Министерство образования и науки Российской Федерации
Федеральное государственное автономное
образовательное учреждение высшего образования
«Южно-Уральский государственный университет»
(Национальный исследовательский университет)
Юридический институт

Кафедра «Правоохранительной деятельности и национальной безопасности»

РАБОТА ПРОВЕРЕНА
Рецензент, старший
оперуполномоченный по особо
важным делам Отдела «К» ГУ МВД
России по Челябинской области
_____ А.С. Акимов
«____»_____2017 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой ПДиНБ
доктор юридических наук

_____С.В. Зуев
«____»_____2017 г.

Криминологические аспекты противодействия преступлениям в сфере компьютерной информации

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
ЮУрГУ-400401.2017.523.ВКР

Руководитель работы
Доцент кафедры ПДиНБ
кандидат юридических наук
_____ С.Т. Фаткулин
«____»_____2017 г.

Автор работы
Студент группы 386-ЮИ
Рублева Ольга Олеговна
_____
«____»_____2017 г.

Нормоконтролер
Специалист по учебно-методической
работе кафедры ПДиНБ
_____С.А. Поливцева
«____»_____2017 г.

Челябинск 2017

РЕФЕРАТ

Рублева О.О. «Криминологические аспекты противодействия преступлениям в сфере компьютерной информации» – Челябинск, ЮУрГУ, 386-ЮИ, 2017. – 93 с., библиографический список – 84 наименования.

Объектом работы являются криминологические аспекты противодействия преступлениям в сфере компьютерной информации. Предмет работы – уголовно-правовые отношение в сфере компьютерной информации, меры уголовно-правового, организационного содержания направленные на обеспечение безопасности в сфере информационных отношений.

Целью данной работы является теоретическое исследование преступлений в сфере компьютерной информации, определение перечня предложений по совершенствованию организационных и правовых мер по противодействию компьютерной преступности.

Задачи работы:

- определить теоретико-криминологическую характеристику компьютерной преступности;
- провести анализ состояния компьютерной преступности в настоящее время, дать характеристику её тенденциям;
- рассмотреть состояние компьютерной преступности в международном правовом поле;
- дать характеристику личности компьютерного преступника, составить типологию;
- исследовать и охарактеризовать причины и условия компьютерной преступности современных условиях;
- проанализировать виктимологические проблемы компьютерной преступности;

- обосновать и предложить меры по совершенствованию уголовного законодательства;

- провести сравнительное исследование национального и международного законодательства в аспекте компьютерных преступлений.

В ходе работы мной изучена и проанализирована различная учебная литература, публикации, статьи, нормативно-правовая документация и комментарии к ней, в результате предложены меры по противодействию преступности в сфере компьютерной информации. Поставленные мною задачи считаю выполненными.

ОГЛАВЛЕНИЕ

стр.

ВВЕДЕНИЕ

Одной из социальных проблем в современном российском обществе является возникновение и активное развитие компьютерной преступности, причиняющей колоссальный вред экономической, политической, культурной, научной, образовательной и информационной сферам Российской Федерации.

Все более актуальным становится вопрос о защите граждан, муниципальных и государственных учреждений, предприятий, органов власти от несанкционированного доступа к компьютерной информации, вредоносных компьютерных программ и иных компьютерных угроз.

Масштабы ущерба, причиняемого компьютерными преступлениями, впечатляют. Так, по оценкам аналитиков компании Group-IB, объем рынка киберпреступности в РФ в 2012 г. составил 1,93 млрд дол., а с середины 2013 по середину 2014 г. в России и СНГ русскоговорящие хакеры «заработали» 2,5 млрд дол., что составляет 2 % от глобального рынка.

В свою очередь, американская корпорация Symantec оценила ущерб от киберпреступности в России в 2013 г. в 1 млрд дол., в 2012 г.□ – в 1,48 млрд дол. При этом общий ущерб от киберпреступности в мире в 2013 г. составил 113 млрд дол.[1].

По данным исследования 2014 Cost of Cyber Crime Study, проведенного компанией Ponemon Institute при поддержке HP Enterprise Security, среднегодовой ущерб российских организаций от киберпреступлений в 2014 г. достигает 3,3 млн дол.[2].

По данным «Лаборатории Касперского», в мире ежедневно появляется до 70 тыс. вредоносных программ. При этом за последний год в 96 % российских компаний фиксировались инциденты в области IT-безопасности.

---

[1] Norton report 2013 [Электронный ресурс] - Режим доступа: http://go.symantec.com/norton-report-2013. – Загл. с экрана.

[2] 2014 Global Report on the Cost of Cybercrime [Электронный ресурс] - Режим доступа: http://www.octree.co.uk/Documents/2014-Global-Report-on-the-Cost-of-Cybercrime.pdf. – Загл. с экрана.

Больше половины опрошенных специалистов признали факт потери данных в результате заражения компьютеров вредоносным программным обеспечением. При этом чаще всего инциденты в области IT-безопасности приводят к потере данных о платежах (13 %), интеллектуальной собственности (13 %), клиентских баз (12 %) и информации о сотрудниках (12 %).

Поэтому в настоящее время противодействие компьютерным преступлениям является одним из главных направлений деятельности правоохранительных органов по обеспечению информационной безопасности российского общества.

1. ТЕОРЕТИКО-КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

1.1. Понятие и типология компьютерной преступности

На эффективность борьбы с преступностью влияет количество и глубина знаний о ней, а также от специфических особенностей вида преступности, определения причинно-следственных связей. Прогресс в обществе породил новые виды преступлений, в том числе компьютерные. Составляющими криминологической характеристики компьютерной преступности являются следующие: общественная опасность, отделение данного вида преступности от других подобных явлений, её типичные свойства и как следствие определение типологии компьютерных преступлений, данные о социальных условиях, способствующих совершению компьютерных преступлений (экономические, политические, временные и др.), проблемы латентности, изучение личности потенциального преступника, мотивы и цель преступления, особенности потерпевшего лица, а также набор мер по противодействию совершения компьютерных преступлений. Для того чтобы дать характеристику компьютерному преступлению необходимо обособление данного вида преступности в качестве отдельного предмета для исследований, определение терминологии и отличий компьютерных преступлений в определенных обстоятельствах, привязанных к месту и времени.

Относительно недавно в научном сообществе начали дискутироваться такие явления как «компьютерное преступление» и «компьютерная преступность». Впервые явление компьютерной преступности появилось за рубежом, связано это было с появлением первых нарушений, совершенных с применением вычислительных машин, но при этом отсутствовал понятийный аппарат и другие характеристики преступления. Не смотря на отсутствие закреплённого понятия, этот термин активно использовался в

судебной практике и использовался транснационально. Эксперты международного масштаба делали неоднократные попытки развернуть сущность компьютерного преступления, но формализованного понятия получить не удалось, впоследствии проблема была передана на уровень национального масштаба. До сих пор отсутствует единственная позиция относительно широко используемых понятий: «компьютерное преступление», «компьютерная преступность», и в науке данный вопрос и на сегодняшний день является дискуссионным.

В масштабе нашего государства впервые дано определение понятию «компьютерное преступление» весной 1993 года в рамках семинара «Криминалистика и компьютерная преступность»: «компьютерное преступление – это общественно опасное действие, предусмотренное уголовным законом, в котором машинная информация является либо средством, либо объектом преступного посягательства».

С другой стороны, иностранные эксперты под компьютерным преступлением понимают преступление, совершенное с использованием компьютерной техники или направленное против безопасности компьютерной информации. На сегодняшний день количество способов реализации преступлений и правоприменительная практика констатируют необходимость актуализации предложенного термина.

В ряде стран (Южная Корея, Норвегия, Сингапур, Филиппины и др.) существует определение компьютерного преступления как противоправное посягательство, в котором ЭВМ является объектом или орудием совершения преступления, а посягательствами являются: несанкционированный доступ в защищенные компьютерные сети, заражение их вредоносным ПО, незаконное использование компьютерных сетей и информации. Но данное определение несет слишком обширный смысл и включает в себя такие преступные деяния, которые не имеют отношения к компьютерной информации, например, причинение вреда здоровью путем нанесения ударов электронно-вычислительной машиной.

Существует иная позиция других стран (Дания, Швеция, Япония, Швейцария, Россия): компьютерное преступление – это противоправное общественно опасное посягательство с использованием информационно-вычислительных систем либо с воздействием на них. Объект посягательства – информация, которая обрабатывается в ЭВМ, а ЭМВ является орудием посягательства[3]. Следует учитывать, что информация может быть определена, и может содержаться на машинном носителе, ЭВМ или сети ЭВМ. , в таком случае компьютерными преступлениями являются только те, которые связаны с обработкой информации в электронном виде.

Сформировано и третья позиция, где «компьютерное преступление» заменяется на «информационное преступление»[4], причем ЭВМ – один из видов средств для совершения преступления, а в свою очередь объектом является не сам компьютер, а данные, которые обрабатываются с помощью компьютера.

Согласно четвертому мнению компьютерные преступления не сгруппированы в отдельную группу преступлений, а являются лишь составляющим другого преступления, если оно совершенно с помощью средств вычислительной техники. Так, компьютер выступает в качестве средства совершения других, более распространенных в уголовном законодательстве преступлений, и применяется к роли признака для определения состава преступления. Данная позиция применена в законодательстве республик Узбекистан и Беларусь, в статьях 167 «Хищение путем присвоения или растраты» и 168 «Мошенничество» в качестве одного из признаков является использование средств компьютерной техники; в статье 169 «Кража» один из признаков – несанкционированное проникновение в компьютерную систему

[3] Вехов, В. Б. Компьютерные преступления: учебное пособие / В.Б. Вехов. – М.: Финансы и статистика, 1996 – 247 с.

[4] Черкасов, В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий / В.Н. Черкасов. – Саратов, 1995. – С. 80-81.

В последнее время эксперты совершают попытки и отделить те преступления, в которых преступники применяют компьютерные сети. Особенностью таких преступлений является способ достижения цели – удаленный способ. Компьютерное преступление может являться сетевым как один из видов компьютерных преступлений, реализуемые с использованием компьютера или против него. В Германии законодатель использует понятие «киберпреступление», которое включает в себя все противоправные деяния, в которых информация в машинном виде являлась средством или объектом преступления.

Ряд экспертов считают синонимами «компьютерное преступление» и «преступление в сфере компьютерной информации»[5]. Уголовное право определяет термин «преступление», как изменение общественного отношения, которое предполагает связь между обществом в аспекте охраняемых законодательством факторов. Объектом преступления выступают определенные нормативно-правовыми актами действия по легальному и законному использованию компьютерной информации. Таким образом к преступлениям относятся три состава: неправомерный доступ к компьютерной информации; оборот вредоносных программ для ЭВМ; нарушение требований эксплуатации ЭВМ, их системы или сети.

Понятие «компьютерное преступление» на самом деле по смыслу обширнее, и обладает криминалистическими качествами, так как связано с методами и путями реализации преступления. Судебная практика говорит об увеличении вариантов путей совершения преступных деяний. Если ранее уделялось много внимания на шпионаж, мошенничество, вымогательство в аспекте компьютерной информации, то сегодня актуальными проблемами являются информационный терроризм и войны, действия организованных групп на международном уровне с помощью новейших технологий.

[5] Гаджиев, М. С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дисс. ... канд. юрид. Наук / М.С. Гаджиев. – Махачкала, 2004. – 215 с.

Указанные и перечисленные выше изменения качества компьютерных преступлений практически не реально учесть в понятии термина. В связи с этим понятие «компьютерное преступление» следует рассматривать с нескольких точек зрения. Часть авторов определяют главной криминалистическую характеристику, обосновывая свою точку зрения на основании того, что она выступает как своеобразное системно-структурное образование, составляющее часть более общей системы – характеристики преступлений в целом[6]. С этой точки зрения под понятие компьютерного преступления попадают не только преступления в сфере компьютерной информации, но и преступления, совершаемые с использованием компьютерных технологий. Преступления, совершаемые с использованием компьютерных технологий, в зависимости от характера использования компьютеров подразделяются:

а) на преступления, в которых компьютер используется как орудие преступления (например, электронное мошенничество);

б) на преступления, в которых компьютер играет роль интеллектуального средства (например, размещение в Интернете порносайтов с несовершеннолетними).

На основании вышесказанного можно сделать следующие заключения:

1) *При уголовно-правовом подходе* внимание концентрируется на юридическом анализе посягательства, и определение «преступления в сфере компьютерной информации» полностью ему соответствует и вытекает из диспозиций соответствующих статей Уголовного кодекса Российской Федерации.

2) *При криминалистическом подходе* отдельный вид преступлений должен содержать характеристику первичной информации, системы данных о способе совершения и сокрытия преступления и типовых последствиях его применения, личности наиболее возможного преступника и вероятных

[6] Ермолович, В.Ф. Научные основы криминалистической характеристики преступлений / В.Ф. Ермолович. – Минск: ЗАО «Веды», 1999. – 273 с.

мотивах и целях преступления, личности наиболее возможной жертвы преступления, о некоторых обстоятельствах совершения преступления[7]. Термин «компьютерное преступление» отвечает заявленным требованиям.

Только при криминологическом подходе происходит глубокое изучение и анализ преступления, рассматривая совместно индивидуума с условиями внешней среды, которые его окружают, и преступление, как конкретный процесс, длящийся во времени и пространстве. В двадцать первом веке происходит постоянное развитие как научного, так и технического прогресса, которое совершенствует способности людей. Аналогично установленным и закрепленным порядкам проведения процедуры звукозаписи при осуществлении допросов, были разработаны аналогичные правила в отношении видеозаписи при проведении допросов. В настоящее время преступления в различных сферах происходят в том числе и с использованием компьютерных технологий.

Как показывают результаты научной деятельности криминологов, преступная компьютерная деятельность начинается с познавательного процесса и увлеченности компьютером. Последующее осуществление такой деятельности, но уже с использованием незаконных методов может быть двоякого рода. Во-первых, законная предпринимательская деятельность, в процессе которой в целях получения прибыли применяются незаконные деяния, во-вторых, изначально нелегальная деятельность.

Современную отечественную компьютерную преступность можно *определять и как особый вид общественных отношений рыночного характера, выраженных в криминальной форме.* Связь с рыночной экономикой вытекает из широкого применения компьютерных технологий в сфере бизнеса и предпринимательства, наличие которого возможно лишь в рамках рыночных моделей хозяйства. Несмотря на определенную категоричность сделанного вывода, считаем, что наличие самого феномена компьютерной преступности связано в том числе и с фактом капитализации

[7] Курс криминалистики. Р.С. Белкин – М.: Юрист, 1997. – Т. 3. 315 с.

экономики и существующими рыночными отношениями конкуренции. Справедливость последнего утверждения убедительно демонстрируется на примере возникновения феномена криминализации многих общественных отношений и целого массива, неизвестных ранее видов преступлений, связанных с генезисом экономики в России, с началом проведения рыночных реформ.

Обобщая вышеизложенное, подведем некоторые итоги:

Компьютерное преступление определяется как общественно опасное деяние с использованием компьютера, которое нанесло или могло нанести ущерб, а также иное незаконное использование компьютера в совершении преступления.

Компьютерная преступность в «узком значении» включает все преступления в сфере компьютерной информации, а также преступления с использованием компьютерных технологий. В «широком значении» ассоциируется с информационной преступностью, являясь его важной составной частью.

Компьютерная преступность – совокупность совершенных на определенной территории за определенный период преступлений, непосредственно посягающих на отношения по обработке компьютерной информации, а также преступлений с использованием компьютера в целях извлечения материальной выгоды или иной личной заинтересованности. *Информационная преступность* – совокупность совершенных на определенной территории за определенный период преступлений (лиц, их совершивших), непосредственно посягающих на информационные отношения.

Таким образом, понятие «компьютерное преступление» представляется не вполне определенным, но, тем не менее, широко используемым в литературе, в том числе и научной, поскольку иного термина, столь же емко отражающего суть рассматриваемого явления, не предложено. Анализ существующих подходов к определению дефиниции «компьютерное

преступление» наталкивается на проблему: что же взять за основу отнесения преступления к категории компьютерного? Таким объединяющим началом для вышеуказанных определений является единый инструмент обработки информации – компьютер. Поэтому большинство определений компьютерного преступления дается в границах общего подхода: *компьютерное преступление – это преступление, совершаемое с использованием компьютерных технологий.* Законодатель не дает определения компьютерного преступления, но выделяет преступления, посягающих на один и тот же объект.

Компьютерные преступления подразделяются:

а) на экономические преступления;

б) преступления против неприкосновенности частной жизни;

в) преступления против общественной безопасности и общественного порядка.

1.2. Состояние и тенденции компьютерной преступности

За прошедшие годы компьютерная преступность в нашей стране значительно трансформировалась, приобретя по сравнению с 1990-ми гг. более организованный, «профессиональный» и экономически направленный характер. При этом вред, причиняемый российскому обществу преступлениями в сфере компьютерной информации, имеет колоссальный масштаб.

По оценкам экспертов, объем рынка киберпреступности в России в 2012 г. составил 1,93 млрд дол. В свою очередь, американская корпорация Symantec оценила ущерб от киберпреступности в России за 2013 г. в 1 млрд дол., а за 2012 г. – в 1,48 млрд. Между тем общий ущерб от

киберпреступности в мире в 2013 г. составил 113 млрд дол. против 110 млрд дол. в 2012 г.[8].

Информация имеет различия, это объясняется высоким уровнем латентности компьютерных преступлений, а также отсутствием единой международной методики расчета вреда, причиненного киберпреступниками.

Согласно официальной статистике ГИАЦ МВД РФ, за последние годы в России были возбуждены уголовные дела по таким видам преступлений в сфере компьютерной информации, как неправомерный доступ к компьютерной информации (ст. 272 УК РФ) (в 2010 г. – 6 132, в 2011 г. – 2 005, в 2012 г. – 1 930, в 2013 г. – 1 799); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) (в 2010 г. – 1 010, в 2011 г. – 693, в 2012 г. – 889, в 2013 г. – 764); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) (в 2010 г. – 0 [9], в 2011 г. – 0, в 2012 г. – 1, в 2013 г. – 0).

Ппонятие «компьютерные преступления» шире по своему значению и включает в себя не только преступления, предусмотренные ст. 272–274 УК РФ, где предметом преступного посягательства выступает компьютерная информация, но и преступления, где компьютерная информация служит средством совершения преступного деяния, а непосредственный объект состава преступления может включать в себя и другие общественные отношения, например, отношения в сфере собственности. Это позволяет отнести к компьютерным преступлениям такие деяния, как мошенничество с использованием платежных карт (ст. 159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Данный подход преобладает в

[8] Norton report 2013 [Электронный ресурс] Режим доступа: http://go.symantec.com/norton-report-2013. – Загл. с экрана.

[9] Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации [Электронный ресурс] - Режим доступа: http://giz.mvd.ru. – Загл. с экрана.

уголовном законодательстве большинства европейских стран, ратифицировавших Европейскую конвенцию о киберпреступности[10].

Учитывая серьезность компьютерной преступности и существующих киберугроз национальной безопасности РФ, Россия сделала первые шаги по защите своих интересов и суверенитета. Так 15 января 2013 г. президент РФ издал указ № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»[11], в соответствии с которым возложил на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации – информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

По данным Group-IB, международной компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий, выросло и количество, и средний ущерб от целенаправленных атак на банки. Доход хакеров от них перекрыл суммарный заработок от всех остальных способов хищений, сделав банки самой привлекательной мишенью для атак. Уже несколько лет подряд наблюдается снижение объема хищений у физических и юридических лиц с использованием вредоносного ПО для персональных компьютеров. Их место занимают атаки с использованием ПО для мобильных устройств, которые стремительно упрощаются и автоматизируются.

---

[10] Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс] : http://base.garant.ru/4089723/□- Загл. с экрана.

[11] Собрание законодательства Российской Федерации.□- 2013.□- № 3.□- Ст. 178

Целевые атаки на банки, которые только начинают распространяться по миру, происходят в России с 2013 года. Русскоговорящие преступные группы имеют опыт атак практически на все банковские системы.

За 2015 год период ущерб российских банков от целевых атак вырос почти на 300%. Все преступные группы, стоящие за ними, ранее специализировались на хищениях денежных средств у юридических лиц (клиентов банков). Наиболее профессиональные преступные группы, атаковавшие компании, переориентируются на банки, а преступные группы, получившие опыт целевых атак в России, выходят в другие страны. Атаки на банки Западной и Восточной Европы, СНГ, Азиатско-Тихоокеанского региона, Ближнего Востока выполнялись по схожему шаблону.

Хакеры делают ставку на автоматизацию хищений:

- Все новые вредоносные программы для хищений у юридических лиц, появившиеся в России поддаются автоматизации

- С помощью легальных сервисов переводов с карты на карту хакерам удалось полностью автоматизировать атаки на физических лиц, для завершения которых требуется SMS-код подтверждения транзакции с телефона жертвы. Такая атака укладывается в несколько минут и не требует от хакера никакого участия.

Развитие функциональности троянов для мобильных устройств и их доступность стимулируют взрывной рост числа успешных атак. В России ежедневно жертвами становятся 350 пользователей устройств на платформе Android, а объем хищений вырос более чем на 450%. Хищения у физических лиц с помощью троянов для ПК при этом практически прекратились – ими занимается только одна преступная группа. Прогнозируется, что темпы роста объема хищений будут трехзначными по всему миру, поскольку заражения вредоносным ПО становятся незаметнее, а хищения автоматизируются.

Растет число опасных мобильных приложений. Вредоносные программы не только мимикрируют под приложения, стабильно держащиеся в региональных топах, но и отвечают на ситуативные всплески интереса

пользователей: например, они распространялись под видом приложения Pokemon Go. Для продвижения мобильных приложений активно используются инструменты интернет-маркетинга: контекстная реклама по ключевым словам, накрутка установок и отзывов в GooglePlay, SEO-оптимизация сайтов с загрузчиками. Растет количество атак на пользователей мобильных устройств. Под угрозой не только пользователи гаджетов на Android. Не имея возможности заразить шифровальщиком iOS-устройства, преступники блокируют устройства посредством перехвата доступа к iCloud.

Отслеживание местоположения и прослушивание разговоров пользователей мобильных телефонов предлагают все больше легальных компаний. Растет и черный рынок услуг: соответствующие предложения все чаще можно увидеть на хакерских форумах. Техника перехвата трафика привлекает еще больше внимания со стороны атакующих. Android-трояны совмещают инструменты для шпионажа и хищений. Так, практически все мобильные трояны для хищений, активные в России, имеют функционал для перехвата SMS. Это открывает доступ к системам с двухфакторной аутентификацией, например, облачным хранилищам, почте, корпоративным порталам, а через них ко всей персональной и конфиденциальной информации.

Внимание к хакерским атакам со стороны медиа привлекает на рынок новых заказчиков. Технологические аварии, утечки пользовательских данных, остановка бизнес-процессов становятся привлекательным инструментом для борьбы за рынки и покупателей. Появление эффективного шаблона целевой атаки, позволяющего получить доступ к критической инфраструктуре без разработки дорогостоящих вирусов, упрощает атаку для исполнителя и снижает ее стоимость для заказчика. Владельцы бот-сетей для хищений начали продавать доступы к компьютерам, не представляющим для них интереса. Например, переговоры о продаже доступов к рабочим станциям, взаимодействующим со SWIFT, и пакетные предложения для последующих атак с помощью программ-шифровальщиков. Таким же

образом атакующие могут получить доступ к компьютерам, входящим в сети промышленных и энергетических компаний. То есть, если раньше злоумышленники, получавшие доступ к критичной инфраструктуре без возможности его монетизации, ничего с ним не делали, то теперь они ищут покупателя, интересующегося этим доступом. Появляются новые схемы атак. Например, атака может быть замаскирована под шифровальщика, а преступники могут попросить предоставить удаленный доступ к зараженной системе, чтобы провести расшифровку файлов вручную. Усиливается рекрутинговый потенциал террористических групп. Европейский миграционный кризис, ухудшение социально-экономической ситуации, обострение этнических и религиозных конфликтов целом ряде регионов мира питают почву для восприятия пропаганды террористических и экстремистских группировок, которые открыто рекрутируют хакеров в теневом сегменте интернета.

Преступники активнее используют инструменты интернет-маркетинга для продвижения сайтов и приложений с использованием популярных брендов, что не только наносит ущерб репутации, но и приводит к снижению потока клиентов. Контекстная реклама в поисковых системах лишает официальные ресурсы части целевого трафика, а использование преступниками методов SEO-оптимизации приводит к понижению позиций в поисковой выдаче официальных сайтов. Доверие к брендам позволяет успешно атаковать не только физических, но и юридических лиц. Так, зафиксированы создания и продвижения копий сайтов российских промышленных, машиностроительных предприятий, компаний нефтегазового сектора, производителей удобрений для последующего заключения мошеннических контрактов от их имени. Средний подтвержденный ущерб от такой атаки составил 1,5 млн рублей□.

Group-IB делают следующие прогнозы:

Целевые атаки на банки продолжат победное шествие по миру. Команды, занимавшиеся логическими атаками на банкоматы, будут

пробовать себя в атаках на SWIFT. Хакеры начнут уделять больше внимания поиску инсайдеров для предоставления нужной информации и первичного заражения. Средний размер ущерба одной успешной атаки увеличится.

Хищения с помощью троянов для ПК в мире останутся на высоком уровне, но постепенно уступят свои позиции. Атакующие начнут использовать Android-трояны.

Инцидентов с программами-шифровальщиками станет больше. Атаки на компании будут более качественно изменены, что приведет к повышению средней суммы выкупа. Программы-вымогатели усилят направленность на специфичные корпоративные сектора (например, колл-центры, аутсорсинговые бухгалтерские компании накануне сдачи отчетности и т.п.), где у атакующих будет больше шансов зашифровать критичную информацию и требовать выкупа.

Преступники продолжат использовать политические разногласия, чтобы совершать хищения и атаки в других странах, не боясь экстрадиции (примеры: Россия-Украина, Израиль-Ливан, Пакистан-Индия). Хакерские атаки на фоне взаимного недоверия спецслужб также могут быть использованы для оказания влияния на развитие конфликта извне или изнутри оппонирующих стран.

2. ДЕТЕРМИНАНТЫ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

2.1. Причины и условия компьютерной преступности

В криминологии детерминанты преступного поведения классифицируются по различным критериям: объективные и субъективные причины[12], полная и специфическая причины[13], причины разных социальных уровней функционирования, причины, коренящиеся в различных сферах общественной жизни[14]. Каждая из этих классификаций позволяет высветить те или иные стороны воспроизводства преступлений. Наиболее удачной представляется уровневая классификация криминогенных факторов:

первый уровень – социальная среда (макросреда) в целом;

второй – непосредственные факторы формирования личности (микросреда);

третий – сама личность, взаимодействующая с конкретной жизненной ситуацией[15].

Компьютерная преступность является составной частью общей преступности, а значит, порождается в том числе и общими причинами. Противоправное поведение, посягающее на охраняемую законом компьютерную информацию, выступает конкретным результатом существующих не просто социальных противоречий, а противоречий в информационной среде на фоне общегосударственных противоречий. Информационная среда – это сфера деятельности субъектов, связанная с

---

[12] Криминология / под ред. В. К. Звирбуля, Н. Ф. Кузнецовой, Г. М. Миньковского. – М., 1979. – С. 118-201.

[13] Кузнецова, Н.Ф. Проблемы криминологической детерминации / Н.Ф. Кузнецова – М., 1984. – С. 54 – 55.

[14] Сахаров А. Б. Социальные условия и преступность (постановка исследовательской проблемы) // Методологические вопросы изучения социальных условий преступности: Сборник научных трудов / под ред. В. К. Звирбуля. – М, 1979. – С. 6-7.

[15] Кудрявцев, В.Н. Причинность в криминологии / В.Н. Кудрявцев. – М., 1987. – 106 с.

созданием, преобразованием и потреблением информации[16], которая существует внутри общества, пронизывая все его области жизнедеятельности. Поэтому ученые справедливо отмечают, что воздействие среды на противоправное поведение приобретает особую актуальность в условиях научно-технического прогресса, обусловливающего расширение рамок социальной среды личности[17].

Выделим причины компьютерной преступности, её существования и роста в аспектах сфер жизнедеятельности.

1. Экономические причины. Общие причины компьютерной преступности необходимо искать в недостатках экономической политики и экономических отношений. В условиях жесткой конкуренции и безработицы экономика прививает людям стремление к финансовому достатку.

В нашей стране важную роль играет нестабильность экономических и политических условий в жизни общества[18]. Как следствие получилась ситуация, при которой положение экономики провоцирует массовую обиду и злобу на власть, что в результате порождает повышение в обществе преступной активности. Поэтому выделяется несоответствие уровня фактических доходов реальному уровню жизни как одну из причин корыстной мотивации компьютерных преступлений.

Экспертами отмечается, что, наряду с устойчивым формированием социального слоя богатых граждан, устойчиво формируется слой бедных. Такое экономическое положение большей части граждан способствует совершению компьютерных преступлений прежде всего из корыстных побуждений. Преступникам предоставляется реальная возможность получения значительной экономической выгоды за противоправные деяния с

---

[16] Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене» [Электронный ресурс]. – Режим доступа: http://base.garant.ru/135401/. - Загл. с экрана

[17] Антонян, Ю. М. Социальная среда и формирование личности преступника / Ю.М. Антонян. – М., 1975. – 351 с.

[18] Социальная политика: учебник / под ред. Н. А. Волгина. – М.: Экзамен, 2002. – С. 150-156.

использованием ЭВМ, систем ЭВМ или их сети. Большинством исследователей отмечается, что соотношение корысти с другими мотивами в компьютерных преступлениях составляет 60-66%.

Доминированию такой мотивации способствует и наличие большого количества безработных. Спрос порождает предложения, поэтому существующее экономическое положение в государстве порождает двоякую ситуацию. С одной стороны – совершение компьютерных преступлений приносит существенную прибыль преступникам. С другой стороны – для компьютерных преступников появилась возможность реализовать продукт своего интеллектуального незаконного труда на иную выгоду.

Экономическая ситуация является причиной следующей проблемы – отставание профессионального уровня деятельности правоохранительных органов от общего уровня компьютеризации преступной деятельности. Недостаточное финансирование правоохранительных органов не позволяет обеспечивать их новейшими информационными системами и технологиями, является одной из экономических причин. Недостаточное финансирование сказывается на материально-техническом оснащении органов выполнение которых невозможно без наличия современной компьютерной техники. Расследование компьютерных преступлений требует навыков разбираться в тонкостях работы ЭВМ и информационную обеспеченность оперативно-следственной деятельности.

2. Общесоциальные причины. Социальные отношения, аналогично экономическим, многообразны и разноуровневы, существуют на микро- и макроуровнях. Макроуровень характеризует отношения человека с обществом и государством (например, производственные отношения, образование, общественную деятельность и т. п.) и его положение как личности (имеются в виду права человека). Социальные причины обусловлены несовершенством социально-экономических отношений, выражающимся в противоречии между провозглашенными в обществе целями (достижение финансового успеха) и имеющимися легальными

средствами их реализации. Комплекс социальных причин имеет связь и обусловленность со свойствами и спецификой процессов информатизации и компьютеризации. Предполагается скрытый характер преступной деятельности в сфере компьютерной информации, ее свобода и анонимность, отсутствие жесткой регламентации, позволяющие быстро и эгоцентрично придавать забвению морально-нравственные нормы.

Существующая сложная взаимная связь и обусловленность совокупности социальных факторов, способствующих криминализации отношений в информационной сфере, позволяет выделить в качестве одной из социальных причин компьютерной преступности отсутствие социального благополучия в обществе и разрушение системы воспитательного воздействия в решках государства. В настоящее время для страны характерно отсутствие устойчивого социального мира, что вызывает состояние напряженности и негативных ожиданий в обществе, с одной стороны, и наличие социальных групп, ориентированных на противозаконный образ жизни, – с другой. Отсутствие полного соблюдения принципа социальной справедливости и обеспечения нормального в правовом отношении существования людей приводит к неустойчивому, конфликтному положению между ними и неизбежно ведет к преступлениям. По мнению экспертов, 98% населения считают приемлемым нелегальный образ жизни, а 85% совершают те или иные противозаконные действия[19]. У населения формируются вульгарно рыночные приоритеты в системе ценностей, при явном игнорировании социальной, а иногда и правовой составляющей. Опасность социального неблагополучия, отсутствие гарантий социальной и правовой защиты порождает убеждение в бессилии государства и необходимости обеспечить себя только самому.

В современной реальности «политическая мотивация» порождает терроризм, в том числе и международный. К новым видам преступлений

[19] Банковский бизнес в России: криминологические и уголовно-правовые проблемы / Н.Я. Заблоцис и др. – М., 1994. – С. 56.

следует отнести высокотехнологичный терроризм нового поколения. Такой терроризм способен продуцировать системный кризис всего мирового сообщества или по крайне мере стран с развитой инфраструктурой информационного обмена. Это становится возможным потому, что современная цивилизация выстроена вокруг высоких технологий информационного обмена. Их реализуют средства обработки и хранения информации: компьютеры и созданные на их основе специализированные системы: банковские, биржевые, архивные, исследовательские, управленческие, а также средства коммуникации – от спутникового телевидения и связи до сотовых телефонов.

3. Причины правового характера. В качестве одной из причин компьютерной преступности является недостаточное правовое регулирование общественных отношений в информационной сфере на всех уровнях. Анализ законодательства свидетельствует о том, что ряд вопросов находятся вне поля правового регулирования, а некоторые законопроекты – на стадии разработки. Принятые ранее нормативные акты нуждаются в корректировке с учетом настоящего развития государства и общества, а также достижений науки и техники. Ненадлежащая правоприменительная практика в отношении правонарушений в информационной сфере является одной из причин компьютерной преступности. Развитие экономических отношений в мире происходит под влиянием процессов внедрения средств компьютерной техники. На сегодняшний день многие организации в нашей стране, заинтересованы в привлечении клиентов, имеют свои ресурсы в Интернете, которые используют как для рекламы собственных продуктов и оказываемых услуг, так и для электронного документооборота с контрагентами. Вместе с тем действующее уголовное законодательство России не отделяет преступления, совершаемые в сфере электронной коммерции, от остальных экономических преступлений и преступлений против собственности, что ослабляет для работников правоохранительных органов возможность четко определить наличие в действиях субъектов

электронной экономической деятельности состава преступления. Как следствие, фактов привлечения в России к уголовной ответственности за преступления в данной сфере практически нет. Само расширение компьютерной преступности вызывает ее дальнейший рост и становится привычной формой существования в обществе.

Обобщая вышеизложенное, подведем некоторые итоги:

1. Причины компьютерной преступности в настоящее время только начинают выявляться. Во многом это объясняется первоначальным этапом формирования информационных отношений и еще недостаточной компьютеризацией общества, а в этой связи – недостаточным вниманием к этому виду преступности отечественной криминологией.

2. Компьютерная преступность является составной частью общей преступности, поэтому порождается как общими социальными, так и специфическими противоречиями в информационной сфере. Информационная сфера, в свою очередь, существует внутри общества, пронизывая все его области жизнедеятельности, расширяя рамки социальной среды человека и преломляя обшесоциальный причинно-следственный комплекс противоречий. Выделяются группы правовых, экономических, социальных причин, которые оказывают непосредственное влияние на совершение компьютерных преступлений.

2.2. Личность компьютерного преступника

Криминологами признано, что в качестве непосредственной причины преступления выступает сложное сплетение объективных и субъективных факторов и отдельных частей взаимодействующих явлений – личности и среды. Личность, выступая в единстве всех ее социальных, нравственных и психологических свойств и признаков, формируется в процессе жизни и деятельности человека. Формирование личности является сложным и противоречивым развивающимся "по спирали" процессом, который сам

подготавливает условия для своего последующего развития, является в некотором роде причиной самодвижения. Поэтому, говоря о причинах совершения компьютерных преступлений, необходимо выделить и личностный уровень.

Авторы по-разному подходят к определению личности преступника. Одни полагают, что личность преступника представляет собой систему социальных и психических свойств, образующих ее общественную опасность, которая детерминирует совершение преступления[20]. Другие – как один общий социальный тип, к которому можно отнести всех тех, кто совершил преступление[21]. Третьи – как совокупность социально значимых негативных свойств, образовавшихся в нем в процессе многообразных и систематических взаимодействий с другими людьми[22]. В целом, личность преступника можно определить как совокупность присущих ей биолого-психологических и социальных особенностей, антиобщественных взглядов и нравственных ориентиров, определивших выбор общественно опасного пути для удовлетворения своих потребностей, либо непроявление необходимой социальной активности в предотвращении общественно отрицательного результата своего виновного поведения. Это определение охватывает тех, кто совершил преступление умышленно, и тех, кто виновен в преступной неосторожности. Кроме того, оно содержит перечень признаков, которые являются предметом криминологического изучения:

1) *социальный статус* как совокупность признаков, отражающих место преступника в системе общественных отношений;

2) *социальные функции,* выраженные посредством показателей реальных проявлений личности преступника в основных сферах его

---

[20] Криминология / под ред. Н. Ф. Кузнецовой. – М.: Зерцало, ТЕИС, 1996. – С. 44.

[21] Ведерников, Н.Т. Личность обвиняемого как объект изучения на предварительном следствии / Н.Т. Вердников // Актуальные вопросы борьбы с преступностью. – Томск: Томский университет, 1990. – С. 99.

[22] Антонян, Ю.М. Преступник как предмет криминологического изучения / Ю.М. Антонян // Вопросы борьбы с преступностью. Вып. 34. – М., 1981. – С. 21.

деятельности (профессионально-трудовой, социально-культурологической, социально-бытовой);

3) *нравственно-психологические установки,* отражающие отношение преступника к общегражданским обязанностям, государственным органам, закону, правопорядку, семье, иным культурным ценностям, к самому себе и окружающему миру.

В криминологическом изучении личности преступника выделяются два основных подхода. *Первый подход* предусматривает изучение личности конкретного преступника. В данном случае о личности преступника можно говорить лишь применительно к субъекту конкретного преступления. Для определения, содержит ли деяние определенный состав преступления и возможна ли уголовная ответственность, необходимо установить конкретное лицо и факт обладания им всей совокупностью установленных в уголовном законе признаков. Понятие и особенности субъекта компьютерного преступления будет рассмотрено в главе 3-й диссертационного исследования.

Второй подход дает представление об общих свойствах группы лиц, совершающих преступления. Применительно к компьютерным преступлениям диапазон таких лиц широк: от беспечных подростков, манипулирующих своими компьютерами, до особо опасных преступников, являющихся членами хорошо организованных, мобильных и технически оснащенных преступных групп. Опираясь на выделенные типы компьютерных преступников, охарактеризуем их социально-психологические особенности и деформации, которые могут обусловливать совершение уголовно-противоправных деяний в сфере компьютерной информации, и на их основе сформулируем индивидуально-личностной причиной компьютерного преступления.

Первая группа – лица с ярко выраженными целями, отличающиеся по уровню профессиональной компьютерной подготовки, по социальному, должностному (или служебному) положению, респектабельности, имеющие

ориентацию на совершение преступления с использованием возможностей компьютерных технологий. Они могут находиться внутри системы – это банковский персонал, сотрудники фирм и учреждений, имеющие доступ к финансовым ресурсам. Используя свои специальные знания, они совершают преступления, руководствуясь корыстными и иными меркантильными мотивами, из политических соображений и мести или иной личной заинтересованности. На долю этих преступников приходится максимальное число совершенных особо опасных посягательств, различного рода должностных преступлений, связанных со шпионажем в области промышленной, государственной, экономической и другой безопасности, с проникновением к сведениям, составляющим коммерческую, банковскую, профессиональную тайну, тайну частной жизни.

В этой группе выделяются «узкие профессионалы», технический уровень которых позволяет заниматься созданием вредоносных компьютерных программ или их модификацией. Создание такой программы представляет собой комплекс операций, состоящих из подготовки исходных данных, предназначенных для управления процессами уничтожения, блокирования, модификации или копирования информации[23]. Такую работу могут исполнить только высококвалифицированные специалисты: профессионально подготовленные программисты; лица, имеющие возможность модифицировать программу с целью сделать ее вредоносной. К ним примыкают и лица, занимающиеся незаконным обращением вредоносных программ или машинных носителей с такими программами.

Общими признаками для указанной группы являются: наличие специальной компьютерной подготовки; доступ к ЭВМ, системе ЭВМ или сети ЭВМ; наличие целеустремленной, продуманной подготовки к совершению преступления; совершение преступления по заранее

---

[23] Уголовное право Республики Казахстан. Особенная часть: учебник / под ред. И. Ш. Борчашвили и С. М. Рахметова: В 2-х ч. Часть 2. – Алматы: Институт Данекер, 2000. – С. 93.

сформировавшемуся мотиву; применение системы продуманных мер к сокрытию следов преступления; совершение преступления, как правило, в целях решения жизненных финансовых проблем; многократность совершения преступлений с обязательным использованием действий, направленных на их сокрытие; обладание устойчивыми преступными навыками.

Вторая группа – это лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности. Исследователи к ним относят хакеров и крэкеров. «Хакер» – это пользователь вычислительной техники, занимающийся поиском и разработкой незаконных способов проникновения в ЭВМ, системы ЭВМ или их сети и несанкционированного использования последних. Хакерская среда определяется как computer undergraund (компьютерное подполье), в котором выделяются представители мирового класса – 0,1%, профессионалы – 9,9%, любители – 90%.

Грань между «хакерами» и «крэкерами» очень тонка и проводится по целям деятельности. Первые осуществляют поиск и устранение слабых мест системы защиты в познавательных, исследовательских целях. Вторые – простые воры, которые взламывают системы защиты, незаконно проникают в компьютерную сеть и крадут, подменяют или иным несанкционированным способом используют компьютерную информацию в преступных целях.

По нашему мнению, подвидом хакеров являются также фрикеры (freak) – пользователи, предпочитающие альтернативные варианты оплаты теле- и прочих коммуникационных услуг. В России наибольшее распространение получил телефонный фрикинг, действующий, как правило, в городских мегаполисах. В крупных городах установлены таксофоны на электронных кредитных картах, в основе которых лежат чипы определенного стандарта. Путем установления разновидности временной

диаграммы такого чипа фрикер перепрограммирует его и на карте открывается неограниченный кредит на ведение телефонных переговоров.

Общими признаками для указанных подгрупп, которые и обусловливают совершение преступления, являются: завышенная оценка своих профессиональных и, как следствие, интеллектуальных способностей; отсутствие интереса к проблемам повседневной жизни, определенная поведенческая дерзость (бахвальство о совершенном преступлении; совершение преступления как демонстрация компьютерного профессионализма или способ зарабатывания авторитета среди сотоварищей). Преступление, как правило, совершается открыто. Могут использоваться оригинальные способы его совершения или собственные ноу-хау. Для данной категории лиц характерна внезапность формирования умысла на совершение преступления, непринятие мер к его сокрытию, а методы взлома атакованной ЭВМ, системы ЭВМ или сети ЭВМ могут даже тиражироваться среди «коллег».

Третья группа – это лица, страдающие новым видом психических расстройств – информационными болезнями или компьютерными фобиями, чья психика деформирована постоянным использованием компьютерной техники. В связи с охватившим современное общество процессом всеобщей компьютеризации, оснащением рабочих мест персональными компьютерами, внедрением их в повседневную бытовую жизнь многие люди подвергаются

- технострессу – болезни адаптации, когда человек не способен адекватным образом реагировать на информационно-компьютерную технологию;

- социальной изоляции – состоянию, связанному с усилением в человеке психологии индивидуализма, с абстрагированием человека от окружающей его среды обитания и общения. Потребности в новых впечатлениях удовлетворяются не за счет знакомств, традиционного занятия спортом или путешествия, а прогулками по Интернету. Исследователи

констатируют факт «виртуализации» духовной жизни, которая отделяет компьютерных пользователей от человеческого социума.

Печать, радио, телевидение, а сейчас и компьютерные сети (к примеру, Интернет) превратились в мощный инструмент психологического воздействия, охватывая своим влиянием не просто множество людей, а миллионы. Современные средства приема и передачи информации, к числу которых относится, в первую очередь, Интернет, для многих людей стали единственными источниками формирования представления о многих явлениях, понятиях и стереотипов поведения. Поэтому к данной группе следует относить также *лиц, страдающих компьютерной зависимостью, не связанной с болезненным расстройством психики.*

Типичным компьютерным преступником может быть как немолодой хакер, использующий телефон и домашний компьютер для получения доступа к большим компьютерам, так и служащий, которому разрешен доступ к системе[24].

По официальной статистике, в США компьютерные преступления, совершенные служащими, составляют 70-80% ежегодного ущерба, связанного с компьютерами. Остальные 20% – это действия нечестных и недовольных сотрудников и совершаются они по целому ряду причин[25].

Наибольшую опасность представляют лица из числа штатных сотрудников – системные администраторы, специалисты по информационной безопасности, операторы ПК, инженеры и другие пользователи.

Существенную угрозу безопасности могут нанести конкуренты или лица, занимающиеся промышленным шпионажем, а также профессиональные преступники и кибертеррористы. Представители этих групп осуществляют противоправную деятельность в широком диапазоне от

[24] Старостина, Е.В. Защита от компьютерных преступлений и кибертерроризма / Е.В. Старостина, Д.Б. Фролов. – М.: Изд-во Эксмо, 2005. – С.29

[25] Scbwartau W. Information Warfare: Chaos on the Electronic Superhighway. – NY, 1994. – P.215-248

корпоративного шпионажа до чрезвычайно опасных диверсий против вычислительных систем жизненно важных объектов[26].

На основании вышеизложенного подведем некоторые итоги:

1. Основные индивидуально-личностные причины компьютерных преступлений.

Объективные причины

1. Отсутствие гарантированной защищенности программных продуктов, бесконечные возможности разработки новых компьютерных программ, наличие профессиональных знаний и навыков, доступность к интересующим компьютерным базам (относительно первой группы компьютерных преступников).

2. Принципиальная ориентация работы с информацией на востребованность, творческий поиск, высокая степень анонимности преступного компьютерного поведения, широкое поле для проявления интеллектуальных возможностей в открытом информационном пространстве (относительно второй группы компьютерных преступников).

3. Доступность и информационная привлекательность компьютерной среды, слабая формализация поведенческих реакций пользователей (относительно третьей группы компьютерных преступников).

Субъективные причины

1. Ярко выраженная автономия профессионального самосовершенствования, стремление достичь корыстных целей с помощью использования компьютерных технологий (относительно первой группы компьютерных преступников).

2. Непрофессиональные знания основ информатики, стремление достичь высокой технической самостоятельности и компьютерной изобретательности (относительно второй группы компьютерных преступников).

---

[26] Осипенко, А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт / А.Л. Осипенко. – М.: Норма, 2004. – С. 152

3. Социально-психологические и медико-личностные характеристики, особенности индивида-пользователя (относительно третьей группы компьютерных преступников).

2.3. Виктимологические аспекты компьютерной преступности

Потерпевшими от компьютерных преступлений могут быть как отдельные лица, так и определенные социальные группы.

В криминологической литературе рассмотрено множество факторов, влияющих, по мнению исследователей, на совершение преступления[27]. Основываясь на изложенных в криминологической литературе научных подходах, и с учетом особенностей совершения компьютерных преступлений виктимологические факторы, влияющие на совершение преступлений в сфере компьютерной информации, по своему содержанию нами подразделяются на индивидуально-личностные, социальные, поведенческие. К виктимологическими факторам могут быть отнесены как типичные свойства физических лиц или общности людей, которые превращают их в объект преступных посягательств, так и их субъективные, также типичные свойства, которые снижают способность самостоятельно обеспечивать свою защиту. То есть сначала лицо привлекает к себе внимание криминальных элементов, а затем, если это лицо не обеспечило себе должной охраны, оно становится жертвой посягательства. Получается, если бы лицо позаботилось о своей безопасности, то оно не стало бы жертвой.

Таким образом, содержание понятия потерпевшего от компьютерного преступления как физического лица связано с его статусом (с совокупностью прав и обязанностей, сферой деятельности), поведением и ролью в криминогенно-криминальном механизме отдельного преступления. Под

[27] Глухова, А. А. Виктимологические факторы преступности: дис. ... канд. юрид. наук / А.А. Глухова. – Н. Новгород, 1999. – 278 с.

воздействием виктимологических факторов лицо становится потенциальной или реальной жертвой преступления.

Применительно к физическому лицу – это *совокупность индивидуально-личностных (социально-психологических) свойств,* связанных с особенностями социализации его личности. Виктимность конкретного индивида – это потенциальная способность его оказаться в роли жертвы преступления в результате отрицательного взаимодействия его личностных качеств с внешними факторами. Преступник обычно хорошо информирован о виктимности потенциальной жертвы. Информация не остается без его внимания: пол, возраст, профессия, специальность, должностное и семейное положение жертвы нередко играют существенную роль в механизме преступления. По классификации потерпевших, данных В. Устиновым и Д. Ривманом, выделяются:

«нейтральный» тип – поведение потерпевших такого типа во всех отношениях безупречно и никоим образом не вызывает преступных действий; в пределах своих возможностей данные жертвы могут критически осмысливать ситуацию;

«некритичный» тип – поведение потерпевших такого типа отличается неосмотрительностью, неумением правильно оценить жизненные ситуации, легковерностью и доверчивостью. Они, если не видят очевидной опасности ситуации, то, естественно, допускают, что их поведение выходит за рамки правомерного.

Применительно к компьютерным преступлениям к первому типу относятся *потерпевшие пользователи мобильной связи.* Это абоненты различных компаний сотовой связи, которые из-за ограниченности технических навыков, стесненности в финансовых средствах используют слабо защищенные выходы в сеть Internet и становятся жертвами вирусных программ, которые несанкционированно «снимают» денежные средства с баланса пользователей. К ним примыкают потерпевшие пользователи телефонной связи – абоненты, которые становятся жертвами телефонных

«пиратов». В Москве ими стали около 60 тыс. человек, а общий ущерб МГТС достиг уровня 40 млн.долл. Ко второму типу относятся *потерпевшие от компьютерных пиратов.* Это рядовые пользователи, которые в силу дороговизны лицензированной программной продукции используют её контрафактные копии и тем самым становятся потенциальными жертвами. По оценкам российского представительства корпорации «Майкрософт», сегодня 89% компьютерных программ в России – пиратские. Для сравнения: продажи пиратских программ в Сингапуре составляют примерно 59%, в Малайзии – 80%, Таиланде – 80%, Филиппинах – 92%, Китае – 96% от общего числа продаж.

Виктимные свойства потенциальных потерпевших формируются под воздействием не только внешних – социальных, но и внутренних – психологических черт, поэтому применительно к потерпевшим от компьютерных преступлений можно выделить еще один тип «патологический». К этому типу следует относить потерпевших, поведение которых характеризуется патологической компьютерной зависимостью, неболезненными формами пристрастия к компьютерным играм или многочасовому пребыванию в Internet, что обусловливает совершение преступления против них. Поведение потерпевших такого типа отличается привыканием к «виртуальному» образу жизни, систематичностью в установлении виртуальных контактов, легковерностью и доверчивостью при взаимодействии с виртуальными партнерами. Психологическая характеристика личности таких потерпевших имеет значение, в первую очередь, применительно к тем категориям компьютерных преступлений, в которых указанные черты обусловливают их совершение. Например, жертвой от мошенничества на виртуальных биржах в первую очередь могут стать те участники, которые систематически с маниакальной зависимостью играют на виртуальных биржах, пытаясь таким образом решить свои финансовые проблемы. Потенциальные жертвы не видят очевидной опасности ситуации и поэтому могут оказаться в роли жертвы преступления

в результате отрицательного взаимодействия внутренних личностных качеств с внешними факторами.

Если в результате компьютерного преступления вред причиняется определенной общности людей, то виктимологическими являются факторы социального характера, способствующие через сложную систему взаимосвязей совершению конкретного преступления. К *факторам социального характера* относится, в частности, положение потенциальной жертвы преступления в социальной иерархии общества. Когда речь идет о выборе организации как жертвы планируемой кибератаки, то её репутация в промышленно-финансовых кругах будет иметь определяющее значение. Естественно, что преступник своим объектом скорее выберет банк, процветающую компанию, богатый холдинг, чем какую-нибудь фирму по реализации мелкооптовой продукции. Наглядным примером может служить факт изъятия информации за период с марта 2003 года по сентябрь 2004 года из компьютерного банка данных Центробанка России, о котором в средствах массовой информации было объявлено только в апреле 2005 года.

К виктимологически значимым факторам относятся *поведенческие (деятелъностные) факторы,* предопределяющие совершение компьютерного преступления. Поведенческие факторы, при которых лицо становится (или может стать) потенциальной жертвой преступления, представляют собой результат взаимодействия среды пребывания и личностных социально-психологических свойств. Причем такое взаимодействие может привести к самым разным результатам. Конкретная жизненная ситуация является объективным фактором, который воспринимается лицом с его субъективных позиций. Поэтому поведение потерпевших от преступлений в сфере компьютерной информации, как и в других видах преступного поведения, может быть правомерным, противоправным или нейтральным (безразличным с точки зрения права).

Причины виктимного поведения потерпевших от компьютерных преступлений могут быть обусловлены разными обстоятельствами. Органы,

ведущие расследование, обычно рассчитывают на помощь «потерпевшей стороны», но необходимость в изучении большого количества служебных документов не всегда желательна для юридического лица, и оно выбирает роль латентного потерпевшего. Нельзя не учитывать и тот факт, что в случае уголовного следствия убытки от расследования могут оказаться выше суммы причиненного преступлением ущерба, возмещаемого в судебном порядке. Поэтому многие организации предпочитают ограничиваться разрешением конфликта своими силами, нередко это завершается принятием мер, которые вряд ли исключат впоследствии рецидив компьютерного преступления. В таких ситуациях можно говорить о «рецидивной виктимности» к компьютерным преступлениям.

Применительно к поведению потерпевших – физических лиц – субъективные причины могут быть следующими:

- использование зараженных носителей информации;
- отсутствие контроля доступа к собственной ЭВМ;
- использование простых паролей к личной информации;
- халатность пользователей;
- низкая культура общения пользователей в сети;
- отсутствие навыков использования ЭВМ и программного обеспечения;
- нахождение с преступником в социально значимых отношениях, в силу которых преступники и избирают их объектом своего преступного посягательства. Это могут быть родственные, супружеские, соседские, товарищеские, дружеские и служебные отношения.

Социально-психологические личностные свойства потерпевших физических лиц, связанные с особенностями социализации их личностей, факторы социального характера, относящиеся к положению потерпевшей организации в социальной иерархии общества, поведенческие

(деятельностные) факторы «провоцируют» возможность совершения компьютерных преступлений.

Таким образом, у компьютеров, хранящих массу ценной, а порой и охраняемой законом информации, присутствует особое свойство, которое можно определить как «компьютерная» уязвимость или технологическая виктимность.

Обобщая вышеизложенное, подведем некоторые итоги:

1. Компьютерные преступления характеризуются, отсутствием прямого контакта с жертвой. Противоправные деяния в сфере компьютерной информации совершаются опосредованно – с помощью ЭВМ, систем ЭВМ или их сетей. Жертвы посягательства являются обезличенными, неперсонофицированными для компьютерного преступника. В связи с этим виктимность потерпевшего как нежелательная совокупность его личностных и поведенческих черт может играть существенную роль в качестве условия, способствующего преступлению. Информация о таких чертах помогает не только точнее очертить круг подозреваемых лиц, но и предоставляет возможность глубже разобраться в причинах конкретного преступления и соответствующего видового ряда.

2. Виктимологические факторы, влияющие на совершение преступлений в сфере компьютерной информации, с учетом изложенных в криминологической литературе научных подходов к данной проблеме и принимаемых во внимание особенностей совершения компьютерных преступлений, подразделяются на индивидуально-личностные, социальные и поведенческие.

Виктимологические факторы, провоцирующие возможность совершения компьютерных преступлений, рассматриваются как единый причинно связанный процесс, находящийся, если даже не в прямой зависимости с преступлением, то в определенной опосредованной связи, поскольку личностная уязвимость может остаться гипотетической и «не

востребованной», а может быть реализованной преступным посягательством.

3. В виктимологическом плане непосредственная жертва преступления рассматривается как потерпевший, т.е. лицо, с одной стороны, непосредственно пострадавшее от преступления, а с другой – являющееся носителем реализованной виктимности. Потерпевшие от компьютерных преступлений подразделяются на физических лиц и определенные общности людей в разной степени интеграции.

Традиционные типы потерпевших (нейтральный и некритичный), рассмотренные применительно к компьютерным преступлениям, дополнены «патологическим» типом, к которому отнесены лица, чьё поведение определяется наличием не только традиционно признаваемых виктимологических факторов, но и личностными психологическими особенностями, вызываемыми патологической компьютерной зависимостью и не болезненными формами пристрастия к компьютерным играм или пребыванию в Internet, что может привести к социальной дезадаптации, нарушению имеющихся общественных связей. Виртуальный вид общения задает новые качества личности, а компьютерная зависимость из личностного фактора трансформируется в криминологический.

3. НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

3.1. Формы противодействия компьютерной преступности

В теории употребляется множество терминов, призванных понятийно определить сущность государственно-правового воздействия на преступность. Традиционные термины «борьба с преступностью»[28] и «предупреждение преступности»[29] постепенно заменяются иными: «война с преступностью», «противодействие преступности», «контроль над преступностью»[30] и др. В терминологическом отношении в словарях русского языка борьба трактуется как активное столкновение противоположных интересов, война – как указание на антагонистическое противоречие, профилактика – как совокупность мероприятий, предупреждающих от чего-то или предохраняющих что-либо, превентивный – предохраняющий что-либо, предупреждающий, пресечение – как деятельность, направленная на прекращение уже чего-то начатого, противодействие – как идти наперекор чему-либо, мешать чему-либо, контроль – как наблюдение за кем-либо, чем-либо с целью проверки. Подобное разграничение представляется искусственным, противоречащим смысловому значению указанных терминов, поэтому они используются в руководящих документах и нормативных актах как взаимозаменяющие.

С точки зрения обеспечения социального спокойствия в обществе предупредительная деятельность государства предусматривает *пресечение* преступлений посредством принятия мер, направленных на прекращение

---

[28] Криминология. учебник для юридических вузов / под ред. А. И. Долговой. – М., 1997.

[29] Лунеев, В.В. Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями / В.В. Лунев // Государство и право. – 2000. – № 9.

[30] Криминология: преступность как свойство общества. Краткий курс. – СПб: ЛАНЬ, 2001.

действий лиц, готовящих или покушающихся на преступление; *предотвращение* преступлений посредством выявления лиц, замышляющих конкретные преступления; *противодействие* преступлениям посредством выявления и устранения причин и условий, способствующих их совершению, и применению соответствующего комплекса мер.

В социальном плане из трех названных выше аспектов предупреждения преступности наибольший интерес представляет противодействие как комплексная система мер, сформулированная на знаниях причин и условий, способствующих совершению преступлений (или отдельных видов преступлений), и ориентированная на опережение их действия. Этим меры противодействия кардинально отличаются от мер пресечения и предотвращения, которые носят пост фактический характер.

Борьба с компьютерной преступностью основывается на взаимодействии государства, общества, отдельных пользователей на факторы, сопутствующие противоправному поведению в информационной сфере. Осуществление такого целенаправленного воздействия возможно совокупностью методов и средств различных отраслей права. Возможности криминального цикла (уголовного, уголовно-процессуального, уголовно-исполнительного законодательства) должны сочетаться с нормами гражданского права. Человечество перепробовало самые разнообразные средства уголовных репрессий, и в настоящее время ученые все чаще говорят о «кризисе наказания» и кризисе всей системы уголовной юстиции[31]. Отсюда – повышенное внимание к иным превентивным мерам, которые должны реализовываться посредством максимально полной, исчерпывающей регламентации конкретных общественных отношений как своеобразного заслона уголовно наказуемым деяниям.

Противодействие компьютерной преступности без надлежащей нормативной базы (основополагающего закона и систематизации прочих

[31] Жилинский, С. Э. Правоохранительная деятельность / С.Э. Жилинский // Российская криминологическая энциклопедия. – М., 2000.

законов и подзаконных актов в данной области) может оказаться неэффективным. Криминологическое законодательство в России имеется. Его можно разделить на две основные части. Первую часть составляет уголовное законодательство в широком его смысле, которое включает в себя наряду с нормами материального права также нормы уголовного процесса и уголовно-исполнительного права. Вторая часть – это криминологическое законодательство в узком смысле слова, которое регулирует не связанную с применением уголовной репрессии деятельность, предупреждающую совершение преступлений. Этот пласт законодательства складывается из нормативных актов, регламентирующих криминологическую политику государства; ресоциализацию криминогенных контингентов населения; контроль финансовой деятельности, а также оборота наркотиков, сильнодействующих веществ, оружия и боеприпасов, культурных и исторических ценностей, валюты и др., профилактику мелких правонарушений и аморальных поступков несовершеннолетних; виктимологическую профилактику преступлений; деятельность самих субъектов социального контроля преступности и др.

В зависимости от средств и методов, функционально предопределяемых характером регулируемых законом общественных отношений, противодействовать преступности можно посредством установления правового контроля, который можно подразделить на два вида: позитивный и репрессивный.

Позитивный правовой контроль над преступностью включает в себя совокупность правовых норм, регламентирующих в отраслевом порядке соответствующие правоотношения. Степень эффективности позитивного правового контроля находится в прямой зависимости от глубины и четкости механизма правового регулирования позитивных общественных отношений, обоснованности правовых предписаний, их общественной полезности и экономичности в правовом смысле.

Эти критерии позволяют проанализировать нынешнее состояние права применительно к позитивному контролю над компьютерной преступностью. С этой точки зрения контроль выражается в правовых нормах, регулирующих в соответствующих отраслях права информационные отношения, и устанавливающих порядок функционирования информационных ресурсов, а также условия использования информационного продукта в целях, не влекущих уголовно-правовую ответственность. Речь идет о защите открытой информации, ориентированной на коммерческую среду деятельности, широкого пользователя ЭВМ, системы ЭВМ или их сети. Защита средствами позитивного правового контроля осуществляется посредством норм конституционного, международного, информационного, гражданского и административного права.

Репрессивный правовой контроль, прежде всего, обеспечивается нормами уголовного права и уголовно-процессуального права. Последние, являясь формой воплощения уголовно-правовых норм, носят постфактический характер. Поэтому первостепенное значение для решения проблем репрессивного правового контроля имеет регламентация отношений в сфере компьютерной информации средствами материального уголовного права. И в этой связи Уголовный кодекс РФ предусматривает ответственность за нарушение авторских и смежных прав (ст. 146), незаконное использование товарного знака (ст. 180), а также самостоятельный уголовно-правовой институт «Преступления в сфере компьютерной информации» (ст.ст. 272-274). Вопросы совершенствования форм и методов репрессивного правового контроля над компьютерными преступлениями имеют актуальное значение, поскольку случаи совершения компьютерных преступлений имеют тенденцию постоянного роста. Такое положение дел имеет место на фоне роста числа пользователей компьютерных сетей и объемов передаваемой информации.

Уголовно-правовые нормы содержат в себе два аспекта: общую и частную превенцию преступлений. Общая превенция обращена к потенциальным преступникам, частная – к лицам, уже совершившим преступление. При этом негативный аспект общей превенции направлен на устрашение потенциального преступника, позитивный – на попытку поддержки и укрепления законопослушания. Негативный аспект специальной превенции определяется как стремление устрашить индивида совершать новые преступления. Позитивный – подразумевает ресоциализацию отдельного человека. Следовательно, общая превенция предполагает как установление запрета на то или иное поведение под страхом уголовного наказания, так и подкрепление действия запрета распространением сведений о применении наказания к конкретным лицам.

Криминологи давно поставили под сомнение действенность позитивной составляющей общей превенции и возможность реального удержания от совершения преступления запугиванием уголовным наказанием. Нельзя наказывать для того, чтобы устрашить других. Действие частной превенции более реально потому, что такие виды наказания как арест, ограничение свободы, лишение свободы могут пресечь преступную деятельность, удержать преступника от совершения новых преступлений на какой-то период. Меры наказания, связанные с финансовым воздействием на преступника (штраф, обязательные и исправительные работы), могут продемонстрировать ему экономическую невыгодность совершения преступлений.

Таким образом, из осознания того, сколь велико число людей, нарушающих уголовный закон, и сколь мала результативность мер уголовной репрессии, вытекает осознание того факта, что контролировать поведение людей посредством одних законодательных санкций практически невозможно. Поэтому эффективность правового контроля над компьютерной преступностью предполагает комплексный характер решения задач средствами позитивного и репрессивного правового контроля на фоне

реализации комплекса государственных мер социально-экономического, политического и организационного характера, обеспечивающих доминирующую роль права и законности в общественной жизни и в информационной сфере в частности. В государстве только предпринимаются попытки формирования «законодательного пакета прав», связанных с информационным продуктом и ориентированных не на элемент собственности, а на правовой контроль за использованием информации и нормативным регулированием отношений в сфере компьютерной информации.

При создании правовой основы процессов информатизации и компьютеризации необходимо учитывать:

- международные нормы в сфере информатизации;

- систему национального законодательства в разрезе всех её уровней (от конституционных норм и основных общих федеральных законов до узко специальных нормативно-правовых актов) в целях обеспечения преемственности и совместимости разноуровневых законов и консолидации нормативно-правовых норм;

- ведомственные подзаконные акты в сфере применения информационного продукта в целях их совершенствования, соответствия и конкретизации федерального законодательного правового массива;

- эффективность механизмов обеспечения действенного позитивного правового контроля в сфере информатизации и компьютеризации;

- правоприменительную практику и её соответствие имеющемуся национальному и международному информационному законодательству.

Очевидно, что комплексный характер правового регулирования преступности в информационной сфере требует и комплексного подхода к формулированию основополагающих задач и форм их достижения, который должен учитывать перспективу построения информационного общества на географическом пространстве Российской Федерации. При этом основополагающим фактором в этом процессе является государственная

политика в области информатизации и компьютеризации Российской Федерации, формирующаяся по следующим основным направлениям:

- создание и развитие федеральных и региональных систем и сетей информатизации с обеспечением их совместимости и взаимодействия в едином информационном пространстве России;

- формирование и защита информационных ресурсов государства как национального достояния;

- обеспечение интересов национальной безопасности в сфере информатизации;

- формирование законодательной базы в сфере информации и информатизации;

- развитие отечественной индустрии телекоммуникационных и информационных средств;

- осуществление международного сотрудничества по обеспечению интеграции России в мировое информационное пространство.

Приведенный перечень не является исчерпывающим и носит прогностический характер в части определения упреждающих мер правового контроля над преступлениями в сфере компьютерной информации. Вместе с тем одними правовыми нормами достичь положительного результата невозможно. Необходимо сочетание правового запрета с морально-этическими мерами, которые призваны формировать в обществе профессиональное морально-нравственное сознание пользователей ЭВМ, систем ЭВМ и их сетей на базе общечеловеческих ценностей. Этические нормы и принципы могут оказать положительное влияние на информационную культуру общества в целом и на снижение уровня компьютерных преступлений в частности.

Не случайно в разработанных Организацией экономического сотрудничества и развития руководящих принципах безопасности информационных систем назван *принцип этики общения пользователей информационных технологий,* который предполагает уважение прав и

законных интересов всех субъектов, занятых в использовании и развитии информационных технологий. Морально-этические нормы не носят обязательного характера, но со временем смогут заменить законопослушным пользователям отдельные правовые предписания. Сегодня формирование таких этических принципов в информационной среде может не только существенно отразиться на состоянии компьютерной преступности, но и положительным образом повлиять на информационную культуру общества в целом.

Обобщая вышеизложенное, подведем некоторые итоги:

1. Противодействовать компьютерной преступности посредством влияния на факторы, сопутствующие противоправному поведению пользователей ЭВМ, систем ЭВМ или их сети в информационной сфере, возможно совокупностью методов и средств различных отраслей права, посредством максимально полной, исчерпывающей регламентации информационных отношений как своеобразного заслона уголовно наказуемым деяниям. В зависимости от средств и методов, функционально предопределяемых характером регулируемых законом общественных отношений, противодействовать преступности можно посредством установления правового контроля, который подразделяется на два вида: позитивный и репрессивный.

2. Правовой контроль над компьютерной преступностью, слагающийся из правовых средств репрессивного и позитивного характера, требует также и должной системы организационных, социальных, экономических мер. В условиях широкого использования информационных технологий контрольная функция государства приобретает все более существенное значение, поскольку государство поступательно накапливает огромные электронные данные о гражданах и организациях, доступ к которым (или их уничтожение) может повлечь самые серьезные последствия. Поэтому действенность правового контроля над компьютерной преступностью зависит от создания соответствующей системы безопасности как

совокупности правовых, организационно-технических и иных мер, направленных на обеспечение санкционированного применения средств электронно-вычислительной техники и способствующих своевременному выявлению и предотвращению наступления негативных последствий в случаях несанкционированного вторжения в компьютеры, компьютерные системы или их сети.

3.2. Проблемы предупреждения компьютерной преступности

Проведенный анализ специальной и научной литературы показывает, что вопросам уголовно-правовой защиты компьютерной информации и противодействия компьютерным преступлениям в Российской Федерации уделяется пристальное внимание как со стороны государства, так и со стороны научного сообщества[32].

Целью предупреждения компьютерной преступности выступает обеспечение в Российской Федерации необходимых условий для безопасного создания, обработки и распространения компьютерной информации, а также нормального функционирования компьютерных устройств и информационно-телекоммуникационных сетей.

К основным задачам предупреждения данного вида преступности относится выработка и реализация комплекса мер, направленных на предотвращение:

– преступных посягательств на основы конституционного строя, общественную безопасность и общественный порядок в РФ;

– угроз информационной безопасности личности, общества, государства, т.е. обеспечение возможности безопасного создания, хранения,

[32] Ефремова, М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий / М.А. Ефремова. – М. : Юрлитинформ, 2015. – 200 с.

обработки и передачи вышеуказанными субъектами права не запрещенной законом компьютерной информации;

– несанкционированных действий, направленных на уничтожение, блокирование, модификацию, копирование компьютерной информации или нейтрализацию средств защиты компьютерной информации физических и юридических лиц, либо угрозы причинения указанных последствий;

– противоправных действий, направленных на нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям;

– угроз информационной безопасности коммерческих и некоммерческих организаций, органов власти, предприятий и учреждений, связанных с обеспечением режима тайны конфиденциальной информации (персональных данных и информации частного характера, сведений, представляющих государственную, служебную, профессиональную, коммерческую и иную тайну);

– несанкционированных действий, направленных на нарушение работы средств защиты, хранения, обработки и передачи компьютерной информации на военных, стратегических и социально значимых объектах (транспортных, промышленных, энергетических, научных, здравоохранительных, образовательных и т.д.);

– нарушения конституционных прав граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом, неприкосновенность частной жизни, личной и семейной тайны, собственности и др.[33].

[33] Евдокимов, К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации / К.Н. Евдокимов // Академический юридический журнал. – 2015. – № 1 (59). – С. 25-26

Содержание указанных задач позволит определить круг мер общего и специального характера, направленных на предупреждение компьютерных преступлений.

Анализ научной литературы позволяет выделить следующие подходы к освещению данной проблематики. Так, В.Б. Вехов и В.Е. Козлов в своих работах указывают три основные группы мер предупреждения компьютерных преступлений, а именно правовые, организационно-технические и криминалистические[34].

Близкой точки зрения придерживается Е.А. Маслакова, по мнению которой можно выделить три группы мер предупреждения указанных преступных деяний, составляющих в своей совокупности целостную систему борьбы с этим социально опасным явлением, а именно правовые, организационные и технические[35].

Можно согласиться с точкой зрения, согласно которой система профилактических мер, направленных на предупреждение компьютерных преступлений, должна носить комплексный и многосторонний характер. Между тем, учитывая методологический подход криминологической науки, выделяются меры предупреждения (например, политические, экономические, социальные, научно-технические, духовно-культурные) и специальные предупредительные меры (правовые, духовно-культурные, организационно-управленческие, технические, криминалистические и др.).

Меры предупреждения компьютерных преступлений носят всеобщий характер и направлены на профилактику как компьютерной преступности в частности, так и преступности в целом. Они сформулированы в указе

[34] Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / В.Б. Вехов ; под ред. Б.П. Смагоринского. – М. : Право и Закон, 1996. – 182 с.

[35] Маслакова, Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. ... канд. юрид. наук / Е.А. Маслакова. – Орел : РГБ, 2008. – 198 с.

Президента РФ «О Стратегии национальной безопасности Российской Федерации до 2020 года» от 12 мая 2009 г. № 537[36].

Общеэкономические предупредительные меры включают: повышение конкурентоспособности национальной экономики; экономический рост, который достигается прежде всего путем развития национальной инновационной системы и увеличения инвестиций в человеческий капитал; повышение производительности труда и др.

Общие социальные меры предполагают: снижение уровня социального и имущественного неравенства населения, стабилизацию его численности в среднесрочной перспективе, а в долгосрочной перспективе – коренное улучшение демографической ситуации; обеспечение личной безопасности, а также доступности комфортного жилья, высококачественных и безопасных товаров и услуг, достойной оплаты активной трудовой деятельности и т.д.

К научно-техническим предупредительным мерам относятся: формирование системы целевых фундаментальных и прикладных исследований и ее государственной поддержки в интересах организационно-научного обеспечения достижения стратегических национальных приоритетов; создание сети федеральных университетов, национальных исследовательских университетов, обеспечивающих в рамках кооперационных связей подготовку специалистов для работы в сфере науки и образования, разработки конкурентоспособных технологий и образцов наукоемкой продукции, организации наукоемкого производства и др.

Духовно-культурные меры предупреждения включают: признание первостепенной роли культуры для возрождения и сохранения культурно-нравственных ценностей, укрепления духовного единства многонационального народа Российской Федерации и международного имиджа России в качестве страны с богатейшей традиционной и динамично

[36] Стратегия национальной безопасности Российской Федерации до 2020 года : указ Президента РФ от 12 мая 2009 г. № 537 // Российская газета.□– 2009.□– 19 мая

развивающейся современной культурой, создание системы духовного и патриотического воспитания граждан России.

К специальным правовым мерам предупреждения компьютерных преступлений можно отнести следующие:

1. Совершенствование действующего уголовного законодательства. Например, необходимо законодательное закрепление ряда юридических понятий, содержащихся в диспозициях ст. 272-274 УК РФ, а именно: «компьютерная программа», «несанкционированное уничтожение, блокирование, модификация, копирование компьютерной информации», «нейтрализация средств защиты компьютерной информации», «средства хранения, обработки или передачи охраняемой компьютерной информации», поскольку указанные юридические термины законодательно нигде не определены, а разъяснения Пленума Верховного Суда РФ на данный счет отсутствуют.

Следует дополнить гл. 28 УК РФ новыми составами преступлений, например, ст. 272.1 «Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации». Данная позиция обусловлена тем, что преступник тайно, открыто или обманным путем завладев, например, флэш-картой или DVD-диском с компьютерной информацией для последующего ее использования, избегает уголовной ответственности по ст. 158, 159, 161 УК РФ в связи с малозначительностью совершенного деяния, так как стоимость вышеуказанных носителей информации не превышает 1 тыс. р. При этом виновное лицо получает доступ к компьютерной информации, которая представляет для ее владельца бóльшую ценность, чем сам материальный носитель информации, тем самым потерпевшему причиняется более существенный вред.

Кроме того, представляется целесообразным введение уголовной ответственности за создание, использование и распространение «ботнетов», т.е. сети компьютеров или компьютерных устройств, зараженных

вредоносной программой, позволяющей удаленно управлять инфицированными машинами без ведома их владельца (пользователя), использовать ресурсы зараженных компьютерных средств в преступных целях (рассылки спама, анонимного доступа в Интернет, совершения Ddos-атак, фишинга, кибершантажа, компьютерного мошенничества, сбыта наркотических средств, распространения детской порнографии и иных преступных деяний, а также сокрытия следов преступной деятельности).

Кроме того, для более эффективного противодействия преступлениям в сфере компьютерной информации ряд авторов предлагают дополнить диспозиции ч. 3 ст. 272, ч. 2 ст. 273, ч. 1 ст. 274 УК РФ новыми квалифицирующими признаками:

1. «Те же деяния, совершенные с целью скрыть другое преступление или облегчить его совершение».

2. «Те же деяния, совершенные с целью устрашения населения или воздействия на принятие решения органами государственной власти и (или) местного самоуправления, а также воспрепятствования нормальной деятельности средств массовой информации, органов государственной власти и местного самоуправления, государственных и муниципальных учреждений, предприятий»[37].

Данная позиция обусловлена тем, что преступления в сфере компьютерной информации часто выступают или могут стать способом совершения множества других тяжких и особо тяжких преступных деяний (убийства, причинения тяжкого вреда здоровью, умышленного уничтожения или повреждения имущества, вымогательства, шпионажа, государственной измены и т.д.).

2. Совершенствование судебной практики по уголовным делам о компьютерных преступлениях в Российской Федерации. До сих пор

[37] Малыковцев, М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дис. ... канд. юрид. наук / М.М. Малыковцев. – М., 2007. – 186 с.

отсутствуют разъяснения Пленума Верховного Суда РФ о практике рассмотрения судами уголовных дел по преступлениям в сфере компьютерной информации, что негативно сказывается на следственно-судебной практике и единообразии применения уголовно-правовых норм правоохранительными органами.

Кроме того, в подавляющем большинстве случаев суды при вынесении обвинительных приговоров назначают компьютерным преступникам наказания, не связанные с лишением свободы (штраф, условное наказание, ограничение свободы и др.), обосновывая свое решение тем, что данные преступления относятся к деяниям небольшой и средней тяжести.

Например, 25 мая 2016 г. Миасский городской суд Челябинской области рассмотрел уголовное дело по обвинению Ш. в совершении преступления, предусмотренного ч. 2 ст. 273 УК РФ, создание, распространение или использование компьютерных программ, заведомо предназначенных для несанкционированного блокирования, модификации, копирования компьютерной информации, совершенные из корыстной заинтересованности.

В ходе судебного рассмотрения дела было установлено, что Ш. используя ноутбук, в целях реализации преступного умысла, направленного на создание, использование и распространение в сети Интернет компьютерной программы, предназначенной для несанкционированного блокирования, копирования и модификации компьютерной информации пользователей сети Интернет, создал файл, являющийся компьютерной программой, работающей на мобильных устройствах, предназначенный для манипулирования СМС-сообщениями, без ведома пользователя зараженного устройства, в том числе СМС-сообщениям, поступающим по системе «Мобильный банк» с целью дальнейшего хищения денежных средств с банковских карт. Ш. разместил в сети Интернет созданную компьютерную программу. К., не знавшая и не предполагавшая о преступных намерениях Ш., загрузила на свой сотовый телефон файл, размещенный Ш. Ш. получил

доступ по удаленному управлению сотовым телефоном К., а именно возможность манипулировать СМС-сообщениями, сформировал команду с текстовым приложением, проверив баланс банковской карты К., получил ответ, что на банковской карте, имеются денежные средства. Ш. реализуя свой преступный умысел, сформировал без ведома владельца команду об отправке денежных средств, таким образом Ш., незаконно осуществил перевод денежных средств на лицевой счет, тем самым получил возможность распоряжаться денежными средствами по своему усмотрению. Ш., продолжал реализовывать свой преступный умысел неоднократно.

Действия Ш. подлежат квалификации по ч.2 ст. 273 УК РФ, как создание, распространение или использование компьютерных программ, заведомо предназначенных для несанкционированного блокирования, модификации, копирования компьютерной информации, совершенные из корыстной заинтересованности.

При назначении наказания Ш. суд учитывает, что им совершено оконченное умышленное преступление, отнесенное к категории средней тяжести в сфере компьютерной информации.

Суд приговорил Ш. признать виновным в совершении преступления, предусмотренного ч.2 ст.273 УК РФ, и назначить ему наказание в виде лишения свободы сроком на один год со штрафом в размере ста пятидесяти тысяч рублей, без лишения права занимать определенные должности или заниматься определенной деятельностью.

В соответствии со ст. 73 УК РФ назначенное Ш. наказание в виде лишения свободы считать условным, установив ему испытательный срок, продолжительностью в два года, в течение которого обязать осужденного не менять места жительства и места работы без уведомления специализированного государственного органа, осуществляющего контроль за поведением условно-осужденных, являться на регистрацию в данный орган. На основании п.9 Постановления Государственной думы «Об объявлении амнистии в связи с 70-летием Победы в Великой Отечественной

войне 1941-1945 годов» Ш. от назначенного наказания освободить. Меру пресечения в виде подписки о невыезде и надлежащем поведении отменить.

21 января 2016 г. Миасский городской суд Челябинской области рассмотрел уголовное дело по обвинению П. в совершении преступления, предусмотренного ч. 2 ст. 273 УК РФ.

В ходе судебного рассмотрения дела было установлено, что П. совершил неправомерный доступ к охраняемой законом компьютерной информации, принадлежащей Ф., с использованием своего служебного положения, при следующих обстоятельствах.

В соответствии с условиями трудового договора, П. был назначен на должность заместителя начальника отдела персонифицированного учета. П., занимая указанную должность, имел доступ к компьютерной информации о состоянии индивидуального лицевого счета застрахованного лица, которая является конфиденциальной.

У П. возник умысел и затем реализовал его, направленный на неправомерный доступ к охраняемой законом компьютерной информации, о состоянии индивидуального лицевого счета застрахованного лица, с целью ее копирования, из личной заинтересованности, выраженной в желании передать ее третьему лицу.

Обвинение, с которым согласен подсудимый, обоснованно, подтверждено собранными по делу доказательствами. Действия П. подлежат квалификации по ч.3 ст. 272 УК РФ – неправомерный доступ к компьютерной информации путем её копирования, с использованием своего служебного положения. При назначении наказания П. суд учитывает, что им совершено оконченное преступление средней тяжести в сфере компьютерной информации, общественную опасность содеянного, оснований для снижения категории тяжести преступления не имеется.

Не вызывает сомнений, что неправомерный доступ к персональным данным гражданского истца причинил ему нравственные страдания; изложенное, в соответствии со ст.1064 ГК РФ влечет обязанность виновного

лица – П. компенсировать причиненный моральный вред. Размер компенсации и ее форму суд определяет с учетом требований ст.1101, 151 ГК РФ, учитывая характер нравственных страданий потерпевшего, степень вины ответчика, его материальное и семейное положение, иные обстоятельства дела. Учитывая все изложенное, суд приходит к выводу о том, что причиненный моральный вред сможет компенсировать сумма в 10 000 рублей.

Суд приговорил признать П. виновным в совершении преступления, предусмотренного ст. 272 ч.3 УК РФ, и назначить ему наказание в виде штрафа. На основании п.9 Постановления Государственной думы «Об объявлении амнистии в связи с 70-летием Победы в Великой Отечественной войне 1941-1945 годов» П. от назначенного наказания освободить. Меру пресечения П. отменить. Взыскать с П. в пользу Ф. компенсацию морального вреда, причиненного преступлением в размере 10 000 (десяти тысяч) рублей. В удовлетворении оставшейся части исковых требований Ф. отказать.

Недостаточная жесткость наказания, назначаемого лицам, безусловно, будет способствовать рецидиву со стороны данной категории преступников.

Кроме того, совершенствование судебной практики требует разъяснений Пленума Верховного Суда РФ по вопросам квалификации деяний, предусмотренных главой 28 УК РФ.

3. Активизация и совершенствование международно-правового сотрудничества в сфере предупреждения компьютерных преступлений и борьбы с ними. Учитывая транснациональный и трансграничный характер рассматриваемых преступлений, большое значение приобретает вопрос взаимодействия правоохранительных органов России и зарубежных стран в сфере противодействия компьютерной преступности.

В 2014 г. Псковским городским судом Псковской области за совершение преступлений, предусмотренных ч. 3 ст. 183, ч. 3 ст. 272, ч. 2 ст. 273 УК РФ, был осужден Б., гражданин Республики Молдова. Приговором суда ему назначено наказание в виде 11 месяцев лишения свободы в

колонии-поселении со штрафом в размере 100 тыс. р. без лишения права занимать определенные должности или заниматься определенной деятельностью. Однако остальные три члена преступной группы, граждане Республики Молдова, занимавшиеся скиммингом в Пскове, скрылись от следствия и суда, предположительно на территории Молдовы или Румынии[38].

Между тем Россия до сих пор не ратифицировала Конвенцию Совета Европы о киберпреступности, участниками которой являются 47 государств[39]. Официальная причина – отсутствие в УК РФ правовой нормы, предусматривающей уголовную ответственность юридических лиц за преступления в сфере компьютерной информации.

Данное обстоятельство, несомненно, препятствует эффективной борьбе с международными преступными группами, совершающими компьютерные преступления на территории Российской Федерации, и полноценному международному сотрудничеству в сфере информационной безопасности.

4. Совершенствование информационного законодательства РФ. Полагается возможным принятие федерального закона о страховании информационных рисков, который бы закреплял страхование компьютерной информации, а также средств ее хранения, обработки и передачи, информационно-телекоммуникационных сетей и оконечного оборудования от несанкционированного уничтожения, блокирования, модификации либо копирования.

При этом перед заключением страхового договора следует обязать собственника (владельца) компьютерной информации или средств хранения, обработки, передачи охраняемой компьютерной информации, информационно-телекоммуникационных сетей и оконечного оборудования

[38] Уголовное дело № 1-382/2014 // Архив Псковского городского суда Псковской области. – 2014

[39] Конвенция о преступности в сфере компьютерной информации (ETS N 185) : (заключена в г. Будапеште 23 нояб. 2001 г.) // Собрание законодательства Российской Федерации.□– 2005.□– № 47.□– Ст. 4929

установить необходимое программное обеспечение по антивирусной защите компьютерной информации и фиксации (предупреждении) несанкционированного доступа. Эта мера позволит уменьшить наносимый материальный ущерб и снизить количество несанкционированных проникновений в компьютерные системы, происходящих по вине потерпевших. Данную меру из 150 проанкетированных сотрудников ОВД Иркутской области поддержали 86,7 % опрошенных[40].

Кроме того, по мнению авторов, следует законодательно закрепить полномочия правоохранительных органов (Прокуратуры РФ, СК РФ, МВД РФ, ФСБ РФ и др.) по контролю появляющихся в информационно-телекоммуникационных сетях материалов противоправного характера, а в необходимых случаях разрешить им проводить соответствующие надзорные, оперативно-розыскные, следственные мероприятия.

Полагается необходимым для предупреждения совершения компьютерных преступлений в сети Интернет в Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ закрепить юридическую обязанность пользователей информационно-телекоммуникационных сетей, в том числе сети Интернет, при регистрации сайтов, веб-страниц, получении аккаунтов в социальных сетях указывать свои персональные данные (Ф.И.О., год рождения, данные паспорта)[41].

Опыт Китайской Народной Республики, где официальная персонализация интернет-пользователей была введена в 2010 г., показал, что данная мера значительно снизила количество компьютерных преступлений, совершенных в сети Интернет.

---

[40] Евдокимов К.Н. Проблемы квалификации и предупреждения компьютерных преступлений / К.Н. Евдокимов.□– Иркутск : Иркут. юрид. ин-т (филиал) Акад. Генер. прокуратуры РФ, 2009.□– 171 с

[41] Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации / К.Н. Евдокимов // Академический юридический журнал.□– 2015.□– № 1 (59).□– С. 25-26

В качестве специальных духовно-культурных (идеологических) мер противодействия компьютерным преступлениям предлагается:

1. Активизировать деятельность средств массовой информации по предупреждению компьютерных преступлений. Например, можно возложить обязанность на специализированные средства массовой информации доводить до читателей (зрителей) информацию о привлечении компьютерных преступников к уголовной ответственности с разъяснением правовых положений действующего законодательства, предусматривающего наказание за преступления в сфере компьютерной информации. Данный шаг, несомненно, положительно скажется на профилактике компьютерной преступности.

2. Обратить внимание на правовое воспитание молодежи. По мнению авторов, проводя правовую пропаганду и правовое просвещение среди учащихся и студентов технических образовательных учреждений – будущих программистов, сетевых администраторов и специалистов в области защиты информации, информируя их о действующем уголовном законодательстве и ответственности за указанные противоправные деяния, можно снизить риск появления компьютерных преступников в среде технических специалистов, поскольку, как показывает практика, достаточно большое количество хакеров появляется в молодежной среде технического «андеграунда».

В качестве аргумента в поддержку эффективности этой меры можно привести воспоминания Е.В. Касперского, который писал: «Однажды, где-то в конце 1990-х годов, нам удалось узнать домашний адрес одного вирусописателя из Москвы, весьма активного в то время. На этот адрес была отправлена посылка с книгой о компьютерных вирусах и ксерокопией «компьютерных» статей из Уголовного кодекса РФ. Через несколько дней в

Сети появилось его письмо, в котором он сообщил, что прекращает разрабатывать новые компьютерные вирусы»[42].

К специальным организационно-управленческим и техническим мерам предупреждения компьютерных преступлений можно отнести следующее:

1. Требуется тесное взаимодействие органов прокуратуры, органов внутренних дел (отделов «К»), органов Федеральной службы безопасности со средствами массовой информации при предупреждении и раскрытии преступлений в сфере компьютерной информации. Анализ правоприменительной практики показывает эффективность такого взаимодействия, тем более что основные формы сотрудничества правоохранительных органов и средств массовой информации давно уже апробированы и активно используются.

2. Создание в Российской Федерации национальной операционной системы для компьютерных устройств, а также общенациональной компьютерной системы фиксации, анализа и учета преступлений в сфере компьютерной информации и компьютерных преступников.

К криминалистическим мерам предупреждения преступлений в сфере компьютерной информации можно отнести:

1. Создание новых и совершенствование существующих методик выявления компьютерных преступлений с привлечением специалистов в области информационной безопасности.

2. Обобщение и анализ юридической практики Прокуратурой РФ, СК РФ, МВД РФ, ФСБ РФ, МО РФ для дальнейшей выработки методических рекомендаций по вопросам раскрытия и расследования компьютерных преступлений[43].

---

[42] Касперский, Е.В. Компьютерное зловредство / Е.В. Касперский. – СПб.: Питер, 2009. – 208 с

[43] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс]: – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_161817. – Загл. с экрана.

3. Создание во всех экспертно-криминалистических центрах МВД, ГУ МВД, ОВД отделов компьютерных экспертиз и технологий для производства необходимых судебно-компьютерных экспертиз, выдачи заключений и справок заинтересованным лицам.

4. Совершенствование подготовки экспертов-криминалистов, осуществляющих судебно-компьютерные экспертизы, на базе единого учебного центра.

В данное время системная подготовка экспертов-криминалистов и повышение их квалификации при проведении судебно-компьютерных экспертиз в системе МВД России не осуществляется, поэтому возникает необходимость создания единого учебного центра на базе МВД РФ либо одного из образовательных учреждений МВД России, имеющих необходимый опыт обучения экспертов-криминалистов.

Перечень мер по предупреждению компьютерной преступности может быть продолжен. Однако, вне всякого сомнения, только интегративный и комплексный подходы в применении правоохранительными органами профилактических мер могут повысить уровень информационной безопасности России и сделать предупреждение компьютерных преступлений более эффективным. При этом не стоит забывать, что предложенные предупредительные меры дадут ощутимый результат только в случае совместных действий государства с институтами гражданского общества.

Обобщая вышеизложенное, подведем некоторые итоги:

Выделены общеэкономические, научно-технические, социальные, духовно-культурные предупредительные меры предупреждения компьютерных преступлений.

К специальным правовым мерам предупреждения компьютерных преступлений можно отнести следующие: совершенствование действующего уголовного законодательства, совершенствование судебной практики по уголовным делам о компьютерных преступлениях в Российской Федерации,

активизация и совершенствование международно-правового сотрудничества в сфере предупреждения компьютерных преступлений и борьбы с ними, совершенствование информационного законодательства РФ

В качестве специальных духовно-культурных (идеологических) мер противодействия компьютерным преступлениям предлагается: активизировать деятельность средств массовой информации по предупреждению компьютерных преступлений, обратить внимание на правовое воспитание молодежи.

К специальным организационно-управленческим и техническим мерам предупреждения компьютерных преступлений можно отнести следующее: тесное взаимодействие органов прокуратуры, органов внутренних дел (отделов «К»), органов Федеральной службы безопасности со средствами массовой информации при предупреждении и раскрытии преступлений в сфере компьютерной информации, создание национальной операционной системы для компьютерных устройств.

К криминалистическим мерам предупреждения преступлений в сфере компьютерной информации можно отнести: создание новых и совершенствование существующих методик выявления компьютерных преступлений с привлечением специалистов в области информационной безопасности, обобщение и анализ юридической практики для дальнейшей выработки методических рекомендаций по вопросам раскрытия и расследования компьютерных преступлений, создание во всех экспертно-криминалистических центрах отделов компьютерных экспертиз, совершенствование подготовки экспертов-криминалистов.

3.3. Международное сотрудничество России в области противодействия компьютерной преступности

Анализ опыта международного сотрудничества в противодействии компьютерной преступности свидетельствует о том, ++что оно реализуется в двух основных общепризнанных формах:

1) на основе международных соглашений;

2) в рамках международных органов и организаций.

Первая форма международного сотрудничества осуществляется по следующим направлениям:

1. *Защита прав личности в информационной сфере.* Национальные законодательства государств мирового сообщества исходят из ст. 19 Всеобщей декларации прав человека: «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любым способом и независимо от государственных границ».

2. *Защита национальных государственных интересов.* Проблема решается с помощью определения национальных приоритетов защиты, определения исполнительных механизмов, в рамках которых правовое обеспечение защиты информации ограниченного доступа имеет большое значение. При этом в мировой практике все отчетливее явствует тенденция к уменьшению количества государственных секретов и увеличению «прозрачности» деятельности государств в лице их соответствующих органов. В этих целях периодически публикуются специальные отчеты о количестве рассекреченных и засекреченных документов, количестве официальных лиц, уполномоченных засекречивать и рассекречивать государственную информацию, стоимости обеспечения данных мероприятий.

3. *Защита частной предпринимательской и финансовой деятельности.* К этому направлению относятся законодательные акты, определяющие условия «добросовестной» конкуренции, формирующие антимонопольное законодательство, предусматривающие правовые механизмы защиты авторских прав. Общим в законотворчестве различных стран в вопросе о защите информации от преступных посягательств является законодательное определение и закрепление государственной политики в области информатизации и компьютеризации; установление уголовной ответственности за нарушение порядка обработки и несанкционированное использование охраняемой законом компьютерной информации; применение жестких мер наказания за преступления в сфере компьютерной информации, представляющие опасность не только для граждан, но и для всего общества, государства, а в отдельных случаях и для мирового сообщества.

4. *Определение юрисдикции компьютерных правонарушений.* Как правило, деяние совершается в стране пребывания правонарушителя, но объект посягательства может находиться в другом государстве. Возможна иная ситуация, когда правонарушитель, находясь и в одной стране, осуществляет неправомерный доступ к данным компьютерной системы в другом государстве, а результат получает в третьем государстве (путем передачи фальсифицированных данных по компьютерной сети). В рассмотренных вариациях правом отправления правосудия на основании территориальной юрисдикции обладают как минимум три государства, если исключить страны, телекоммуникационные сети которых были использованы при передаче фальсифицированных данных. Возникают вопросы, связанные с юрисдикцией дел о компьютерных правонарушениях и применением правовых санкций на основе территориальной юрисдикции или принципа экстерриториальности. Помимо коллизии возникает вопрос о необходимости арбитражного разбирательства равных претензий на юрисдикцию.

В процессе взаимодействия государства руководствуются такими принципами международного права, как принципы невмешательства, территориальной целостности и суверенного равенства. Все они не исключают возможности применения экстерриториальной юрисдикции. В целях предотвращения коллизий юрисдикция над серьезными компьютерными преступлениями возможна на основе принципа универсальности и защитительного принципа, обеспечивающих право государства на защиту основополагающих интересов.

Установление приоритетов в определении территориальной и экстерриториальной юрисдикции подлежит на основе как многосторонних, так и двухсторонних соглашений, в рамках которых должны согласовываться вопросы унификации законодательств, сотрудничества в расследовании, судебном преследовании и наказании за транснациональные компьютерные правонарушения, выдачи виновных лиц (экстрадиция). Таким образом, речь идет о пределах уголовной юрисдикции государств в пространственных сферах.

5. *Расследование транснациональных компьютерных преступлений.* Расследование компьютерных преступлений требует существенного изменения традиционной следственной практики и норм материального международного уголовного права. Межгосударственные отношения в данной сфере должны предусматривать унификацию национальных уголовных законодательств, касающихся ответственности за компьютерные правонарушения, и гармонизацию уголовно-процессуальных законодательств сторон. Инструментарий международного сотрудничества в области уголовного правосудия охватывает совершение таких процессуальных действий, как исполнение судебных поручений, проведение обысков, изъятие, пересылка и выдача вещественных доказательств, проведение экспертизы, возбуждение уголовного дела, выдача лиц, совершивших правонарушение, и иных. Поэтому необходимость расширения и детализации содержания процессуальных норм,

регулирующих процедуру расследования компьютерных преступлений в рамках международных соглашений, очевидна.

При этом следует иметь в виду и такой аспект специфики расследования компьютерных преступлений, как их чрезмерная мобильность. В силу этого обстоятельства орган, осуществляющий функцию уголовного преследования, может быть поставлен в условия необходимости совершения таких действий или принятия таких решений, которые выходят за рамки его юрисдикции и не предусмотрены международными соглашениями. В противном случае процедура согласования проведения необходимых следственных мероприятий компетентным органом другого государства может отнять время, достаточное для уничтожения правонарушителем информации, имеющей доказательственное значение. Поэтому Европейской конвенцией о киберпреступности предусмотрены такие нетрадиционные виды взаимной межгосударственной помощи, как: а) совершение безотлагательного блокирования компьютерных данных и незамедлительное предъявление блокированных данных (часть 1 ст. 29); б) доступ к компьютерным данным и фиксация потока данных в режиме реального времени (ст. 30). В контексте указанных процессуальных мероприятий под потоком данных понимаются любые компьютерные данные, относящиеся к передаче связи посредством компьютерной системы; создаваемые компьютерной системой, которая образует звено в цепи коммуникации; определяющие источник связи, адрес назначения, маршрут, размер, продолжительность или тип основной линии связи или службы.

Из перечисленных наиболее актуальным и нетрадиционным видом межгосударственного сотрудничества является *трансграничный доступ к информации.* Трансграничный доступ к компьютерным данным, когда компетентный орган, осуществляющий следствие, производит осмотр или изъятие информации из компьютерной системы, расположенной на территории другого государства, является одной из дискуссионных тем. Несмотря на интенсивность использования информационной и

коммуникационной технологии, вопрос о трансграничном доступе к компьютерным данным в процессе расследования не стал предметом международных соглашений о взаимодействии. Между тем такая необходимость назрела, и обусловлена она темпами роста преступности в сфере высоких технологий. Закрепление компьютерной информации посредством рассматриваемого процессуального действия в качестве доказательства по уголовным делам предваряет новое направление международного сотрудничества в борьбе с компьютерной транснациональной преступностью.

Положительное решение вопросов, касающихся механизма реализации трансграничного доступа к компьютерным данным, должно осуществляться на основе международных соглашений. При этом договаривающиеся стороны должны как следовать фундаментальным международным принципам, так и учитывать нижеследующие специальные положения, реализация которых, безусловно, окажет позитивное влияние на эффективность расследования компьютерных преступлений:

а) применение традиционных методов, предусмотренных в рамках межгосударственной взаимной помощи, может не дать положительных результатов;

б) предоставление права на трансграничный доступ в компьютерную систему или базы данных другого государства лишь в случае совершения правонарушения, негативные последствия которого затрагивают жизненно важные сферы деятельности самого запрашиваемого государства, третьего государства или мирового сообщества;

в) общедоступность компьютерной системы или сети, в которой хранится требуемая информация;

г) предоставление компетентному органу, ведущему уголовное расследование, права на блокирование компьютерной информации только в целях сохранения последней и использования как доказательственного материала;

д) использование данных в качестве доказательства в проводимом расследовании должно быть санкционировано собственником (законным владельцем) компьютерной информации;

е) формулирование исчерпывающего перечня исключительных обстоятельств, позволяющих осуществление трансграничного доступа в компьютерную систему или базы данных другого государства без получения согласия пользователя или собственника, но с последующим обязательным уведомлением последних или компетентных органов страны, где находится компьютерная система или компьютерная база данных;

ж) информирование компетентных органов государства, в котором находится требуемая информация, о начале уголовного расследования, о судебном слушании и последующем распоряжении вещественным доказательством, коим выступала истребованная из компьютерной базы данных информация.

Рассматриваемая проблема крайне сложна как в процессуальном и международном плане, так и в уголовно-правовом, поскольку чревата злоупотреблением со стороны органа, осуществляющего следствие. Поэтому пробел Конвенции о киберпреступности в неурегулированности механизма отказа в трансграничном доступе собственником или законным пользователем, обладающим правом на управление компьютерной системой и хранящимися в ней данными, является существенным и требует определения критериев, на основании которых собственник или законный пользователь компьютерной системы или сети имеет право отказать в трансграничном доступе к информации.

6. *Решение вопросов передачи уголовного судопроизводств и вопросов экстрадиции.* Названные институты международного правового сотрудничества вносят важный вклад в обеспечение эффективности международного уголовного правосудия. «Преступность усложняется, не признает границ; организованная преступность разных стран устанавливает тесные контакты; преступники, совершившие преступление в одной стране,

получают поддержку и содействие со стороны своих «собратьев». Все это делает проблему экстрадиции весьма актуальной». О выдаче преступников говорится в конституциях России, Франции, Германии, Ирландии, Италии, Португалии, Испании. Современный каркас межгосударственных отношений в данной области представлен многими международными документами, соглашениями между членами Европейского сообщества, региональными соглашениями. Вопросы экстрадиции и передачи уголовного судопроизводства в отношении транснациональных компьютерных преступлений вполне разрешимы на основе уже сложившейся договорно-правовой практики между членами мирового сообщества. Вместе с тем, учитывая новизну правоприменительной практики в отношении компьютерных преступлений, следует согласиться с тем, что эффективность применения межгосударственных соглашений зависит и от унификации национальных уголовных законодательств.

7. *Реформирование уголовно-процессуального законодательства.* В течение трех лет (1992-1995 гг.) под эгидой Совета Европы были проведены исследования в рамках планируемой процессуальной реформы. 11 сентября 1995 года на 543-м заседании Комитета министров была принята Рекомендация № R(95)13, касающаяся проблем уголовно-процессуального законодательства в условиях информатизации общества и криминализации возможностей информационных технологий. В данном документе было сформулировано 18 директив-принципов, которые носят рекомендательный характер и которыми следует руководствоваться при реформировании национальных уголовно-процессуальных законодательств.

Таким образом, Рекомендации 1989 и 1995 гг. стали основой международной уголовно-процессуальной базы в сфере расследования компьютерных преступлений, а также отправной точкой в запуске механизма международного процессуального сотрудничества в противодействии компьютерной преступности.

8. *Выработка мер защиты компьютерной информации.* В настоящее время сфера международного сотрудничества в борьбе с криминальными проявлениями в сфере информационных технологий переместилась на более высокий научно-прикладной уровень и знаменуется представлением Советом Европы 27 апреля 2000 года Проекта конвенции о киберпреступности.

Документ является первым международным соглашением, регламентирующим уголовно-правовые и процессуальные аспекты преступлений, направленных против компьютерных систем, сетей или информации, хранящейся либо циркулирующей в их пределах.

В Конвенции предусмотрено несколько способов защиты компьютерной информации. *Первый способ* носит превентивный характер, поскольку связан с выделением таких противоправных действий, связанных с киберпреступностью, как преступления и правонарушения, ответственность за которые устанавливается государствами на национальном уровне. *Второй способ* носит уголовно-процессуальный, оперативный и организационный характер. Конвенцией предусмотрено оперативное обеспечение сохранности компьютерной информации, закрепляется право компетентных органов на обыск и выемку данных, хранимых в компьютерных системах, на компьютерных носителях, на возможность сбора в режиме реального времени данных о потоках информации, её перехват. В Конвенции регламентируются процедуры направления запросов о взаимной помощи в отсутствие применимых международных соглашений, характер неотложных мер, которые необходимо предпринять в связи с сохранностью компьютерных данных, обозначены случаи ограничения либо отказа в предоставлении информации.

9. *Формирование глобального информационного общества.* В июле 2000 года в Окинаве руководителями восьми развитых стран мира была принята Хартия глобального информационного общества, в которой устанавливаются основные принципы вхождения государств в такое

общество. В Хартии обращено внимание государств на укрепление нормативной базы для борьбы с компьютерными злоупотреблениями, которые подрывают целостность глобальных сетей и способствуют утечке информации, на защиту прав интеллектуальной собственности на информационные технологии[44]. После подписания Президентом России Окинавской Хартии глобального информационного общества была утверждена Доктрина информационной безопасности, которая наметила направления государственной политики по обеспечению практического участия России в деятельности международного сообщества и закрепила основные составляющие национальных интересов Российской Федерации в информационной сфере.

Вторая форма международного сотрудничества осуществляется в следующих направлениях:

1) содействие заключению международных договоров и соглашений по борьбе с международной преступностью;

2) выработка общих международных стандартов противодействия преступности, преследования и наказания за совершение международных преступлений, преступлений международного характера;

3) выработка рекомендаций по борьбе с общеуголовными преступлениями и консультативная помощь государствам с учетом того, что каждое государство ведет эту борьбу в пределах своей территории в соответствии с собственными социальными и экономическими условиями[45].

Противодействие ООН компьютерным преступлениям стало развиваться в начале 90-х годов, когда на двенадцатом пленарном заседании Восьмого конгресса ООН (в Гаване) был рассмотрен Проект резолюции по преступлениям, совершаемым с использованием компьютерных технологий, в подготовке которого участвовало 21 государство. По результатам

---

[44] Окинавская Хартия глобального информационного общества // Дипломатический вестник. – 2000. – № 8.

[45] Международное уголовное право: учебное пособие / под ред. В. Н. Кудрявцева. – 2-изд., перераб. и доп. – М.: Наука, 1999. – С. 193.

обсуждения Конгресс принял резолюцию с призывом ко всем участникам направить усилия на борьбу с компьютерной преступностью.

На сегодняшний день многие документы, принятые в рамках ООН, имеют прикладную значимость в нейтрализации проблемы транснациональной компьютерной преступности. Последним вкладом ООН в борьбе международного сообщества с компьютерной преступностью стала Декларация о преступности и правосудии: ответы на вызовы XXI века, принятая на Десятом конгрессе по предупреждению преступности и обращению с правонарушителями (Вена, 10-17 апреля 2000 года).

В ходе Десятого конгресса ООН был проведен семинар-практикум по компьютерным преступлениям, который, аккумулируя опыт практических работников и рекомендации ученых-теоретиков, способствовал техническому и правовому сотрудничеству государств[46]. Представленные на семинаре-практикуме материалы и рекомендации могут быть использованы для опубликования обновленного варианта Руководства ООН по предупреждению компьютерных преступлений и борьбе с ними, расширения и совершенствования борьбы с транснациональной компьютерной преступностью, принятия глобальных программ, укрепления практического сотрудничество между государствами[47].

Особое место во взаимодействии государств в борьбе с транснациональной преступностью занимает Международная организация уголовной полиции (Интерпол), основной задачей которой является обеспечение международного взаимодействия органов уголовной юстиции в борьбе с преступностью, с соблюдением национального законодательства и общепринятых прав и свобод человека. Международное сотрудничество государств – членов Интерпола осуществляется по принципу уважения

[46] Родионов К. С. Интерпол: вчера, сегодня, завтра. – М., 1990.

[47] Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century. The Tenth UN Congress on the Prevention of Crime and Treatment of Offenders: Vienna, 10-17 April 2000: PJ CONF. 187/ Rev. 3.

национального суверенитета, применения уголовного законодательства, универсальности и включает:

1) учреждение международного бюро идентификации с едиными приемами описания и системой классификации объектов уголовной регистрации;

2) проведение совместных оперативно-розыскных мероприятий в отношении международных преступников с целью их выдачи; подозреваемых лиц с намерением установления их фактического местонахождения и получением требуемой следственной информации по данному делу; пропавших без вести лиц в интересах конкретной семьи; похищенных культурных ценностей и произведений искусства;

3)создание технических служб по поддержанию на современном уровне связей с НЦБ государств – членов Интерпола с целью сбора информации (обобщение, обработка, распространение) по всему кругу вопросов борьбы с международной уголовной преступностью[48].

Международное сотрудничество в сфере противодействия компьютерной преступности является неотъемлемой составляющей политического, военного, экономического, социального, культурного взаимодействия членов мирового сообщества, включая Российскую Федерацию. Реализация вышеназванных положений позволит создать надежную основу будущей активности членов международного сообщества в противодействии транснациональной компьютерной преступности, согласованности национального законодательства и заложит фундамент для механизма нового «техногенного» международного сотрудничества.

Обобщая вышеизложенное, подведем некоторые итоги:

1. Государство в рамках общей стратегии информатизации и компьютеризации общества должно направить усилия на решение триединой задачи: формирование информационной среды общества; развитие

[48] Национальное центральное бюро Интерпола в Российской Федерации. – М., 1994. – С. 34.

информационного сервиса услуг; создание организационно-правовых основ безопасности в сфере информатизации и компьютеризации как на национальном, так и на международном уровнях. Поскольку компьютерный экстремизм, компьютерный терроризм все больше превращается из национальной проблемы отдельного государства в международную проблему человеческого выживания, постольку на международном уровне противодействие компьютерной преступности понимается как одна из главных задач уголовной политики мирового сообщества. На глобальном уровне противодействие компьютерной преступности формулируются в документах ООН как уголовно-политическая задача. На региональном в рамках Совета Европы – как деятельность с отдельными видами преступлений.

Мировой опыт межгосударственной интеграции является эмпирической базой для отечественного законодателя. А весь комплекс мероприятий, направленных на совершенствование международного сотрудничества России в рамках интеграции в единое информационное пространство, должен способствовать повышению эффективности в борьбе с компьютерной преступностью на глобальном, региональном и национальном уровнях.

2. Стратегия международного сотрудничества в противодействии компьютерной преступности может быть реализована в различных направлениях: межгосударственное сотрудничество (принципы взаимодействия, проблемы защиты информации); межгосударственные соглашения (о взаимной выдаче обвиняемых и компьютерных преступников); организация межгосударственной оперативно-розыскной деятельности (через создание транснациональных оперативно-розыскных подразделений); принятие межгосударственного регламента (к примеру, передачи материалов уголовного судопроизводства в отношении граждан, совершивших компьютерное преступление на территории чужого

государства); совершенствование интеграционных процессов в рамках межгосударственных организаций.

3. Анализ организационных проблем международного сотрудничества свидетельствует о необходимости разработки и принятия комплексных межгосударственных программ по борьбе с преступностью. Разработка такой программы применительно к компьютерным преступлениям может основываться на международной Конвенции о киберпреступности и предусматривать два уровня – международный и национальный.

На международном уровне возможно решение таких задач, как стабильный международный обмен информацией с учетом транснационального характера компьютерной преступности, оказание консультативной, организационной, финансовой и другой помощи государствам-участникам в реализации программ предупреждения компьютерной преступности, взаимодействие правоохранительных органов путем оказания правовой и оперативной помощи по уголовным делам.

На национальном уровне – оценка состояния законодательства и правоприменительной деятельности в противодействии компьютерной преступности, разработка мер по совершенствованию национального законодательства с учетом имплементации международных правовых норм, подготовка профессиональных кадров для пресечения преступных проявлений в сфере высоких технологий, вовлечение общественности и негосударственных формирований в деятельность по превенции компьютерной преступности.

4. Реализация рассмотренных в настоящем параграфе предложений обеспечит совершенствование не только конвенционного (договорно-правового) элемента, но и правового регулирования всего механизма международного сотрудничества России в вопросах противодействия компьютерной преступности. В совокупности с национальными комплексными мерами это повлечет повышение эффективности национальной уголовной политики в рассматриваемой сфере.

ЗАКЛЮЧЕНИЕ

Компьютерная преступность – это совокупность преступлений, посягающих на отношения по обработке (сбору, накоплению, хранению, поиску и распространению) компьютерной информации, а также преступлений с использованием компьютера.

В характеристике компьютерной преступности выделяются моменты:

– высокий темп роста в связи с криминальной привлекательностью компьютерных преступлений;

– компьютерные преступления всё больше приобретают международный масштаб;

– увеличение ущерба от компьютерных преступлений на фоне других видов преступлений;

– корыстные мотивы у преступников;

– прогресс в методах реализации преступлений и навыков преступников;

– несоответствие уровня национального уголовного законодательства с нормами международного права и имеющейся международной практикой;

– виктимность пользователей компьютеров;

– высокий уровень нераскрытой преступности.

Выделяются шесть причин латентности компьютерной преступности: невыявленностъ, неустановленностъ, неучтенность компетентными органами, непривлечение виновных лиц к уголовной ответственности, нераскрытие и неполнота раскрытия следственными органами.

Уровень компьютерной преступности определяется следующими факторами:

– степень компьютеризации общества;

– развитие информационных систем, сети Интернет;

– уровень законодательства в сфере компьютерной информации;

– личными характеристиками компьютерных преступников.

Имеющаяся совокупность профилактических мер не достаточна эффективна, судя по динамики компьютерных преступлений. Наблюдается рост как количества преступлений, так и материального ущерба. Существует необходимость комплексного подхода к предупредительной деятельности в отношении преступлений в сфере компьютерной информации.

Меры борьбы с компьютерными преступлениями должны быть:

– учитывать виктимное поведение пользователей;

– выражены не только правовыми, но и социальными нормами;

– учитывать дальнейшее развитие международного сотрудничества в сфере противодействия компьютерным преступлениям.

Выработка предупредительных мер должна затрагивать такие факторы, как уровень экономики, политическая стабильность, уровень разрешения социальных проблем, вектор уголовной политики государства, состояние правового регулирования.

Правовой аспект выражается в совершенствовании и гармонизации законодательства с применением международных норм; закреплении в нормативно-правовых актах терминов, используемых в главе 28 УК РФ.

В качестве законодательных инициатив предлагается: Часть 1 ст. 273 УК изложить в следующей редакции: «Создание программ для ЭВМ или внесение изменений в существующие программы *с целью* несанкционированного уничтожения, блокирования, модификации либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами».

Часть 2 ст. 273 УК сформулировать следующим образом: «То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо повлекшее по неосторожности *причинение существенного вреда или иных* тяжких последствий».

Дополнить ст. 242.1 УК РФ частью третьей следующего содержания: «Производство детской порнографической продукции с целью распространения через ЭВМ, систему ЭВМ или их сеть, предложение или предоставление в пользование, распространение либо приобретение детской порнографии через компьютерную систему для себя или для другого лица, – наказывается лишением свободы на срок от восьми до десяти лет».

Дополнить ст. 20 УК:

«...создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК)».

Анализ организационных проблем международного сотрудничества свидетельствует о необходимости разработки и принятия соответствующей комплексной межгосударственной программы, которая может основываться на международной Конвенции о киберпреступности и в структурном отношении предусматривать два блока: международный и национальный.

В качестве практических рекомендаций предлагается:

- законодательное урегулирование соотношения понятий доступ к информации и её доступность в соответствующем Федеральном Законе «О доступе к информации», который позволит закрепить механизм реализации прав пользователей на доступ к компьютерной информации;

- принятие Пленумом Верховного Суда Российской Федерации постановления по вопросам квалификации преступных деяний в сфере компьютерной информации, дифференциации ответственности за их совершение, формулирования определений терминов, вызывающих споры в науке и практике расследования данного вида преступлений.

- принятие системообразующего правового акта или долговременной криминологической программы, включенной в систему государственного комплексного программирования и планирования, в качестве основы для выработки комплексной системы мер противодействия компьютерной преступности отдельными субъектами такой деятельности;

В качестве общего вывода о компьютерных преступлениях можно сказать, что высокая техническая подготовленность преступников – их основная черта, высокий уровень латентности – стимул для реализации преступной направленности, внутренняя предрасположенность пользователей ЭВМ, систем ЭВМ или их сети – общее условие вступления на преступный путь, социально-экономическая ситуация в стране – общий фон окончательного выбора.

I. НОРМАТИВНЫЙ МАТЕРИАЛ. ОФИЦИАЛЬНЫЕ ДОКУМЕНТЫ (ИЛИ НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ)

1. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс] – Режим доступа: http://base.garant.ru/4089723/□- Загл. с экрана.

2. Собрание законодательства Российской Федерации.□- 2013.□- № 3.□- Ст. 178.

3. Модельный Уголовный кодекс [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/901781490 – Загл. с экрана.

4. Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями: Сборник документов. М., 2001. С. 346-350.

5. Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене» [Электронный ресурс]. – Режим доступа: http://base.garant.ru/135401/. - Загл. с экрана.

6. Стратегия национальной безопасности Российской Федерации до 2020 года : указ Президента РФ от 12 мая 2009 г. № 537 // Российская газета.□– 2009.□– 19 мая.

7. Конвенция о преступности в сфере компьютерной информации (ETS N 185) : (заключена в г. Будапеште 23 нояб. 2001 г.) // Собрание законодательства Российской Федерации.□– 2005.□– № 47.□– Ст. 4929.

8. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс]: – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_161817. – Загл. с экрана.

II. КНИГИ, МОНОГРАФИИ, УЧЕБНИКИ, УЧЕБНЫЕ ПОСОБИЯ

9. Вехов, В. Б. Компьютерные преступления: учебное пособие / В.Б. Вехов. – М.: Финансы и статистика, 1996 – 247 с.

10. Черкасов, В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий / В.Н. Черкасов. – Саратов, 1995. – С. 80-81.

11. Курс криминалистики. Р.С. Белкин – М.: Юрист, 1997. – Т. 3. 315 с.

12. Горбатов, В. С. Мировая практика криминализации компьютерных правонарушений / О. Ю. Полянская, В.С. Горбатов. – М., 1998. – С. 31.

13. Ожегов, С. И. Толковый словарь русского языка / С. И. Ожегов, Н. Ю. Шведова. – М., 1996. – 334 с.

14. Криминология: учебник для юридических вузов / под ред. В.Н. Бурлакова, В.П. Сальникова, С.В. Степашина. – СПб.: Санкт-Петербургский университет МВД России, 1999. – 165 с.

15. Криминология: учебник / под ред. А.И. Долговой. – 4-е изд., перераб. и доп. – М.: Норма : ИНФРА-М, 2013. – 1008 с.

16. Вехов, В.Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов - М. : Право и закон, 1996. - 182 с.

17. Козлов, В.Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов - М., 2002. С. 127-129.

18. Криминология: учебник для вузов / под ред. Н. В. Кузнецова, В. В. Лунеева. – М.: Волтерс Клувер, 2004. – С. 116-118.

19. Антонян, Ю.М. Почему люди совершают преступления. Причины преступности / Ю.М. Антонян. – М., 2005. - 57 с.

20. Криминология / под ред. В. К. Звирбуля, Н. Ф. Кузнецовой, Г. М. Миньковского. – М., 1979. – С. 118-201.

21. Кузнецова, Н.Ф. Проблемы криминологической детерминации / Н.Ф. Кузнецова – М., 1984. – С. 54 – 55.

22. Сахаров, А. Б. Социальные условия и преступность (постановка исследовательской проблемы) // Методологические вопросы изучения социальных условий преступности: Сборник научных трудов / под ред. В. К. Звирбуля. – М, 1979. – С. 6-7.

23. Кудрявцев, В.Н. Причинность в криминологии / В.Н. Кудрявцев. – М., 1987. – 106 с.

24. Антонян, Ю. М. Социальная среда и формирование личности преступника / Ю.М. Антонян. – М., 1975. – 351 с.

25. Социальная политика: учебник / под ред. Н. А. Волгина. – М.: Экзамен, 2002. – С. 150-156.

26. Криминология: учебник / под ред. В. Н. Кудрявцева, В. Е. Эминова. – М.: Юристь, 2000. – С. 74.

27. Банковский бизнес в России: криминологические и уголовно-правовые проблемы / Н.Я. Заблоцис и др. – М., 1994. – С. 56.

28. Информатизация и информационная безопасность правоохранительных органов. – М.: Академия управления МВД России, 2003. – С. 347-348.

29. Кобелев, О.А. Электронная коммерция / О. А. Кобелев, В. И. Скиба. – М., 2003. – С. 12.

30. Уголовное право Республики Казахстан. Особенная часть: учебник / под ред. И. Ш. Борчашвили и С. М. Рахметова: В 2-х ч. Часть 2. – Алматы: Институт Данекер, 2000. – С. 93.

31. Криминология / под ред. Н. Ф. Кузнецовой. – М.: Зерцало, ТЕИС, 1996. – С. 44.

32. Старостина, Е.В. Защита от компьютерных преступлений и кибертерроризма / Е.В. Старостина, Д.Б. Фролов. – М.: Изд-во Эксмо, 2005. – С.29.

33. Scbwartau W. Information Warfare: Chaos on the Electronic Superhighway. – NY, 1994. – P.215-248.

34. Осипенко, А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт / А.Л. Осипенко. – М.: Норма, 2004. – С. 152

35. Ривман, Д.В. Криминальная виктимология / Д.В. Ривман. – СПб.: Питер, 2002. – С. 10.

36. Криминология: преступность как свойство общества. Краткий курс. – СПб: ЛАНЬ, 2001.

37. Ефремова, М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий / М.А. Ефремова.□– М. : Юрлитинформ, 2015.□– 200 с.

38. Криминология. учебник для юридических вузов / под ред. А. И. Долговой. – М., 1997.

39. Вехов, В.Б. Компьютерные преступления: Способы совершения и раскрытия / В.Б. Вехов ; под ред. Б.П. Смагоринского.□– М. : Право и Закон, 1996.□– 182 с.

40. Евдокимов, К.Н. Проблемы квалификации и предупреждения компьютерных преступлений / К.Н. Евдокимов.□– Иркутск : Иркут. юрид. ин-т (филиал) Акад. Генер. прокуратуры РФ, 2009.□– 171 с.

41. Касперский, Е.В. Компьютерное зловредство / Е.В. Касперский.□– СПб.: Питер, 2009.□– 208 с.

42. Игнатенко, Г. В. Международное сотрудничество в борьбе с преступностью / Г.В. Игнатенко. – Свердловск, 1980. – С. 285-288.

43. Ушаков, Н. А. Основания международной ответственности государств / Н.А. Ушаков. – М., 1983. – С. 140.

44. Панов, В. П. Сотрудничество государств в борьбе с международными уголовными преступлениями / В.П. Панов. – М, 1999. – С. 5.

45. Международное уголовное право: учебное пособие / под ред. В. Н. Кудрявцева. – 2-изд., перераб. и доп. – М.: Наука, 1999. – С. 193.

46. Родионов, К. С. Интерпол: вчера, сегодня, завтра. – М., 1990.

47. Национальное центральное бюро Интерпола в Российской Федерации. – М., 1994. – С. 34.

III. СТАТЬИ И ПУБЛИКАЦИИ

48. Ермолович, В.Ф. Научные основы криминалистической характеристики преступлений / В.Ф. Ермолович. – Минск: ЗАО «Веды», 1999. – 273 с.

49. Номоконов, В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45–55.

50. Сухаренко, А. Киберугроза для кошелька / А. Сухаренко // ЭЖ-Юрист. – 2014. – № 6. – С. 1–3.

51. Гульбин, Ю. Преступления в сфере компьютерной информации / Ю. Гульбин // Российская юстиция. - 1997. - № 10. – С. 24-25.

52. Проблемы борьбы с компьютерной преступностью // Борьба с преступностью за рубежом (по материалам зарубежной печати): - М., 1992. № 4. С. 3-5.

53. Герасимов С.И. Роль власти в предупреждении преступности / С.И. Герасимов // Власть: криминологические и правовые проблемы. - М., 2000. - С. 3-10.

54. Ведерников, Н.Т. Личность обвиняемого как объект изучения на предварительном следствии / Н.Т. Вердников // Актуальные вопросы борьбы с преступностью. – Томск: Томский университет, 1990. – С. 99.

55. Антонян, Ю.М. Преступник как предмет криминологического изучения / Ю.М. Антонян // Вопросы борьбы с преступностью. Вып. 34. – М., 1981. – С. 21.

56. Рыбальская, В.Я. О виктимологическом анализе преступности несовершеннолетних / В.Я. Рыбальская // Виктимологические проблемы борьбы с преступностью. – Иркутск, 1982. – С. 41.

57. Некоторые правовые аспекты защиты и использования сведений, накапливаемых в информационных системах // Борьба с преступностью за рубежом. – М.: ВИНИТИ. – 1990. – № 7. – С. 36.

58. Лунеев, В.В. Десятый Конгресс ООН по предупреждению преступности и обращению/ Жилинский, С. Э. Правоохранительная деятельность / С.Э. Жилинский // Российская криминологическая энциклопедия. – М., 2000.равонарушителями / В.В. Лунев // Государство и право. – 2000. – № 9.

59. Евдокимов, К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации / К.Н. Евдокимов // Академический юридический журнал.□– 2015.□– № 1 (59).□– С. 25-26.

60. Окинавская Хартия глобального информационного общества // Дипломатический вестник. – 2000. – № 8.

IV. ДИССЕРТАЦИИ И АВТОРЕФЕРАТЫ ДИССЕРТАЦИЙ

61. Гаджиев, М. С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дисс. ... канд. юрид. Наук / М.С. Гаджиев. – Махачкала, 2004. – 215 с.

62. Зинина, У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореферат. дис. ... канд. юрид. наук: / У.В. Зинина.□ – М., 2007.□ – 33 с.

63. Бессонов, В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации: дис. ... канд. юрид. наук / В.А. Бессонов. – Н. Новгород, 2000.□ – 249 с.

64. Копырюлин, А.Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты: автореферат дис. ... канд. юрид. наук / А.Н. Копырюлин.□ – Тамбов, 2007. – 22 с.

65. Сербина, И. А. Криминологический анализ и предупреждение преступлений, совершаемых в сфере банковской деятельности: дис. ... канд. юрид. наук. / И.А. Сербина – М., 1996. – 245 с.

66. Глухова, А. А. Виктимологические факторы преступности: дис. ... канд. юрид. наук / А.А. Глухова. – Н. Новгород, 1999. – 278 с.

67. Маслакова, Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. ... канд. юрид. наук / Е.А. Маслакова. – Орел : РГБ, 2008. – 198 с.

68. Малыковцев, М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дис. ... канд. юрид. наук / М.М. Малыковцев. – М., 2007. – 186 с.

V. СУДЕБНАЯ ПРАКТИКА

69. Уголовное дело № 1-521/2014 // Архив Октябрьского районного суда г. Уфы. – 2014.

70. Уголовное дело № 1-3/2011 // Архив Ленинского районного суда г. Нижнего Тагила. – 2012.

71. Уголовное дело № 1-520/2013 // Архив Тушинского районного суда г. Москвы. – 2014.

72. Уголовное дело № 1-382/2014 // Архив Псковского городского суда Псковской области. – 2014.

VI. ЭЛЕКТРОННЫЕ ИСТОЧНИКИ

73. Norton report 2013 [Электронный ресурс] – Режим доступа: http://go.symantec.com/norton-report-2013. – Загл. с экрана.

74. 2014 Global Report on the Cost of Cybercrime [Электронный ресурс] - Режим доступа: http://www.octree.co.uk/Documents/2014-Global-Report-on-the-Cost-of-Cybercrime.pdf. – Загл. с экрана.

75. Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации [Электронный ресурс] – Режим доступа: http://giz.mvd.ru. – Загл. с экрана.

76. Kaspersky Security Bulletin 2012: Основная статистика за 2012 год [Электронный ресурс]. – Режим доступа: http:// www.securelist.com/ru/analysis/208050778/Kaspersky_Security_Bulletin_2012_ Osnovnaya_statistiks_za_2012_god#6 – Загл. с экрана.

77. Красноярского хакера будут судить за атаку на сайт правительства РФ РИА Новости [Электронный ресурс] – Режим доступа: http://ria.ru/incidents/20130117/918552526.html. – Загл. с экрана.

78. Компьютерный червь не повредил системе АЭС Бушер, сообщают СМИ РИА Новости [Электронный ресурс] – Режим доступа: http://ria.ru/science/20100926/279475025.html. – Загл. с экрана.

79. Stuxnet Worm Used Against Iran Was Tested in Israel - The New York Times [Электронный ресурс] – Режим доступа: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html. – Загл. с экрана.

80. Kaspersky Security Bulletin 2012. Кибероружие – Securelist – Всё об интернет-безопасности [Электронный ресурс] – Режим доступа: http://www.securelist.com/ru/analysis/208050779/Kaspersky_Security_Bulletin_2012_Kiberoruzhie. – Загл. с экрана.

81. ФСБ России подготовлены законопроекты о защите информационных ресурсов РФ от компьютерных атак [Электронный ресурс] – Режим доступа: http://www.garant.ru/news/488680. – Загл. с экрана.

82. G8 Information Centre. Kyushu-Okinawa Summit 2000. Okinawa Charter on Global Information Society. [Электронный ресурс]. – Режим доступа: www.library.utoronto.ca/g7/summit/2000okinawa/gis.htm. – Загл. с экрана.

83. Доклады и иные документы российских и международных организаций [Электронный ресурс]. – Режим доступа: http://sartraccc.ru/i.php?oper=read_file&filename=pub_inter.htm. – Загл. с экрана.

84. Конвенция о компьютерных преступлениях [Электронный ресурс]. – Режим доступа: www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm. – Загл. с экрана.