 млн. руб. в месяц.

3. Квалификация следователей. Вряд ли следует надеяться, что следователь территориального органа внутренних дел с минимальной компьютерной грамотностью, сможет расследовать преступление, охватывающее несколько регионов. Эта проблема заключается в недостаточной подготовленности сотрудников правоохранительных органов в области IT-систем, интернет-технологий, программного обеспечения.

Опросы среди следователей показывают, что 95% респондентов получили юридическое образование. И только 5% обладают еще и образованием по специальности «Информатика и вычислительная техника». 63% опрошенных владеют компьютером на уровне «среднего пользователя», 37% - на уровне «продвинутого пользователя». 79% при этом постигают компьютер самостоятельно, курсы для сотрудников правоохранительных органов посещали только 21%, и незначительный процент (5%) – коммерческие курсы.

Несмотря на это, следует отметить, что Россия была одной из первых держав, создавшая еще в 90-х годах киберполицию, а в 2014 были созданы кибервойска. По оценкам экспертов, Россия находится в первой пятерке государств мира по уровню развития кибервойск.

4. Учитывая, что в случае уголовного расследования убытки от расследования могут оказаться выше суммы причиненного ущерба, многие организации предпочитают ограничиваться разрешением конфликта своими силами.

5. Боязнь подрыва собственного авторитета в деловых кругах и как результат этого — потеря значительного числа клиентов. Эго обстоятельство особенно характерно для банков и крупных финансово-промышленных организаций, занимающихся широкой автоматизацией своих производственных процессов.

6. Боязнь возможности выявления в ходе расследования собственного незаконного механизма осуществления отдельных видов деятельности и проведения финансово-экономических операций.

7. Правовая и законодательная неграмотность пострадавших[9,10].

8. Судебная система фундаментально не готова рассматривать цифровые доказательства ни в арбитражном, ни уголовном процессе. Когда

[1] Слово Botnet (ботнет) образовано от слов «robot» (робот) и «network» (сеть). Киберпреступники используют специальные троянские программы, чтобы обойти систему защиты компьютеров, получить контроль над ними и объединить их в единую сеть (ботнет), которой можно управлять удаленно.

банк идет в суд с доказательствами в виде IP-адресов, его просят предоставить документ, заверенный подписью.

9. Несвоевременность выявления киберпреступлений. В соответствии с результатами опросов:

- ✓ в 53% случаев с момента совершения преступления до поступления информации о совершенном преступлении проходит более 10 дней;
- ✓ 73% респондентов отметили запоздалое начало предварительного расследования, когда многие важные доказательства уже утрачены.

В юридической науке до сих пор остается открытым вопрос об ответственности, которая должна применяться к правонарушителям в сфере компьютерной информации. Одни исследователи полагают, что так как компьютеризация общества распространяется во все сферы жизнедеятельности, то к правонарушителям должно применяться столько видов ответственности сколько существует в юридической науке, то есть: конституционная, уголовная, административная, дисциплинарная и гражданско-правовая, а в некоторых случаях и материальная.

Другие же придерживаются трех видов ответственности: 1) уголовной, 2) административной и 2) гражданской.

Наибольшую роль по юридической нагрузке играет уголовная ответственность. В Уголовном кодексе Российской Федерации часть преступлений выделены в отдельную главу 28 «Преступления в сфере компьютерной информации»:

- ✓ статья 272. Неправомерный доступ к компьютерной информации;
- ✓ статья 273. Создание, использование и распространение вредоносных компьютерных программ;
- ✓ статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Статья 272 УК РФ. Неправомерный доступ к компьютерной информации.

По этой статье предусмотрено наказание, в виде «штрафа в размере до трехсот тысяч рублей, либо исправительными работами на срок до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

В случае совершения группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок. Если же они повлекли тяжкие последствия или создали угрозу их наступления, – наказываются лишением свободы на срок до семи лет[11].

Объективной стороной состава данного преступления является неправомерный доступ к охраняемой законом компьютерной информации. Под таким доступом понимается получение возможности ознакомиться и/или воспользоваться ею. Сам доступ может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств, которые позволяют преодолеть установленные системы защиты, а так же незаконное использование паролей или кодов, либо совершения иных действий в целях проникновения в сеть или систему под видом законного пользователя. Неправомерным признается доступ лица, не имеющего права на работу и получения данной информации, в отношении которых приняты специальные защитные меры, ограничивающие круг лиц имеющих к ним доступ.

Охраняемая законом информация – те данные, для которых установлен специальный режим правовой защиты, например государственная, служебная и коммерческая тайна, персональные данные, объекты авторского права и смежных прав.

Данный состав носит материальный характер и предполагает обязательное наступление одного или нескольких указанных в законе последствий: уничтожение, блокирование, модификация (переработка), копирование информации. Одним из важных моментов является установление причинной связи между несанкционированным доступом и наступлением последствий. Данное преступление считается оконченным в момент наступления последствий.

Субъективная сторона характеризуется умышленной формой вины.

Субъект преступления – любое вменяемое лицо достигшее 16 летнего возраста.

Пример: По приговору Орджоникидзевского районного суда г. Екатеринбурга 25.06.2017г., гр. Александровскому по совокупности преступлений назначено наказание в виде лишения свободы на срок 2 года за преступления предусмотренные ч. 3 ст. 183 Уголовного Кодекса Российской Федерации, то есть незаконное разглашение сведений, составляющих

коммерческую тайну без согласия их владельца лицом, которому она была доверена по работе, совершенное из корыстной заинтересованности и ч. 2 ст. 272 Уголовного Кодекса Российской Федерации, то есть как совершение неправомерного доступа к охраняемой законом компьютерной информации, повлекшее копирование компьютерной информации, совершенное из корыстной заинтересованности, совершенное группой лиц по предварительному сговору.

Статья 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ.

Наказание – принудительные работы на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей.

В случае совершения группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Преступление считается оконченным с момента создания, изменения, использования или распространения вредоносной программы, создающей угрозу указанных в законе последствий.

Объектом преступления является общественная безопасность и общественный порядок, а также совокупность общественных отношений по правомерному и безопасному использованию информации.

Объективную сторону составляет сам факт создания компьютерных программ или иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Наиболее распространенными видами вредоносных программ являются компьютерные вирусы, черви, программы-сканеры, эмуляторы электронных средств защиты, программы управления потоками компьютерной информации, программы - патчеры.

Субъект – физическое, вменяемое лицо, достигшее 16 летнего возраста.

Субъективная сторона – вина в форме прямого умысла.

Данная статьей, имеет некоторые общие черты с составом преступления, предусмотренного ст. 272 УК. Сложность разграничения этих преступлений заключается в том, что неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) ведут к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нейтрализации средств защиты компьютерной информации.

Предметом преступления, предусмотренного ст. 272 УК, является только та информация, которая охраняется законом. Предметом же ст. 273 УК является создание, использование и распространение вредоносных программ, а так же любая информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Состав преступления, предусмотренный частью 1 статьи 273 - формальный. Для признания преступления оконченным не требуется реального наступления вредных последствий

Пример: Приговор Лямбирского районного суда Республики Мордовия от 3.10.2017 г. в отношении Галабир С.В. о наказании на срок 1 год 6 месяцев ограничения свободы за преступления предусмотренные ч.1 ст. 273, ч. 2 ст. 273 и ч. 2 ст. 273. Гр. Галабир, использовал вредоносные компьютерные программы, заведомо предназначенные для несанкционированного копирования компьютерной информации из корыстной заинтересованности:

- совершил действия по созданию и распространению компьютерной программы, заведомо предназначенной для несанкционированной модификации и копирования компьютерной информации, совершенные из корыстной заинтересованности,
- совершил действия по использованию вредоносной компьютерной программы, заведомо предназначенной для нейтрализации средств защиты компьютерной информации и преступления.

Статья 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Наказывается штрафом в размере до пятисот тысяч рублей, либо исправительными работами до одного года, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок. В случае если такое деяние повлекло тяжкие последствия или создало угрозу их наступления, то наказывается принудительными работами на срок до пяти лет либо лишением

свободы на тот же срок.

Объективная сторона данного преступления состоит в нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, повлекшем уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб. Предусмотренный комментируемой статьей состав преступления является материальным и его необходимым элементом является причинение крупного ущерба. Между фактом нарушения и наступившим ущербом должна быть установлена причинная связь. Наступившие последствия должны являться результатом нарушения правил эксплуатации, а не программной ошибкой либо действиями, предусмотренными в ст. ст. 272, 273 УК. Понятие крупного ущерба определено в примечании 1 к ст. 272 УК и должно составлять не менее одного миллиона рублей.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации, за которые предусмотрена ответственность данной статьей отличается от преступления, предусмотренного ст. 272 УК РФ тем, что виновный, в силу своего служебного положения, имеет право доступа к информации и является законным пользователем. То есть, субъект данного преступления – специальный.

Преступление может быть совершено и путем бездействия (например, не включать системы защиты информации, в результате чего наступают вредные последствия).

По данной статье редки случаи привлечение к уголовной ответственности из-за высокого материального порога состава преступления. Относится к преступлениям небольшой тяжести.

С 1 января 2018 года вступает в силу новая статья Уголовного Кодекса РФ – ст.274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», которая вводится в соответствии с Федеральным законом № 194 –ФЗ от 26.07.2017.

По существу, новая норма уголовного закона содержит крайне схожее описание уголовно-наказуемых действий, закрепленных в диспозициях статей 272, 273 и 274 УК РФ, за исключением существенного отличия: объектом преступного посягательства является критическая информационная инфраструктура.

Одновременно принятием Федерального закона №187-ФЗ от 26.07.2017 года законодатель установил, что критическую информационную инфраструктуру РФ составляют объекты инфраструктуры в виде: информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления субъектами критической информационной инфраструктуры, а также сети электросвязи**,** используемые для организации взаимодействия таких объектов.

Другой отличительной особенностью статьи 274.1 УК РФ является ужесточение уголовной ответственности за совершение неправомерных действий вплоть до назначения безальтернативного наказания в виде лишения свободы от пяти до десяти лет.

Осуществлять расследование уголовных дел по статье 274.1 УК РФ уполномочена Федеральная служба безопасности Российской Федерации. В тоже время закон допускает возможность производства предварительного следствия следователями органа, выявившего подобное преступление (Следственный Комитет РФ, МВД РФ).

В России киберпреступность за последние три года выросла в шесть раз, сообщил генеральный прокурор России Ю.Я. Чайка. Такие данные он привел на встрече руководителей прокурорских служб государств БРИКС в Бразилии.

Ю. Я. Чайка отметил, что в России число преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, с 2013 по 2016 г. увеличилось с 11 000 до 66 000. Значительный их рост наблюдается и в текущем году (+26%, 40 000).

При этом в Генпрокуратуре добавили, что помимо этого «всемирная сеть широко используется для пропаганды различных экстремистских идей и движений». Например, в 2016 г. в России две трети преступлений экстремистской направленности и каждое девятое преступление террористического характера совершались с использованием Интернета.

Кроме перечисленных ранее причин ненаказуемости за компьютерные преступления, существует несколько важных проблем.

1. Наибольшие трудности возникают при проведении осмотра места происшествия и назначении судебных экспертиз.

При этом многие респонденты отмечали, что и вовсе не проводили осмотр места происшествия. Причина проста – оно отсутствует. Это значит, что распознавание места совершения киберпреступления невозможно без установления обстановки совершения преступления, которая определяется системой киберпространства. Как уже говорилось ранее, основной особенностью киберпреступлений является трансграничность. То есть между преступником и жертвой могут быть тысячи километров. Для расследования преступлений, совершенных в киберпространстве, требуются как технические, так и теоретические знания.

2. Проведение экспертизы. Следователи отмечают высокую загруженность государственных судебно-экспертных учреждений и, как следствие, несвоевременностью выполнения экспертиз.
3. Немаловажной проблемой при назначении экспертиз является постановка грамотных вопросов эксперту. Назначающие экспертизу связывают возникающие трудности с отсутствием у них практики расследования данной категории дел, сложностью технических терминов и отсутствием специальных знаний в этой сфере.

В табл. 1 приводятся данные анализа материалов уголовных дел о киберпреступлениях [12].

Таблица 1. Данные анализа материалов уголовных дел о киберпреступлениях.

Следственные действия	%
1	2
Привлечение к осмотру места происшествия специалиста и эксперта-криминалиста.	91,7
По прибытии на место осмотра происшествия следователь запретил доступ к компьютерам и различным гаджетам (планшетные компьютеры, телефоны, смартфоны и прочее) всем лицам, находящимся на месте осмотра.	2,0
Выявление следов рук, оставшихся на компьютерной технике и периферийных устройствах.	41,7
Установление расположения всей компьютерной техники, в осматриваемом месте, места прокладки телекоммуникационных кабелей, наличие локальной, беспроводной (WI-FI) и глобальной сетей в помещении, наличие сервера.	16,7
Место происшествия осматривалось также на предмет запоминающих устройств.	58,3
Осмотрена документация и записи, относящиеся к киберпреступлениям.	16,7
Работающая компьютерная техника осматривается специалистом для выявления компьютерной информации, содержащей следы, совершённого киберпреступления.	75,0
Производится изъятие компьютерной техники и комплектующих.	50,0
Обыск проводился (да/нет).	30 / 70
Выемка техники проводилась (да/нет).	58.3 / 41.7
Предварительное получение достоверных данных: о виде и конфигурации используемой компьютерной техники; о подключении компьютерной техники к телекоммуникационным сетям; о наличии службы информационной безопасности и защиты от несанкционированного доступа; о системе электропитания помещений, где установлена компьютерная техника; о квалификации пользователей и другие.	16.7

Раскрытие и расследование киберпреступлений остается сложной задачей для сотрудников органов предварительного расследования. Это обусловлено:

- ✓ отсутствием системных обобщений материалов следственной и судебной практики;
- ✓ нехваткой методических рекомендаций по организации расследования данного вида преступлений;
- ✓ небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов;
- ✓ недостаточно высоким уровнем подготовки следователей по соответствующей специализации в высших учебных заведениях.

Так по данным [12] наибольшие трудности при расследовании киберпреступлений вызывают: допрос подозреваемого (71%); осмотр места преступления (42%).

В 69% причинами преступлений является корыстная заинтересованность; хулиганство в 10.5%, месть 9.3%, исследовательский интерес и самоутверждение - 12%.

Выводы

С развитием современных технологий сформировались условия к появлению нового вида преступлений, совершаемых в киберпространстве.

Этому новому виду преступности необходимо противопоставить действенные меры, в число которых входят и меры уголовно-правового воздействия.

Необходимо детальное изучение преступлений в сфере компьютерной информации для их правильной классификации и повышения эффективности борьбы с ними.

При расследовании киберпреступлений необходимы профессиональные знания, что обуславливает необходимость привлечения специалистов соответствующего профиля.

Необходима унификация уголовного законодательства различных государств, в т. ч. и Российской Федерации, предусматривающего уголовную ответственность за преступления в сфере компьютерной информации.

Литература

1. Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Право России. Режим доступа: http://portalus.ru/modules/russianlaw/rus_readme.php?subaction=showfull&id=1105644430&archive=old&start_from=&ucat=&.

2. Securitylab.ru by positive technologies. Российские компании сравнялись с

американскими по уровню кибербезопасности. Режим доступа: https://www.securitylab.ru /news/489586.php

3. Securitylab.ru by positive technologies. Путин поручил российским IT-компаниям перейти на отечественное ПО. Режим доступа: http://www.securitylab.ru/news/488380.php

4. Конвенция о компьютерных преступлениях. Режим доступа: https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680081580.

5. Informática Forense (Компьютерная криминалистика). Режим доступа: https://www.scoop.it/t/informatica-forense.

6. 70 ciberataques en diez días de grupos afines al independentismo. Режим доступа: https://politica.elpais.com/politica/2017/11/21/actualidad/1511286369_774264.html

7. Государство. Бизнес. ИТ. Киберпреступность в мире. Состояние киберпреступности в различных регионах мира. Режим доступа: http://www.tadviser.ru/index.php

8. Ассоциация электронных торговых площадок. Режим доступа: http://aetp.ru/market-news/item/395681

9. Киберпреступность — масштабы огромны, ответственности — ноль? Global CIO. Официальный портал IT - директоров. Режим доступа: http://www.globalcio.ru/theme-2011-03-first/

10. Николаева А.Б., Тумбинская М.В. Киберпреступность: история развития, проблемы практики расследования. Виртуальный компьютерный музей. Режим доступа: http://www.computer-museum.ru/articles/materialy-mezhdunarodnoy-konferentsii-sorucom-2014/629/

11. Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 26.08.2017).

12. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений. Диссертация на соискание учёной степени кандидата юридических наук, Москва, 2016.

Прикмета А. Н. Киберпреступность в России. Юридическая ответственность за нарушения прав в сфере информационных технологий. *Статья посвящена рассмотрению вопросов* ***к****иберпреступности в России. Дается анализ понятий «киберпреступность», «киберкриминальный рынок», оцениваются причины и особенности киберпреступлений. Особое внимание уделяется юридической ответственности за нарушения прав в сфере информационных технологий.*

Ключевые слова: *киберпреступность, киберкриминальный рынок, киберинциденты, ответственность за киберпреступления.*

Prikmeta A. N. Cybercrime in Russia. Legal liability for violations of rights in the field of information technology. *The article is devoted to the consideration of cybercrime in Russia. The analysis of the concepts "cybercrime", "cybercriminal market" is given, the causes and peculiarities of cybercrimes are estimated. Particular attention is paid to legal liability for violations of rights in the field of information technology.*

Keywords: *cybercrime, cybercriminal market, cyberincident, responsibility for cybercrime.*

Статья поступила в редакцию 21 мая 2018 г.
Рекомендована к публикации профессором Миненко А. С.