**ФЕДЕРАЛЬНАЯ СЛУЖБА ИСПОЛНЕНИЯ НАКАЗАНИЙ**

Федеральное казенное образовательное учреждение высшего образования

«Самарский юридический институт Федеральной службы исполнения наказаний»

Факультет внебюджетной подготовки

Кафедра профессиональных дисциплин

# ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: **Административно-правовые средства противодействия киберпреступности (на материале зарубежного и российского законодательства)**


Выполнил:

студент 151-ЗС группы 6 курса

**Жилбаев Куаныш Бауржанович**

Научный руководитель:

доцент кафедры философии и общегуманитарных дисциплин, кандидат философских наук, доцент

**Трофимцева Светлана Юрьевна**

Рецензент:

Заместитель начальника БСТМ ГУ МВД по Самарской области

полковник полиции

**Илюшин Денис Анатольевич**


Решение начальника кафедры о допуске к защите _____

Дата защиты: 25.06.2021 Оценка 4 (хорошо)

Самара

2021

# ОГЛАВЛЕНИЕ

# Введение

**Актуальность темы исследования.** Технический прогресс непосредственно или опосредованно влияет изменение общественных отношений. Так, с 1980-х гг. начался процесс формирования новой стадии общественного развития, которая получила название постиндустриального или информационного общества, которое постепенно, как было подчёркнуто Окинавской Хартией G8, приобретает глобальный характер[1]. В новых условиях начинается процесс изменения общественных отношений, где появляется новый вид – информационные отношения, определяемый А.А. Стрельцовым как общественные отношения в процессе взаимодействия субъектов для интересов в обладании нужной им информацией, передаче части имеющейся информации другим субъектам, и в сохранении в неизвестности оставшейся части информации[2]. Одной из специфичных черт информационных отношений можно считать то, что они возникают по поводу обладания нематериальным предметом – информацией, приобретающей принципиально новые характеристики: сырьё для производства, продукт общественного труда и товар, представленном в сегменте рынка, к которому потребитель должен иметь доступ.

В этой связи проблемы защиты информации с одной стороны, точнее, если рассматривать проблему с юридической точки зрения, проблемы защиты прав собственников (обладателей) в отношении их информации, включающих возможность разрешать или ограничивать доступ иным субъектов, хранить часть информации в неизвестности, извлекать прибыль или избегать неоправданных расходов, совершать определённые действия в экономической сфере, а, с другой стороны, проблемы реализации права физического

[1] Окинавская Хартия глобального информационного общества. Принята 22 июля 2000 года. Окинава [Электронный ресурс]. – Режим доступа: www.g8russia.ru/g8/history/okinava2000/4/ (дата обращения: 23.03.2021).

[2] Развитие правового обеспечения информационной безопасности / Под ред. А.А. Стрельцова. – М.: Престиж, 2006. – С.20.

лица на защиту своей частной жизни, с третьей – проблемы реализации государством функции, направленную на обеспечение национальной безопасности, защиту общества и личности от воздействия негативной информации, придаёт исследованиям в области анализа правовых проблем информационных отношений, особую актуальность.

Все действия злоумышленников в киберпространстве не только нарушают права собственников (обладателей) компьютерной информации, но и создают возможность использования компьютерных технологий в злонамеренных целях, что приводит к крупному ущербу. Так, ежегодный экономический ущерб только в США от компьютерной преступности уже в 1990-х годах приблизился к 100 млрд. долларов[3]. Проведенное в начале 2000-х гг. экспертами английской аналитической компании MI2G исследование показало, что в 2003 г. мировой экономический ущерб только от сетевых хакерских атак и распространения в сетях вирусов превышает 132 млрд. долл., хотя годом раньше – 48,5 млрд.[4].

В России в условиях сохраняющейся тенденции роста числа киберпреступлений: к примеру, в 2012 году зарегистрировано на 28% больше преступлений подобного рода, нежели чем в 2011 году[5]. В Самарской области, по данным отдела «К» БТСМ ГУ МВД, было зарегистрировано в 2017 году по ст.272 – 12 преступлений, по ст.273 – 13; в 2018 году по ст.272 – 22, по ст.273 – 33; а на начало 2019 года по ст.272 – 8, и по ст.273 – 8 преступных деяний. По статистическим данным, полученным в МВД, за 2009 – 2019 гг. всего киберпреступлений было совершено 3160[6].

---

[3] Карпов, Н, Вертузаев, М. К вопросу о борьбе с компьютерными преступлениями в Украине / Н. Карпов, М. Вертузаев // Закон и жизнь. – 2004. - №7. – С.29.

[4] Осипенко, А.Л. Борьба с преступностью в глобальных компьютерных сетях Интернет: Монография [Электронный ресурс] / А.Л. Осипенко. – Режим доступа: http://www.s-quo.com/content/articles/335/949/ (дата обращения: 02.11.2020).

[5] Национальный форум информационной безопасности обсуждает проблемы противодействия киберпреступности [Электронный ресурс] // Опубликовано: официальный сайт МВД, 05 февраля 2013 15:00.– Режим доступа: http://mvd.ru/news/item/830615/ (дата обращения: 11.11.2020).

[6] По данным статистики МВД.

При этом ряд специалистов отмечает и несовершенство российского законодательства в области противодействия киберпреступности, и стереотипность методов и приёмов расследования киберпреступлений со стороны правоохранительных органов[7], а также высокую латентность данного вида преступности: в развитых странах только 10-15% компьютерных преступлений расследуются и доводятся до суда[8], а в России, по данным некоторых специалистов, доля ещё меньше – около 0,1%[9]. Возможно, некоторое снижение статистики расследованных киберпреступлений в России с 2009 г. (347 компьютерных преступлений, 49 – компьютерного мошенничества, в 2019 – 165 и 34)[10] обусловлено недостаточной возможностью выявления злонамеренных деяний в киберсфере, нежеланием потерпевших тратить время на расследование, недостаточной способностью правоохранительных органов компетентно провести расследование и довести дело до суда.

Исходя из этого, можно констатировать, что специфика информационных отношений требует тщательного правового регулирования, и в целях защиты прав обладателей компьютерной информации и различных видов собственности необходима криминализация деяний подобного рода и проведение тщательного расследования, в том числе, на международном уровне, что обусловливает актуальность новых исследований в рассматриваемой предметной области. А выработка рекомендаций при администрировании киберпреступлений на территории РФ придаёт настоящему исследованию научно-практическую значимость.

При этом следует отметить, что, по мнению специалистов, киберпреступления относятся к наиболее сложным в плане квалификации и расследо-

---

[7] Осипенко, А.Л. Борьба с преступностью в глобальных компьютерных сетях Интернет.

[8] Карпов**,** Н, Вертузаев, М. К вопросу о борьбе с компьютерными преступлениями в Украине. – С.29

[9] Васильев, В. Расследование компьютерных преступлений как компонент обеспечения ИБ [Электронный ресурс] / В. Васильев // ИТ-безопасность. – 2001. – Май. – Режим доступа: http://www.pcweek.ru/security/article/detail.php?ID=131239 (дата обращения: 12.12.2020).

[10] По данным статистики МВД.

вания общественно опасным деяниям, поэтому их выявление, раскрытие и расследование в современных условиях борьбы с преступностью является приоритетной задачей, стоящей перед правоохранителями[11].

**Объектом исследования** выступают информационные отношения между субъектами информационной сферы, в том числе, в области защиты прав субъектов инфосферы от злонамеренных посягательств на компьютерную информацию, сети и системы её хранения, обработки и передачи.

**Предметом исследования** являются нормы уголовного права, связанные с криминализацией и расследованием злоумышленных деяний в отношении компьютерной информации, сетей и систем её хранения, обработки и передачи как во внутреннем, так и в международном праве, а также способы администрирования процесса обмена данными во процессе расследования киберпреступлений.

**Целью исследования** является сравнительный анализ специфики административно-правовых и уголовно-правовых средств противодействия киберпреступности в международном, зарубежном и российском праве.

Поставленная цель определила совокупный перечень **задач:**

– дать дефиниции терминам «киберпреступления» и «компьютерные преступления»;

– рассмотреть причины и специфику генезиса киберпреступлений;

– выявить особенности первоначального этапа криминализации злонамеренных деяний в киберсфере в зарубежном праве;

– выявить базовые проблемы, возникшие при реализации административно-правовых мер во время расследования киберпреступлений;

– рассмотреть основные направления организации противодействия киберпреступности в международном праве;

---

[11] Илюшин, Д.А. Особенности возбуждения уголовных дел о преступлениях, совершаемых в сфере предоставления услуг «Интернет» / Д.А. Илюшин // Вестник Самарского государственного университета. – 2007. – № 1 (51). – С. 9.

– проанализировать уголовно-правовые и административно-правовые рекомендации международного права на глобальном и общеевропейском уровне и особенности их реализации в зарубежном праве;

– проанализировать рекомендации по противодействию киберпреступности в законодательстве СНГ и их реализации во внутреннем праве государств СНГ;

– провести сравнительный анализ административно-правовых мер европейского законодательства и законодательства СНГ;

– рассмотреть порядок направления запросов об оказании правовой помощи РФ в предоставлении информации при расследовании киберпреступлений и выработать рекомендации по повышению эффективности противодействия киберпреступности в Российской Федерации.

**Методы исследования.** В настоящей работе использован ряд общенаучных методов: метод логико-теоретического анализа, метод сравнительно-исторического анализа, метод формально-логической типологизации и синтеза, методы научной индукции и дедукции, а также частно-правовые методы: формально-юридический и сравнительно-правовой методы.

**Степень научной разработанности темы.** Общим проблемам в области информационного права были посвящены работы А.Б. Агапова, И.Л. Бачило, О.А. Городова, Ю.Н. Дрешера, С.Н. Загородникова, Н.Н. Ковалёвой, В.А. Копылова, М.А. Лапиной, М.М. Рассолова, А.А. Тедеева и других. Проблемы правового обеспечения информационной и компьютерной безопасности нашли отражение в работах В.А. Галатенко, А.С. Гринберга, Н.Н. Горбачёва, С.А. Диева, С.Я. Казанцева, А.А. Стрельцова, Э. Талапиной, О.В. Танимова, С.Ю. Трофимцевой, А.А. Фатьянова, А.Г. Шаваева, В.И. Ярочкина и других. Отдельные проблемы защиты компьютерной защиты информации были затронуты в работах А.А. Антопольского, Е.Б. Белова, В.П. Лося, А. Брединского, А.С. Дёмушкина, Ю.В. Ковалёва, А.Б. Крысина, А. Кучерены, И.И. Локтионова, О.С. Соколовой, Е.А. Степанова, В.В. Шлыкова и других.

Некоторые вопросы, связанные с оборотом компьютерной информации, были затронуты в работах Н.Н. Богомолова, Н.И. Ветрова, Г.Н. Горшенкова, С.В. Еремина, А.Ф. Жигалова, В.И. Игнатенко, Ю.И. Калинина, И.И. Карпеца, А.В. Касаткина, С.Н. Кленова, В.А. Копылова, И. Майорова, А.Я. Минина, В.И. Першикова, В.М. Савинкова, В.А. Северина, М.А. Севрука, Ю.Ю. Соковых, К.А. Сыча, Ю.В. Трунцевского, Ю.А. Фисуна, М.Д. Шаргородского, И.В. Шмарова, Т.А. Шевцова, В.Н. Черкасова, Е.М. Юцковой, а также в диссертационных исследованиях П.А. Ананьина, Т.П. Бутенко, Н.И. Гусевой, Д.А. Илюшина, Ф.Ф. Кренслера, В. Кудрявцева, В.В. Сурина, А.Н. Третьякова, В.У. Ялунина и других.

Исходя из анализа научной литературы, следует утверждать, что, несмотря на достаточно большой круг раскрытых исследователями вопросов в области правовых проблем киберпреступности, ряд вопросов, связанных с уголовно-правовыми и процессуальными аспектами злоумышленных деяний в киберпространстве, особенно в области международного и зарубежного права, вкупе с присутствием некой неопределённости уголовных норм в области информационного права с учётом необходимости выработки практических рекомендаций для администрирования в области киберпреступлений, обусловили выбор темы настоящего исследования.

**Структура работы.** Настоящая дипломная работа состоит из введения, основной части, включающей в себя три главы, заключения, списка источников и литературы.

**Апробация работы**. Некоторые положения настоящей работы были апробированы на Всероссийской студенческой юридической олимпиаде (2021) по дополнительной номинации: «Проблемы цифрового права».

# Глава 1. СПЕЦИФИКА ГЕНЕЗИСА И НАЧАЛА КРИМИНАЛИЗАЦИИ КИБЕРПРЕСТУПЛЕНИЙ

## 1.1. Конкретизация терминов «киберпреступления» и «компьютерные преступления»

Создание ЭВМ в виде персональных компьютеров привело, как известно, к формированию информационного общества, где информация приобрела новые социальные и экономические характеристики, и революционно изменились средства её хранения, обработки и передачи, в силу чего некоторые виды информации начинают вызывать повышенный интерес у злоумышленников, а новые технологии повлекли за собой появление новых способов её несанкционированного получения.

Конкретная дата появления «компьютерной преступности» до настоящего момента вызывает споры у исследователей. Как указывает Б. Холист, согласно исследованиям, проведённым Д.Б. Паркером (США), одновременно с появлением компьютерной техники около 1940 г. возникла преступность, связанная с системой электронной обработки данных, получившая название компьютерной преступности[12].

Что касается наиболее раннего термина для обозначения злонамеренных деяний в киберсфере, то, в частности, по мнению Т.Г. Смирновой и Б. Фентона, сам термин «компьютерная преступность» стал использоваться не ранее 50-х годов[13], когда в 1958 г. было зарегистрировано первое в мире компьютерное преступление[14]. С приведёнными выше позициями ряд исследователей не согласен, поскольку, по их мнению, указанное понятие впервые

[12] Цит. по: Ястребов, Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового сравнительного анализа) / Д.А. Ястребов // Государство и право. – 2005. – №1. – С.54.

[13] Смирнова, Т.Г. Преступления в сфере компьютерной информации и некоторые особенности их совершения организованными преступными группами / Т.Г. Смирнова // Проблемы повышения эффективности борьбы с организованной преступностью: Сборник научных трудов / Отв. ред. А.Ф. Токарев. - М.: Юристъ, 1998. - С. 129.

[14] Фентон, Б. Интерпол /Б. Фентон. - М., 1996. - С. 290.

стало употребляться в американской литературе в начале 60-х годов, когда случаи преступлений с использованием ЭВМ стали неоднократными[15], а некоторые исследователи относят появление термина к 70-м гг.[16].

Однако для настоящего исследования больший интерес представляет не время начала употребления термина, а его семантические и уголовно-правовые характеристики, поскольку, в чём можно согласиться с М. Дубко, выработка однозначного корректного понятийного аппарата, в частности, используемого для обозначения рассматриваемого типа преступных деяний, крайне важна для уголовного права в целом и уголовного процесса в части деятельности конкретных сотрудников следствия и суда[17].

Как указывают Н. Карпов и М. Вертузаев, несмотря на имеющиеся национальные нормы по борьбе с компьютерной преступностью в ряде стран, «унифицированный» состав терминологии пока чётко не определен[18]. Судя по анализу литературы, наиболее ранним термином становится «computer crime» («die Computerstraftaten») – «компьютерные преступления». Следует указать, что данный термин вызывает у некоторых исследователей серьёзную критику, к примеру, Д.А. Ястребов указывает, что данный термин носит операционный характер[19]. Однако, как отмечают А.К. Бекряшев и И.П. Белозёров, термин, обозначающий преступления, совершаемые опера-

---

[15] Скоромников, К.С. Компьютерное право Российской Федерации / К.С. Скоромников. - М.: Юристъ, 2000. - С. 176.; Каспаров, А.А. Создание, использование и распространение вредоносных программ для ЭВМ: уголовно-правовые аспекты. - М.: МГУ, 2003. - С. 9. Козлов, В. «Computer crime»? Что стоит за названием? (криминалистический аспект) [Электронный ресурс] / В. Козлов. – Режим доступа: http://www.crime-research.ru/library/CCrime.html (дата обращения: 24.11.2020).

[16] Мосин, О.В. Компьютерная преступность и Интернет [Электронный ресурс] / О.В. Мосин. – Режим доступа: http://www.ibil.ru/index.php?Type=review&area=1&p=articles&id=1140 (дата обращения: 24.11.2020).

[17] Дубко, М. О понятии компьютерного преступления [Электронный ресурс] / М. Дубко. – Режим доступа: http://marketing2013.ucoz.ru/blog/o_ponjatii_kompjuternogo_prestuplenija/2013-01-19-632 (дата обращения: 24.11.2020).

[18] Карпов, Н., Вертузаев,М. К вопросу о борьбе с компьютерными преступлениями.

[19] Ястребов, Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового сравнительного анализа) / Д.А. Ястребов // Государство и право. – 2005. – №1. – С.54.

торами ЭВМ, имеет операционный характер [20]. В этой связи указанная Д.А. Ястребовым характеристика компьютерных преступлений представляется сомнительной, поскольку сужает круг субъектов преступления: субъект из общего становится специальным, что нельзя считать правомерным для квалификации данного типа преступных деяний. По мнению ряда нидерландских учёных, причиной отсутствия общего определения термина «компьютерные преступления» является наличие ряда трудностей при формулировке, которое было бы достаточно ёмким и весьма специальным[21].

В международном уголовном праве, кроме термина «computer crimes» («компьютерные преступления») используется также термин «Cybercrime» («die Cyberkriminalität») – «киберпреступность» и «cybercrimes» («киберпреступления»), широко применяемый, в частности, в документах Интерпола, и именно этим термином были объединены преступления в отношении компьютерной информации, средств и систем её обработки, хранения и передачи, а также некоторые преступления в виртуальном пространстве Интернет.

В настоящей работе для обозначения преступлений в киберсфере, непосредственно направленных против конфиденциальности, целостности и доступности компьютерных данных, систем и сетей, т. е., против законно установленного статуса информации и нормального функционирования компьютерной системы[22], будет использоваться термин «компьютерные преступления» («computer crimes»).

Другую группу киберпреступлений образуют общественно опасные деяния, где компьютер как программно-аппаратное устройство, компьютерные технологии использовались злоумышленником как орудие или средство со-

---

[20] Бекряшев, А.К., Белозеров, И.П. Теневая экономика и экономическая преступность [Электронный ресурс] / А.К. Бекряшев, И.П. Белозёров. - Режим доступа: http://sbiblio.com/biblio/archive/bekryashev_belozerov_tenevaya_economica/3.aspx (дата обращения: 23.11.2020).

[21] Цит. по: Панфилова, Е.И., Попов, А.Н. Компьютерные преступления. (Серия: Современные стандарты в уголовном праве и уголовном процессе) / Е.И. Панфилова, А.Н. Попов / Науч. редактор проф. Б.В. Волженкин. - СПб., 1998. – С.10.

[22] Трофимцева, С.Ю. Проблема выделения дефиниций базовых терминов при анализе киберпреступности / С.Ю. Трофимцева // Евразийский юридический журнал. – 2017. – № 7 (110). – С.76.

вершения преступления, т. е., это уголовные преступления, совершенные с помощью компьютерной системы»[23]. Данные преступления «имеют одну общность − компьютер является или инструментом преступника»[24], для чего, исходя из терминологии Рекомендации Совета министров государств, членов Совета Европы No R(89)9 и Будапештской Конвенции СДСЕ № 185 о киберпреступности, в настоящей работе будет использоваться термин «преступления, связанные с компьютерами» («computer-related crimes»).

Третью группу киберпреступлений, исходя из рекомендаций Будапештской Конвенции СДСЕ № 185 о киберпреступности, образуют злонамеренные деяния в киберсреде, по объективной стороне состоящие в том, что, используя компьютерные сети, в первую очередь, Интернет, злоумышленники распространяют информацию, которая запрещена внутренним и / или международным законодательством к распространению (доведению до неограниченного круга пользователей). К такой информации, прежде всего, относится детская порнография, информация ксенофобного характера, в ряде государств − информация, содержащая отрицание Холокоста, и т. д. Для таких преступлений в настоящей работе будет использоваться термин «преступления, связанные с содержанием данных» («data crimes»).

## 1.2. Генезис злонамеренных деяний в киберсфере

### 1.2.1. Зарождение киберпреступности

Как уже отмечалось, по данным исследователей, первое преступление в сфере компьютерных технологий было зафиксировано в 1958 году в США[25].

---

[23] См.: Convention on Cybercrime, ETS No 185, Budapest, 23/11/2001 [Electronic resource]. – Mode access: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (data access: 06/10/2020).

[24] Recommendation No R(89)9 of the committee of ministers to member states on computer-related crime [Electronic resource]. – Mode access: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 (data access: 06/10/2020).

[25] Концепция проекта Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам инфор-

Серьёзное компьютерное преступление в 1969 г. было совершено Альфонсе Конфессоре (США), который осуществил несанкционированный доступ к информации в электронно-вычислительной сети, и совершил налоговое преступление, нанеся тем самым ущерб в 620 тысячи долларов США[26]. В 1970 году также путем незаконного доступа к информации «Секюрити пасифик бэнк» со счетов банка было незаконно списано 10,2 млн. долл. США[27].

Количество компьютерных преступлений стало нарастать в результате создания компьютерных сетей. После превращения в 1975 году локальной экспериментальной сети ARPANET (Advanced Research Projects Agency Network), ставшей в 1983 г. национальной сетью США и перешедшей на протокол IP, в рабочую сеть с расширенным доступом, стали осуществляться первые попытки несанкционированных действий в данной сети. Поскольку одними из пользователей сети становятся правительственные службы США, с 1977 году там предпринимаются попытки разработать законопроект о защите федерального компонента сети[28], работа над которым была ускорена после того, как в 1979 году на конференции Американской ассоциации адвокатов в Далласе была предпринята первая попытка классификации злонамеренных деяний, совершаемых в компьютерной среде.

После подключения к ARPANET сначала Великобритании (1973 г.), а потом после трансформации ARPFNET в Internet (1989 г.), и подключения в нему ведущих европейских стран, а также Японии, Израиля и Новой Зеландии, количество злонамеренных посягательств на информацию, хранимую, обрабатываемую и передаваемую компьютерными средствами и системами, а также на сами информационные средства, стало расти.

---

матизации» [Электронный ресурс]. – Режим доступа: http://referatdb.ru/informatika/3504/index.html?page=2 (дата обращения: 12.12.2020).

[26] Широков, В.А., Беспалова, Е.В. Киберпреступность: история уголовно-правового противодействия [Электронный ресурс]. – Режим доступа: http://www.gosbook.ru/node/29398 (дата обращения: 13.01.2021).

[27] Широков, В.А., Беспалова, Е.В. Киберпреступность: история уголовно-правового противодействия.

[28] Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М.: ООО «Издательство «Юрлитинформ», 2001. – С.15.

К примеру, в 1988 г. студентом Корнуельского университета Робертом Моррисом была создана вредоносная компьютерная программа, которая подложила начало созданию нового типа программ – так называемых «червей», которые через Интернет внедряются в операционную систему компьютера и повреждают информационные ресурсы. По официальным данным, до момента нейтрализации программы, сбои в работе примерно 6200 компьютеров в США и других стран привели к ущербу на сумму более 98 миллионов долларов США[29]. В 1989 году на дискетах некой компании PC Cyborg стала распространяться вредоносная программа типа «троянский конь» под условным названием Aids Information Diskette. Программа внедрялась в операционную оболочку компьютера и после 90 перезагрузок шифровала содержимое жесткого диска, оставляя лишь файл README, содержащий счет на оплату и адрес почтового ящика в Панаме, на который пользователю предлагалось отправить платеж[30].

В 1995 году в Великобритании был вынесен приговор Кристоферу Пайлу (Christopher Pile), известному также как Черный Барон (the Black Baron), который создал вирусы Pathogen и Queeg. В обеих вредоносных программах был использован созданный им полиморфик-генератор SMEG (Simulated Metamorphic Encryption Generator), что затрудняло их обнаружение. Оба вируса уничтожали значительную часть данных на жестком диске жертвы. Общая сумма ущерба от данных деяний превысила 1 млн. фунтов стерлингов[31]. Ущерб от распространения вируса «ILOVEYOU» (тип – «червь») ряд специалистов оценил в 10 млрд. долларов[32]. Вирус, как потом было установлено, был распространён с Филиппин Онелем де Гузманом. При

[29] Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества.

[30] Эмм, Д. Киберпреступность и закон: обзор положений законодательства Великобритании, касающегося компьютерных преступлений [Электронный ресурс]. – Режим доступа: http://www.comprice.ru/articles/detail.php?ID=232278 (дата обращения: 25.03.2021).

[31] Эмм, Д. Киберпреступность и закон: обзор положений законодательства Великобритании, касающегося компьютерных преступлений.

[32] Цит. по: Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – С.27.

открытии файла, полученного по электронной почте с вредоносной программой начинался процесс просмотра и уничтожения файлом с определёнными расширениями, а затем после регистрации в системном реестре – рассылка инфицированных файлов дальше по сети. В числе пострадавших были тысячи компаний в различных странах мира[33].

В 1993 - 1994 гг. нашумевшим делом стало дело В. Левина, где в составе преступной группы были граждане США, Великобритании, ФРГ, Швеции, Израиля, России, а потерпевшие имели счета в Канаде, Мексике, Новой Зеландии, Аргентине, Гонконге, Индонезии, Колумбии, Уругвае, а деньги с этих счетов переводились в Россию, Швейцарию, Нидерланды, Израиль[34]. В результате деятельности этой организованной группы со счетов «City Bank of America» исчезло более 10 млн. долларов[35].

На протяжении 90-х – начала 2000-х гг. неоднократным атакам подвергались правительственные системы США и других стран мира.

С конца 90-х гг. резко выросло количество случаев шантажа посредством и с использованием компьютерных систем и сетей, включая Интернет. К примеру, граждане России А. Иванов и С. Горшков в течение 1999-2001 гг. из точек доступа, расположенных в Челябинске, выявляли уязвимости в системах защиты крупных компаний, осуществляли несанкционированный доступ и получали информацию о клиентах. После этого они информировали пострадавшие компании о выявленных уязвимостях и предлагали за соответствующую компенсацию их устранить[36].

Такая ситуация свидетельствовала о реальной общественной опасности подобных злонамеренных деяний: хищения денежных средств с банковских счётов, распространение вредоносных программ, шантаж и вымогательства,

---

[33] Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – С.27.

[34] Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – С.21.

[35] Карпов, В.С. Уголовная ответственность за преступления в сфере компьютерной информации. – С.5.

[36] Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – С.24.

незаконное использование интернет-трафик, взломы компьютерных систем (хакерские атаки и прочее) давали противозаконный доступ к базам данных как частных лиц, нарушая конфиденциальность их частной жизни, коммерческих и банковских компаний, нарушая коммерческую и банковскую тайны, так и правительственных серверов, создавая тем самым, реальную угрозу национальной безопасности государств.

### 1.2.2. Начало процесса криминализации общественно опасных деяний в киберсфере

Осознание реальности угрозы, исходящей со стороны злонамеренных деяний в киберсфере, а также понимание растущей степени общественной опасности потребовало от законодателей ряда государств, имеющих сегмент в Интернете, включения во внутригосударственное уголовное законодательство новых составов преступлений.

В Европе подобный род деяний впервые был криминализирован в 1973 году путём принятия Швецией закона о противодействии посягательствам на компьютерную информацию (Data Act, 2 апреля 1973 г.), котором предусматривалась уголовная ответственность за незаконное проникновение в компьютерную систему и модификацию компьютерной информации, позволяющую совершить хищение денег, ценных бумаг, имущества, услуг либо ценной информации[37], в результате чего в Уголовном кодексе Швеции появились новые составы преступлений, отсутствующие во внутреннем праве других государств[38]. В 1979 г. схожие составы были введены в уголовный кодекс Норвегии[39].

---

[37] Sverige: Straffbalken 1864 [Elektronisk resurs]. − Åtkomstläge: https://riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700 (datum för åtkomst: 29/02/2021).

[38] Широков, В.А., Беспалова, Е.В. Киберпреступность: история уголовно-правового противодействия.

[39] Norge: Straffeloven 1902 [Elektronisk ressurs]. − Tilgangsmodus: https://lovdata.no/dokument/NLO/lov/1902-05-22-10?q=straffeloven (anke dato: 10/02/2021).

Рост компьютерных злонамеренных деяний в США вынудил принять в 1984 г. с дополнениями 1986 г. Закон о мошенничестве и злоупотреблении с использованием компьютеров (The Computer Fraud and Abuse Act), который запрещал несанкционированный доступ к любой компьютерной системе, несанкционированное получение секретной военной информации, а также данных, циркулирующих в финансовым учреждениям (о кредитных картах, счетах и прочее), принадлежащие правительственным учреждениям, и международным или межштатовым организациям[40]. Кроме этого, в законе содержались нормы, криминализирующие несанкционированное повреждение данных, в том числе, за счёт распространения вредоносных программ[41]. На основе этого закона в Титул 18, часть I, главу 47 Свода законов США были включены некоторые составы в §1030 (a) (1-5)[42].

В 1990 в Великобритании принимается закон о неправомерном использовании компьютеров (Computer Misuse Act). Как отмечают специалисты, проблема актуализировалась после того, как суд не смог вынести обвинительный приговор по делу Стивена Гоулда и Роберта Шифрина, т. к. по действующему британскому законодательству обвинение было по Закону о подлоге и подделках 1981 года, хотя само деяние состояло в получении несанкционированного доступа в 1984 году к принадлежащему компании British Telecom сервису Prestel. Они были оправданы апелляционным судом, и приговор был утверждён палатой пэров[43], поскольку состава преступления по указанному закону деяние не содержало. В результате Закон 1990 года криминализировал три вида деяний, связанных с несанкционированным доступом в компьютерные системы и сети[44]. Кроме этого, рядом новых норм был дополнен Закон о телекоммуникациях (1984 г.), в котором в объекты защиты

[40] USA: U.S. Code. Title 18. Part I. Chapter 47. §1030 [Electronic resource]. Mode access: http://www.law.cornell.edu/uscode/text/18/1030 (data access: 06/10/2020).

[41] USA: U.S. Code. Title 18. Part I. Chapter 47. §1030.

[42] См.: USA: U.S. Code. Title 18. Part I. Chapter 47. §1030.

[43] Эмм, Д. Киберпреступность и закон: обзор положений законодательства Великобритании, касающегося компьютерных преступлений.

[44] UK: The Computer Misuse Act (1990) [Electronic resource]. – Mode access: http://www.legislation.gov.uk/ukpga/1990/18 (data access: 06/10/2020).

были включены компьютерные системы, а также Закон о защите детей (1978 г.) и Закон о сексуальных преступлениях (1956 г.), где в отдельный состав было выделено распространение детской порнографии через Интернет.

Тем самым, первый опыт криминализации злонамеренных деяний в киберсфере показал, что проблема реальности общественной опасности таких деяний стала осознаваться на законодательном уровне, однако глобальным процесс становился недостаточно быстро, несмотря на то, что, как было показано выше, экономический ущерб от таких деяний продолжал расти. Кроме того, процесс расследования киберпреступлений поставил перед законодателями государств ещё ряд проблем, которые необходимо было начать решать.

### 1.2.3. Базовые проблемы, возникшие при администрировании процесса расследования киберпреступлений

Проведённый в рамках настоящей работы анализ научных и научно-практических исследований и опыта первых попыток криминализации киберпреступлений показал, что к концу XX века очевидными для государств, криминализировавших некоторые злонамеренные общественно опасные деяния в киберсфере, показал, что при расследовании таких деяний возникают сложности как практического, так и нормативно-процессуального плана.

В этой связи первой проблемой на уровне процесса стало определение времени совершения преступления. Но, как считают некоторые исследователи, точное время может иметь принципиальное значение только в тех случаях, когда или криминализация деяния проведена относительно недавно, или ответственность за совершение деяния была изменена[45], и тогда правоохранителям требуется соотнести действующую норму и событие преступления.

[45] Трофимцева С.Ю., Илюшин, Д.А. Некоторые аспекты определения места и времени совершения киберпреступлений в Российской Федерации / С.Ю. Трофимцева, Д.А. Илюшин // Евразийский юридический журнал. – С.246.

Другой важной проблемой, возникшей при расследовании уже первых киберпреступлений, прежде всего, с точки зрения норм процессуального законодательства и применения уголовных норм определённого государства, а также конкретизации подследственности внутри государства по следственным отделам правоохранительных структур, стало определение места совершения киберпреступления. Первоочередная сложность, как утверждают исследователи, заключалась в том, что, по мнению Н. Мамедова и Н.П. Яблокова, состоит в том, что место совершения преступления и место наступления общественно опасных последствий не совпадают[46], поскольку киберпреступления относятся к специфическим деяниям, которые можно совершить без непосредственного присутствия преступника на месте преступления путём удалённого доступа к компьютерную систему[47].

По мнению исследователей, место совершения киберпреступления можно конкретизировать лишь в ряде ситуаций, и то иногда условно [48]. Так, например, если определяется IP-адрес точки входа в компьютерную систему, а он, в свою очередь, привязан к определённому физическому или юридическому лицу. И в этом случае некоторые исследователи предложили считать местом совершения преступлении определённые место жительства физического лица или юридический адрес юридического лица[49]. Но развитие IT привело к тому, что к началу XXI века распространение технологий прокси-серверов, анонимайзеров, выхода в Интернет по Wi-Fi привело к тому, что

---

[46] Яблоков, Н.П. Криминалистика: Теоретические, методологические и науковедческие основы криминалистики [Электронный ресурс] / Н.П. Яблоков. – Режим доступа: http://www.be5.biz/pravo/k012/223.htm (дата обращения: 23.12.2020).
Мамедов, Н. Криминалистические проблемы расследования преступлений в сфере компьютерной информации [Электронный ресурс] / Н. Мамедов // Специализированный ежемесячный журнал «ЮРИСТ». – 2008. – Сентябрь. - № 9 – Режим доступа: http://journal.zakon.kz/203375-kriminalisticheskie-problemy.html (дата обращения: 23.12.2020).

[47] Трофимцева С.Ю., Илюшин, Д.А. Некоторые аспекты определения места и времени совершения киберпреступлений в Российской Федерации. – С.246.

[48] Трофимцева С.Ю., Илюшин, Д.А. Некоторые аспекты определения места и времени совершения киберпреступлений в Российской Федерации. – С.246.

[49] Трофимцева С.Ю., Илюшин, Д.А. Некоторые аспекты определения места и времени совершения киберпреступлений в Российской. – С.247.

определить реальное местоположение компьютера (телефона, планшета и других устройств), а, следовательно, и злоумышленника на момент окончания преступления становится невозможным[50]. Исходя из чего, возможным местом совершения преступления, по мнению некоторых специалистов, может считаться юридический адрес юридического лица или место проживания (место регистрации или иное, согласно внутреннему законодательству государств), либо место обнаружения потерпевшим факта деяния[51], либо же место преступления устанавливается согласно внутреннему уголовно-процессуальному законодательству государства.

Кроме того, исходя из изложенного выше, одной из принципиальных особенностей киберпреступлений является их транснациональный характер. Такая специфика обусловлена тем, что виртуальное пространство, в отличие от материального, не имеет и не может иметь государственных границ. В таких ситуациях преступление характеризуется специалистами как транснациональное, и тогда возникает ещё одна проблема, характерная для киберпреступлений: проблема национальной подсудности. Разрешение этой проблемы необходимо в связи с тем, что от определения подсудности зависит определение того, по уголовным нормам какого государства будет вынесена санкция за его совершение и будет ли вообще злонамеренное деяние в киберсреде отнесено к уголовно наказуемым по внутреннему уголовному праву государств[52] (к примеру, поскольку В. Левин, будучи гражданином РФ и находясь на территории России, совершал в составе организованной группы злонамеренное деяние в 1993 – 1994 гг. в то время, когда на территории РФ ещё действовал УК РСФСР (1960 г.), где отсутствовали составы, криминализи-

[50] Трофимцева С.Ю., Илюшин, Д.А. Некоторые аспекты определения места и времени совершения киберпреступлений в Российской Федерации. – С.247.

[51] Трофимцева С.Ю., Илюшин, Д.А. Некоторые аспекты определения места и времени совершения киберпреступлений в Российской. – С.247.

[52] Трофимцева, С.Ю. Международное уголовно-правовое противодействие киберпреступности: к вопросу об «устаревании» Будапештской конвенции / С.Ю. Трофимцева // Сборник докладов II Всероссийской научной конференции (с приглашением зарубежных ученых) «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации», 28-30 октября, Ставрополь. – Ставрополь: , 2020. – С. 23.

рующие общественно опасные деяния в киберсреде, наказание по российским законам он нести не должен был. С аналогичной ситуацией столкнулись Филиппины, когда была установлена личность распространителя вируса «ILOVEYOU». В самих Филиппинах не было уголовной нормы, криминализирующей деяние Онела де Гузмана, а между остальными государствами, как и в случае ситуации с В. Левиным, возник на тот момент фактически не разрешимый спор о подсудности деяния и выдаче (в тех случаях, когда это возможно по внутригосударственному праву) злоумышленника, поскольку на это претендует несколько государств.

Из позитивных моментов в плане разрешения указанных проблем можно отметить только Великобританию, которая, столкнувшись с ситуацией вокруг «дела Левина», приняла решение о том, что если один из элементов (стадий) преступления совершён так или иначе на её территории, то преступление считается оконченным на её же территории, что сразу сняло для британских правоохранительных органов рассматриваемую проблему подсудности для транснациональных деяний в киберсфере.

## Выводы по 1 главе

Итак, на основе проделанного анализа можно констатировать, что прогресс информационных технологий и возникшие информационные отношения по поводу информационного обмена, привёли к появлению нового вида общественно опасных деяний – киберпреступлений, под которыми в настоящей работе понимаются виновные общественно опасные деяния, совершаемые в инфотелекоммуникационной среде и посягающие на безопасность информационных отношений, определяемых как общественные отношения, возникающие в процессе взаимодействия субъектов для удовлетворения их интересов в информационном процессе, протекающем в киберпространстве.

В настоящей работе в качестве базовой классификации киберпреступлений выбрана классификация, принятая в международном праве на основе

Будапештской конвенции о киберпреступности. В качестве основных классов киберпреступлений выделяются: компьютерные преступления, преступления, связанные с компьютерами, и преступления, связанные с данными. Под компьютерными преступлениями в настоящей работе понимаются совершаемые в инфотелекоммуникационной среде виновные общественно опасные деяния, непосредственно направленные против конфиденциальности, целостности и доступности данных, что приводит к нарушению законно установленного статуса информации компьютерных систем и нормального функционирования компьютерной системы и сети. Под преступлениями, связанными с компьютерами, в настоящей работе понимаются виновные общественно опасные деяния, совершённые при помощи компьютерных систем, где компьютер как программно-аппаратное устройство, компьютерные технологии использовались злоумышленником как орудие или средство совершения преступления. Под преступлениями, связанными с данными, в настоящей работе понимаются виновные общественно опасные деяния, состоящие в распространении в киберсфере негативной информации, запрещённой внутригосударственным и международным законодательством.

Зарождение киберпреступности и её эскалация в условиях создания инфотелекоммуникационных сетей, особенно Интернета, свидетельствовало о реальной общественной опасности злонамеренных деяний, совершаемых в киберсфере: хищения денежных средств с банковских счётов, распространение вредоносных программ, повреждающих компьютерные устройства, становящиеся средством шантажа и вымогательства, незаконно использующих интернет-трафик, и т. п. наносили реальный, причём всё чаще, весьма значительный экономический ущерб, взломы компьютерных систем (хакерские атаки и прочее) давали противозаконный доступ к базам данных как частных лиц, нарушая конфиденциальность их частной жизни, коммерческих и банковских компаний, нанося экономический ущерб, нарушая коммерческую и банковскую тайны, так и правительственных серверов, создавая тем самым, реальную угрозу национальной безопасности государств.

В связи с этим, с начала 1970-х гг. сначала в Европе (Швеция и Норвегия), затем и в других странах мира начался процесс криминализации злонамеренных деяний в киберсфере. Однако процесс расследования киберпреступлений поставил перед законодателями государств ещё ряд проблем, в числе которых: определение времени и места совершения киберпреступлений, поскольку именно от определения места совершения преступления зависит конкретизации подследственности как внутри государства, так и на международном уровне в случае совершения транснационального преступления.

При этом сама транснациональность киберпреступлений в настоящей работе рассматривается как специфический атрибут таких деяний, обусловленный особенностями той среды, в которой они совершаются: не имеющее границ и материальных точек привязки киберпространство, где, как указывают специалисты, в отличие от материальной среды сохранность следов весьма непродолжительная и условная, и их выявление напрямую зависит от времени установления признаков преступления и специальной квалификации и технической оснащённости сотрудников правоохранительных органов[53].

Исходя из выше изложенного, очевидным являются три тезиса: развитие компьютерных технологий приводит к тому, что злоумышленники всё время изобретают новые виды злонамеренных деяний в киберсфере и новые способы их совершения, поэтому на внутригосударственном уровне важным является постоянное совершенствование уголовного законодательства в области противодействия киберпреступности, а в связи с постоянно нарастающей степенью их транснациональности, на международном уровне требуется масштабная гармонизация уголовных норм внутреннего права, а также функционирование системы обмена данными между правоохранительными органами государств в сфере противодействия киберпреступности.

[53] Трофимцева, С.Ю. Международное уголовно-правовое противодействие киберпреступности: к вопросу об «устаревании» Будапештской конвенции / С.Ю. Трофимцева // Сборник докладов II Всероссийской научной конференции (с приглашением зарубежных ученых) «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации», 28-30 октября, Ставрополь. – Ставрополь: , 2020. – С. 24.

# ГЛАВА 2. УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

## 2.1. Рекомендации по уголовно-правовому противодействию киберпреступности на глобальном уровне

Поскольку, как было показано выше, с конца 1980-х гг. количество киберпреступлений стало расти, при этом большинство масштабных из них носили транснациональный характер, как по составу участников, так и по месту наступления общественно опасных последствий, и законодателям ряда стран стало очевидно, что в силу повышенной общественной опасности, и отставания норм внутригосударственного права от совершаемых посягательств, а также, как указывает А.Г. Волеводз, в связи с тем, что «любое правоотношение, возникающее в связи с использованием возможностей глобальных компьютерных сетей, подобных Internet, содержит иностранный элемент»[54], требовалось срочное принятие мер на уровне международного права.

Считается, что одной из первых попыток актуализации проблемы на международном уровне стала предпринятая попытка в рамках Организации экономического сотрудничества и развития (ОЭСР), Комитетом которой была обсуждена возможность международной гармонизации уголовного права государств с целью борьбы с экономическими компьютерными преступлениями, и в 1986 г. был предложен список деяний[55].

На глобальном уровне данная проблема вышла на рассмотрение ООН с начала 1990-х гг. В 1990 году киберпреступность и необходимость консолидации усилий международного сообщества обсуждалась на VIII конгресса ООН, на котором была принята резолюция о преступлениях, связанных с применением компьютеров, и дано было поручение Международной уголов-

[54] Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – С.40.

[55] Широков, В.А., Беспалова, Е.В. Киберпреступность: история уголовно-правового противодействия.

ной полиции. Результатом стала разработка МОУП Интерпола в 1991 г. Кодификатора киберпреступлений Интерпола, который был интегрирован в автоматизированную систему поиска и является доступным подразделениям Национальных центральных бюро МОУП Интерпол более чем 120 стран. Для обозначения киберпреступления можно использовать до пяти кодов, расположенные в порядке убывания: QA – несанкционированный доступ и перехват (QAH – компьютерный абордаж, QAI – перехват, QA1 – кража времени, QAZ – прочие виды несанкционированного доступа и перехвата); QD – изменение компьютерных данных (QDL – логическая бомба, QDT – троянский конь, QDV – компьютерный вирус, QDW – компьютерный червь, QDZ – прочие виды изменения данных); QF – компьютерное мошенничество (QFC – мошенничество с банкоматами, QFF – компьютерная подделка, QFG – мошенничество с игровыми автоматами, QFM – манипуляции с программами ввода-вывода, QFP – мошенничество с платежными средствами, QFT – телефонное мошенничество, QFZ – прочие компьютерные мошенничества); QR – незаконное копирование («пиратство» или нарушение авторских прав) (QRG – использование компьютерных игр, QRS – использование программного обеспечения, QRT – использование топографии полупроводников, QRZ – прочее незаконное копирование информации); QS – компьютерный саботаж (QSH – с аппаратным обеспечением, QSS – с программным обеспечением, QSZ – прочие виды саботажа); QZ – прочие компьютерные преступления (QZB – с использованием компьютерных досок объявлений, QZE – хищение информации, с коммерческой тайной, QZS – передача конфиденциальной информации, QZZ – прочие компьютерные преступления)[56]. Данный коди-

[56] Cit.: Urbanovich, P. Information protection. Part 1: introduction to the subject area [Electronic resource]. – Mode access: https://elib.belstu.by/bitstream/123456789/29335/1/Information%20prot_Part%201-introduction.pdf (data access: 01/02/2021).

фикатор используется при отправке запросов или сообщений о компьютерных преступлениях по телекоммуникационной сети МОУП Интерпол[57].

В 1995 году принимается Резолюция AG№/64/P.RES/19 МОУП Интерпол «Компьютерно - ориентированная преступность», где подчёркивалось, что «проблема борьбы с преступностью, связанной с незаконным использованием компьютеров, должна решаться в одинаковой степени в африканском, американском и азиатском регионах, и каждым членом Интерпола в этих регионах»[58], а в итоговом документе X Конгресса ООН по предупреждению преступности и обращению с правонарушителями (Венская декларация о преступности и правосудии: ответы на вызовы XXI века, 2000 г.) отмечалось, что быстрое распространение новых информационных технологий сопровождается их использованием в преступных целях и неспособностью государств и иных организаций справиться с возрастающим количеством юридических проблем как национального, так и международного характера[59], поэтому государствам мира нужно «работать в направлении укрепления наших возможностей по предупреждению, расследованию и преследованию преступлений, связанных с использованием высоких технологий и компьютеров»[60].

В результате обострения проблемы киберпреступности в начале XXI в. в 2001 г. Генеральной Ассамблеей ООН были приняты резолюции 55/63 и 56/121 «Борьба с преступным использованием информационных технологий». Так, в Резолюции ООН 56/121 выражена обеспокоенность в связи с тем, что «технический прогресс создал новые возможности для преступной дея-

---

[57] Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – С.20.

[58] См.: Резолюция AG№/64/P.RES/19 «Компьютерно-ориентированная преступность». Принята Генеральной ассамблеей Интерпола (4–10 октября 1995 г.). [Электронный ресурс]. – Режим доступа: http://www.№ewasp.omskreg.ru/bekryash /app1.htm#6 (дата обращения: 12.01.2021).

[59] Цит. по: Зинина, У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. – С.30.

[60] Цит. по: Жмыхов, А.А. Компьютерная преступность за рубежом и ее предупреждение / А.А. Жмыхов. Дисс. …канд. юридических наук. Спец. 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право». – М., 2003. – С.161.

тельности, и в частности для преступного использования информационных технологий», подчеркнута «необходимость усиления координации и укрепления сотрудничества между государствами в борьбе с преступным использованием информационных технологий», призвало все государства усилить работу в области противодействия киберпреступности[61]. А в Резолюции ООН 55/63 от всех государств было потребовано усилить «сотрудничество правоохранительных органов в расследовании случаев трансграничного преступного использования информационных технологий и судебном преследовании» преступников, для чего государства обязывались «обмениваться информацией о проблемах, с которыми они сталкиваются в борьбе с преступным использованием информационных технологий», а также государствам настойчиво рекомендовалось модифицировать свои правовые системы[62].

В этой связи требовалась реальная координация усилий государств по выработке рекомендаций по гармонизации уголовного законодательства для квалификации как преступление злонамеренного деяния в киберсфере по уголовному законодательству любой страны мира, а также рекомендаций в области уголовно-процессуального права для обмена данными, проведения совместного расследования правоохранительными органами различных государств, а также для экстрадиции преступников (если это является возможным по нормам внутреннего права)

## 2.2. Особенности процесса гармонизации уголовного законодательства зарубежных государств по противодействию киберпреступности

### 2.2.1. Рекомендации по уголовно-правовому противодействию киберпреступности на общеевропейском уровне

[61] Резолюция ООН 56/121 «Борьба с преступным использованием информационных технологий». Принята Генеральной Ассамблеей по докладу Третьего комитета (A/55/593) 22.01.2001 г. [Электронный ресурс] // Официальный сайт ООН. – Режим доступа: https://www.un.org/ru/ga/third/56/third_res.shtml (дата обращения: 22.11.2020).

[62] Резолюция ООН 55/63 «Борьба с преступным использованием информационных технологий». Принята Генеральной Ассамблеей по докладу Третьего комитета (A/55/593) 22.01.2001 г. [Электронный ресурс] // Официальный сайт ООН. – Режим доступа: https://www.un.org/ru/ga/third/55/third_res.shtml (дата обращения: 22.11.2020).

Осознание серьёзности рассматриваемой проблемы заставило начать координировать усилия и европейским государствам. С 1985 начал работу Отдельный комитет экспертов по компьютерным преступлениям Совета Европы. 13 сентября 1989 г. Совет Европы принял Рекомендацию No R(89)9 Комитета Министров стран - членов Совета Европы о преступлениях, связанных с компьютерами, где была сделана попытка выделить ряд компьютерных преступлений и содержались рекомендации по включению в уголовное законодательство стран новых составов[63].

В 1995 году Совет Европы принял Рекомендацию No R(95)13 Комитета Министров стран - членов Совета Европы, касающуюся проблем уголовно-процессуального права, связанного с компьютерами, в которой содержались рекомендации по гармонизации норм уголовно-процессуального права и совместным действиям в области расследований киберпреступлений[64].

В 1996 г. Европейский комитет по проблемам преступлений в ноябре 1996 года принял решение учредить специальный комитет экспертов для обсуждения вопросов киберпреступлений. в феврале 1997 года Решением No CM/Del/Dec(97)583 Комитет Министров учредил Комитет экспертов по преступлениям в киберпространстве, на заседаниях которого шла непосредственная работа над созданием проекта европейской конвенции по проблемам киберпреступлений[65].

В апреле 2000 года появился проект общеевропейского документа по борьбе с киберпреступлениями, который был обнародован для комментариев к тексту конвенции, на основе которых текст был пересмотрен и представлен

---

[63] Recommendation No R(89)9 of the committee of ministers to member states on computer-related crime.

[64] Vid.: Recommendation No R (95)13 of the Committee of ministers to member states concerning problems of criminal procedural law connected with information technology [Electronic resource]. – Mode access: http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp (data access: 06/10/2020).

[65] Кубышкин, А.В. Международно-правовые проблемы обеспечения информационной безопасности государства / А.В. Кубышкин. – М.: Юристъ, 2002. – С.71.

на пятидесятую пленарную сессию Комитета по проблемам преступлений в июне 2001 года. А с 23 ноября 2001 году была открыта для подписания Будапештская Конвенция СДСЕ № 185 о киберпреступлениях (далее – Будапештская конвенция) с изменениями Страсбургского протокола от 28 января 2003 года, которую на настоящий момент ратифицировали 66 государств[66], включая не только европейские, но и США, Канаду, ЮАР, Японию, Австралию (всего присоединилось 68 стран[67]). Конвенция носит рекомендательный характер, и в её статьях подчёркивается, что каждая сторона - участник Конвенции принимает законодательные меры на уровне своего внутригосударственного права в соответствии с Конвенцией, если это не противоречит её национальному законодательству: «Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву…»[68].

Нормы уголовного права содержатся в части I «Материальное уголовное право» главы II «Меры, которые следует принять на национальном уровне». Там выделены составы, рекомендуемые криминализировать во внутригосударственном праве, что должно привести к недопущению возникающих ситуаций, когда злоумышленник, совершая деяние, не привлекается к ответственности из-за отсутствия норм в национальном законодательстве.

Прежде всего, следует отметить, что Конвенция рекомендует криминализировать противозаконный доступ к компьютерной системе в целом или любой ее части (ст. 2), причём по субъективной стороне данное деяние должно являться преднамеренным. Очевидное отличие от российского законодательства заключается в ином выборе объекта доступа: в Конвенции это компьютерная система, что означает факт проникновения в систему как

---

[66] Таблица подписей и ратификации договора 185 «Конвенция о компьютерных преступлениях». Статус на 15/05/2021 [Электронный ресурс] // Сайт Совета Европы. – Режим доступа: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=TVQJuVZx (дата обращения: 15.05.2021).

[67] Из европейских стран к Конвенции не присоединились РФ, Белоруссия.

[68] Convention Committee on Cybercrime ETS No 185, Budapest, 23/11/2001.

непосредственный, так и удалённый, причём, если система является защищённой, то любой несанкционированный доступ является осуществлённым «с нарушением требований безопасности»[69], поскольку если система общедоступная, то сам вход в неё предполагается как данность.

Ст. 3 Конвенции содержит рекомендацию криминализировать умышленный неправомерный перехват с использованием технических данных ограниченного доступа (включая ПЭМИН[70])[71]. Особую опасность представляет съём информации с ПЭМИН. В ст. 4 Конвенции нашли отражение рекомендации по криминализации общественно опасных последствий несанкционированного доступа или пребывания в системе в виде неправомерного воздействия на данные, выразившихся в умышленном повреждении, удалении, ухудшении качества, изменении или блокировании компьютерных данных[72]. Под блокированием данных в Конвенции понимается частичное или полное блокирование доступа лицам, не имеющим, согласно политике безопасности, утверждённой правомочным лицом для данной компьютерной системы, права получать информацию и осуществлять с ней определённые действия.

Ст. 5 Конвенции содержит рекомендацию по криминализации неправомерного воздействия на функционирование компьютерной системы путём ввода информации, а также воздействия на компьютерные данные, содержащиеся в системе. В ч. 1 ст. 6 Конвенция рекомендует считать преступлением противозаконное использование устройств и программ. Под противозаконным использованием понимается умышленное и неправомерное производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в использование[73]. В п.i ч.1 ст.6 рекомендуется криминализировать использование устройств или компьютерных про-

[69] Convention Committee on Cybercrime ETS No 185, Budapest, 23/11/2001.
[70] ПЭМИН – побочные электромагнитные излучения и наводки.
[71] Convention Committee on Cybercrime ETS No 185, Budapest, 23/11/2001.
[72] Convention Committee on Cybercrime ETS No 185, Budapest, 23/11/2001.
[73] Согласно ст.6.3, не образуют состав преступления деяния, указанные в ст.6.1 и 6.2, если это нужно и предназначено для разрешённых испытаний или защиты компьютерной системы.

грамм, разработанных или адаптированных, в первую очередь, для целей совершения преступных деяний[74].

Ст. 7 Конвенции рекомендует криминализировать подлог с использованием компьютерных технологий, состоящий в умышленном и неправомерном воздействии на данные, результатом чего становится нарушение аутентичности информации. Ст. 8 Конвенции рекомендует криминализировать мошенничество с использованием компьютерных технологий как преступление против собственности путём несанкционированного воздействия на данные или вмешательство в функционирование компьютерной системы[75]. В ст. 9 Конвенции рекомендуется признать преступными деяния, связанные детской порнографией и реализуемые через компьютерную систему[76]. Последнее деяние, которое Конвенция рекомендует криминализировать, связано с нарушением авторского права и смежных прав, если эти действия совершаются в коммерческом масштабе (ст. 10)[77].

### 2.2.2. Особенности процесса гармонизации уголовного законодательства зарубежных стран, ратифицировавших Будапештскую конвенцию

Следует, прежде всего, отметить, что, когда Будапештская конвенция была открыта к подписанию, то к ней в течение двух-трёх лет присоединилась большая часть государств - членов Совета Европы. Однако, во-первых, следует констатировать, что процесс присоединения оставшейся часть стран затянулся (так, Андорра, Монако – в 2013 г., Сан-Марино – в 2017 г.[78]). А во-вторых, в ряде европейских государств ратификация Будапештской конвенции последовала спустя лишь весьма продолжительное время: в Польше –

[74] Convention Committee on Cybercrime ETS No 185, Budapest, 23/11/2001.
[75] Convention Committee on Cybercrime ETS No 185, Budapest, 23/11/2001.
[76] Convention Committee on Cybercrime ETS No 185, Budapest, 23/11/2001.
[77] Convention Committee on Cybercrime ETS No 185, Budapest, 23/11/2001.
[78] Таблица подписей и ратификации договора 185 «Конвенция о компьютерных преступлениях». Статус на 15/05/2021.

через 15 лет, а в Швеции – почти 20 лет[79]. Ирландия Будапештскую конвенцию не ратифицировала до настоящего момента. Из ряда позитивных моментов можно отметить то, что Будапештская конвенция, как и другие конвенции Совета Европы, носит открытый характер. Так, после открытия Конвенции для подписания, к ней сразу же в 2001 г. присоединились США, Канада, ЮАР и Япония, и число стран, ратифицировавших Будапештскую конвенцию, постоянно растёт[80].

Рекомендация, сформулированная в ст. 2 Конвенции нашла отражение в уголовных законах большинства западных стран, причём в европейских уголовных кодексах различия незначительны. К примеру, в УК Франции ст. 323-1[81], в УК Австрии (§118a) и УК Нидерландов (ст.138a) - преднамеренный неправомерный доступ в компьютерную систему с нарушением мер защиты[82], при этом в УК Швейцарии (ст.143bis) уточнено, что несанкционированный доступ осуществляется без цели обогащения[83]. Однако, в УК Дании (§263(2)), в отличие от нормы Конвенции, речь идёт о доступе к информации или к компьютерным программам[84], аналогичная норма содержится в ст.I (1) (a)(b)(c) Закона Великобритании о злоупотреблении компьютером (the Computer Misuse Act)[85], а в УК Швеции (ст. 9c главы 4) – о доступе к записи в системе автоматической обработки данных[86]. В УК ФРГ (§202a) карает неза-

---

[79] Таблица подписей и ратификации договора 185 «Конвенция о компьютерных преступлениях». Статус на 15/05/2021.

[80] Таблица подписей и ратификации договора 185 «Конвенция о компьютерных преступлениях». Статус на 15/05/2021.

[81] France: Code pénal [Ressources électroniques]. – Mode d'accès: http://www.legifrance.gouv.fr/affichCode.do;jsessionid=ACAD58662A3CECCA88A42F6142A3DBCF.tpdjo12v_1?idSectionTA=LEGISCTA000006149839&cidTexte=LEGITEXT000006070719&dateTexte=20140405 (date d'appel: 24/03/2021).

[82] Österreich: Das Strafgesetzbuch der Österreich 1974 [Elektronisches Resurs]. – Das Regime des Zugang: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (Datum der Beschwerde: 11/03/2021).

[83] Schwitzerland: Das Strafgesetzbuch 1937 [Elektronisches Resurs]. – Das Regime des Zugang: http://www.admin.ch/opc/de/classified-compilation/19370083/index.html, freies (Datum der Beschwerde: 20/02/2021).

[84] Danmark: Straffeloven 1997 [Elektronisk ressource]. − Adgangstilstand: https://danskelove.dk/straffelovengratis (adgangsdato: 09/01/2021).

[85] UK: The Computer Misuse Act.

[86] Sverige: Straffbalken 1864.

конный доступ к защищаемым от подобных действий данным в случае, если имел место факт получения этих данных как для самого преступника, так и для иного лица[87].

Свод законов США (ст.1030(a)) криминализирует факт не только несанкционированного доступа, но и факт превышения доступа к защищаемой информации[88]. При этом уголовное законодательство США, в частности, §1030(a), содержит квалифицирующие составы по несанкционированному доступу в защищённые правительственные компьютерные системы (§1030(a)(2))[89].

Следующая рекомендация (ст. 3 Конвенции) в европейском законодательстве наиболее чётко с выделением специальных составов преступлений была воплощена в уголовном законодательстве Австрии и Нидерландов (ст. 139b УК Нидерландов[90], §119(1) УК Австрии[91]). В Своде законов США, в отличие, к примеру, от австрийского законодательства, нет ссылки на ПЭМИН, но американский законодатель, так же, как и европейский, относя данное деяние к нарушению тайны коммуникации, вводит санкцию (§2511) за перехват и разглашение сообщений, передаваемых, в том числе, электронным способом[92].

Аналогичные ст. 4 Конвенции нормы содержатся практически во всех уголовных законодательствах (ч. 2 ст. 323-1 УК Франции, §303a(1) УК ФРГ, §126a(1) УК Австрии, ст. 144bis УК Швейцарии, ст. 9c главы 4 УК Швеции, ст. 350a УК Нидерландов, 2701 Свода законов США).

В плане реализации рекомендации ст. 5 Будапештской конвенции нормы уголовного законодательства ФРГ и Австрии схожи в том, что в диспозициях соответствующих статей деяние описывается сходно с нормой Конвен-

---

[87] Die BRD: Das Strafgesetzbuch der BRD [Elektronisches Resurs]. – Das Regime des Zugang: http://www.gesetze-im-internet.de/stgb/, freies (Datum der Beschwerde: 11/03/2021).

[88] USA: U.S. Code. Title 18. Part I. Chapter 47. §1030.

[89] USA: U.S. Code. Title 18. Part I. Chapter 47. §1030.

[90] Nederlanden: Wetboek van Strafrecht 1881 [Elektronische bron]. − Toegangsmodus: http://www.wetboek-online.nl/wet/Sr.html, gratis (datum beroep: 23/02/2021).

[91] Österreich: Das Strafgesetzbuch der Österreich 1974.

[92] USA: U.S. Code. Title 18. Part I. Chapter 47. §1030.

ции (§303b УК ФРГ, §126b УК[93]). Уголовное законодательство Франции (ст.323-2) и Нидерландов (ст.161sexies, 161septies, 351, 351bis) не акцентирует внимание способе осуществления деяния посредством информационного воздействия. По аналогичному пути пошёл законодатель США, разграничив при этом составы преступлений по воздействию на функционирование правительственного компьютера (§1030(a)(3)) и по воздействию на другие защищаемые компьютеры ((§1030(a)(5))[94]. В УК Нидерландов две группы преступных деяний разграничиваются по объекту: деяния, предусмотренные в ст. 351, 351bis наносят ущерба имуществу, а ст. 161sexies, 161septies – преступления против общей безопасности или собственности[95].

Наиболее полно рекомендации ч. 1 ст. 6 Конвенции нашли отражение в УК Австрии, где в ч. 1 §126c криминализировано любое неправомерное использование компьютерной программы, обладающей характеристиками, указанными в Конвенции, для противоправного вмешательства в компьютерную систему[96] или совершения преступлений, приведённых в уже рассмотренных параграфах УК Австрии. В УК Швейцарии, Испании, Нидерландов, ФРГ такое чёткое и детализированное описание не содержится (ч. 2 ст. 144bis УК[97], ст. 350a УК Нидерландов[98], п.2 §202c(1) УК ФРГ[99], ст. 440 УК Испании). В Своде Законов США торговля похищенными или поддельными устройствами доступа криминализируется в случае, если они могут быть использованы в мошеннических целях[100].

Норма ч. 2 §126c УК Австрии, конкретизируя те же предметы, что и в п.ii ч. 1 ст.6 Конвенции, с помощью которых осуществляется преступное деяние по вмешательству в компьютерную систему или её часть, задаёт перечень действий по изготовлению, введению, распространению, продаже или

---

[93] Österreich: Das Strafgesetzbuch der Österreich 1974.
[94] USA: U.S. Code. Title 18. Part I. Chapter 47. §1030.
[95] Nederlanden: Wetboek van Strafrecht 1881.
[96] Österreich: Das Strafgesetzbuch der Österreich 1974.
[97] Schwitzerland: Das Strafgesetzbuch 1937.
[98] Nederlanden: Wetboek van Strafrecht 1881.
[99] Die BRD: Das Strafgesetzbuch der BRD.
[100] USA: U.S. Code. Title 18. Part I. Chapter 47. §1030.

иному предоставлению в доступ[101], что образует объективную сторону данного преступления. УК ФРГ в п. 2 §202c(1) запрещает использование паролей или защитных кодов, которые делают возможным несанкционированный доступ к данным[102]. В УК Нидерландов в п. b ч. 1 ст. 138 криминализируется использование технических средств, генерирующих ложные сигналы, ложные ключи или предоставляющие ложные полномочия[103].

К «чисто компьютерным» преступлениям, не упомянутым в Конвенции в национальных законодательствах, к примеру, швейцарском, относится в ст. 150bis производство и выпуск в обращение предметов, предназначенных для незаконной расшифровки кодированных материалов[104]. Во Франции криминализирован «компьютерный саботаж»[105].

Относительно близки к рекомендациям ст. 7 Конвенции нормы ст.210bis УК Бельгии[106] и §268 УК ФРГ. В УК Испании компьютерным подлогом считаются только аналогичные действия с информацией, составляющей личную тайну в электронных картотеках, архивах и реестрах[107].

В большинстве рассматриваемых государств компьютерное мошенничество (ст. 8) криминализировано, однако нормы большинства уголовных законодательств аналогичны и неполно отражают рекомендации Конвенции (§263a УК ФРГ, §148a УК Австрии, §286(2) УК Дании, ст.147 УК Швейцарии, ст.1 Главы 9 УК Швеции). Единственно, в Нидерландах компьютерным мошенничеством (ст. 232) признаётся фальсификация банковских карт для компьютерных денежных систем[108]. В Своде Законов США выделяется несколько составов по компьютерному мошенничеству: §1030(a)(4) даёт общее

[101] Österreich: Das Strafgesetzbuch der Österreich 1974.
[102] Die BRD: Das Strafgesetzbuch der BRD.
[103] Nederlanden: Wetboek van Strafrecht 1881.
[104] Schwitzerland: Das Strafgesetzbuch 1937 .
[105] France: Code pénal 1994.
[106] België: Strafwetboek 1867 [Elektronische bron]. − Toegangsmodus: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1867060801&table_name=wet, gratis (datum beroep: 23/02/2021).
[107] España: Código Penal 1995 [Recurso electrónico]. − Modo de acceso: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html, gratuito (fecha de acceso: 10/01/2021).
[108] Nederlanden: Wetboek van Strafrecht 1881.

описание компьютерного мошенничества, а §1030(a)(6) конкретизирует компьютерное мошенничество посредством торговли паролями[109].

В уголовных законодательствах ряда государств есть нормы, криминализирующие посягательства на коммерческую тайну посредством компьютерных технологий. К примеру, §263(3) УК Дании[110], ст.278 УК Испании[111].

Деяние, рекомендованное ст. 9 Конвенции криминализировано в значительной части государств, правда, конкретное содержание диспозиций уголовного законодательства по странам разнится. Владение и приобретение детской порнографии на настоящий момент криминализировано пока только в Швеции (ст.10a главы 16)[112], а распространение и изготовление – везде.

В такой именно формулировке, как предусмотрено ст. 10 Конвенции, пока в большинстве рассматриваемых государств данное деяние не криминализировано, а имеется, как правило, общий состав по нарушению авторских и смежных прав. Исключение составляет ст. 270 УК Испания[113].

Кроме указанных деяний, уголовное законодательство некоторых стран содержит нормы, согласно которым криминализируется ещё ряд деяний, связанных с киберсредой. Ст. 351 УК Нидерландов содержит специальный состав, вводящий санкцию за повреждение или разрушение компьютерных систем, связанных с национальной обороной, в УК Франции ст.411-6, 411-7, 411-8, 411-9 квалифицируют различные виды государственной измены с использованием компьютерных сетей, а ст.226-16, 226-17, 226-18, 226-19, 226-20, 226-21, 226-22, 226-23 криминализируют несанкционированные операции с персональными данными.

Таким образом, проведённый анализ показал, что принятие Будапештской Конвенции и присоединение к ней практически всех европейских стран с последующей ратификацией положительно отразилось на уголовном зако-

---

[109] USA: U.S. Code. Title 18. Part I. Chapter 47. §1030.
[110] Danmark: Straffeloven 1997.
[111] España: Código Penal 1995.
[112] Sverige: Straffbalken 1864.
[113] España: Código Penal 1995.

нодательстве европейских стран, поскольку, как показал проведённый анализ, идёт процесс реальной гармонизации законодательства в условиях роста транснациональных киберпреступлений.

При этом обратил на себя внимание и тот факт, что до настоящего момента не все рекомендации Конвенции были учтены на уровне национального законодательства, хотя из рассмотренных государств Конвенцию на настоящий момент ратифицировали все государства (Швеция – 28.04.2021 г., хотя присоединилась ещё в 2001 г.). На десять лет затягивался процесс ратификации Будапештской конвенции в Великобритании – это было связано с противоречиями между правительством, палатой общин и палатой пэров[114]. Свои нюансы есть и в других государствах. Однако судя по уголовному законодательству Австрии, Франции или ФРГ, присоединившихся к Конвенции ещё в 2001 году[115], а также США, процесс приведения национального законодательства к международным стандартам может быть вполне успешным.

А тот факт, что к Будапештской конвенции присоединилось ещё 22 государства мира, включая США, Канаду, Австралию, Израиль, Японию, а девять государств на настоящий момент рассматривают вопрос о присоединении к Будапештской конвенции, придаёт настоящему документу глобальный характер и превратил Будапештскую конвенцию в основное международное соглашение по гармонизации уголовного законодательства государств мира.

Единственным государством - членом Совета Европы, не присоединившимся к Будапештской конвенции, на настоящий момент является Россия (Белоруссия, также не присоединившаяся к Конвенции, не член Совета Европы). Вопрос о присоединении к Конвенции в России был поднят в 2005 г., однако президент РФ отказался от интеграции России в международное со-

[114] Эмм, Д. Киберпреступность и закон: обзор положений законодательства Великобритании, касающегося компьютерных преступлений.

[115] Таблица подписей и ратификации договора 185 «Конвенция о компьютерных преступлениях». Статус на 15/05/2021.

общество[116], противодействующее киберпреступности. Одной из претензий в области уголовного права был тезис о том, что Будапештская конвенция давно устарела, поскольку прогресс IT привёл к появлению новых общественно опасных деяний в киберсфере, которые не учитываются Конвенцией[117]. Однако, как указывают специалисты, с формально-юридической точки зрения, «устаревание» нормативного уголовно-правового акта происходит тогда, когда криминализированное деяние прекратило быть общественно опасным либо прекратило совершаться злоумышленниками, или его совершение по объективным причинам стало невозможным[118]. Если же рассматривать рекомендации Будапештской конвенции (включая Страсбургский протокол) с этой точки зрения, то следует, прежде всего, констатировать, что ни одна из рекомендаций не соответствует указанным выше условиям, и все рекомендации актуальны в связи с тем, что деяния, предлагаемые к криминализации, продолжают сохранять общественную опасность, степень которой неуклонно повышается.

## 2.3. Особенности процесса гармонизации уголовного законодательства стран - членов СНГ по противодействию киберпреступности

### 2.3.1. Рекомендации по уголовно-правовому противодействию киберпреступности на уровне СНГ

[116] Распоряжение президента РФ «О признании утратившим силу распоряжения президента Российской Федерации от 15 ноября 2005 г. №557-рп «О подписании конвенции о киберпреступности» 22 марта 2008 г. №144-рп [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=417185;fld=134;dst=100006;rnd=0.6502687247211727 (дата обращения: 23.07.2020).

[117] «Без договоренностей глобального характера эту проблему не решить»: Глава нового департамента МИД РФ Андрей Крутских о конфронтации в интернете [Электронный ресурс] // Газета «Коммерсантъ». – 2020. – 25.02. – №33. – С. 6. – Режим доступа: https://www.kommersant.ru/doc/4267456 (дата обращения: 27.10.2020).

[118] Трофимцева, С.Ю. Международное уголовно-правовое противодействие киберпреступности: к вопросу об «устаревании» Будапештской конвенции. – С. 23.

Развитие IT-технологий постепенно доходило и до Советского Союза, и, несмотря на всю техническую и технологическую отсталость, первое преступление подобного рода в СССР официально было зарегистрировано в 1979 г. в г. Вильнюсе, ущерб, нанесённый государству, составил 78 584 рубля, что было занесено в международный реестр киберпреступлений[119].

К началу 1990-х гг. данная проблема, наконец, была осмыслена законодателем сначала на уровне Российской Федерации, и в 1996 году был принят и с 01.01.1997 года вступил в силу Уголовный кодекс РФ, в котором компьютерные преступления были объединены в Главу 28 «Преступления в сфере компьютерной информации»: ст.272 «Неправомерный доступ к компьютерной информации», ст.273 «Создание, использование и распространение вредоносных программ для ЭВМ», ст.274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети».

Параллельно Россия инициировала гармонизацию законодательства созданного в декабре 1991 года Содружества независимых государств, и в феврале 1996 года на VII пленарном заседании Межпарламентской Ассамблеи государств - участников СНГ был принят Модельный уголовный кодекс как рекомендательный акт для СНГ (далее – Модельный кодекс), XII раздел которого включал в себя главу 30 «Преступления против информационной безопасности», где объектом преступных посягательств выступает безопасность информационных отношений[120], а ещё часть составов, имеющих отношение к компьютерным технологиям, включено в Раздел XI «Преступления против собственности и порядка осуществления экономической деятельности», где, соответственно, объектом преступления выступают отношения собственно-

[119] Батурин, Ю.М. Проблемы компьютерного права / Ю.М. Батурин. –М.: Юрид. лит., 1991. – С. 126.

[120] Трофимцева, С.Ю. Международное противодействие киберпреступности: сравнительный анализ рекомендаций Будапештской конвенции и законодательства СНГ в области уголовного права / С.Ю. Трофимцева // Евразийский юрид. журнал. – 2020. – С.48.

сти и безопасность экономической деятельности[121]. В июне 2001 года было подписано Минское «Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», которое включает в себя рекомендации по криминализации некоторых деяний в киберсфере (ст. 3): (а) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети; б) создание, использование или распространение вредоносных программ; в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия; г) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб; а также рекомендации по международному сотрудничеству и обмену данными при расследовании киберпреступлений[122].

При анализе рекомендуемых к криминализации составов киберпреступлений, обращает на себя внимание несколько моментов.

Прежде всего, несанкционированный доступ к компьютерной информации (ст. 286 Модельного кодекса) рекомендуется криминализировать только в случае наступления материальных последствий в виде нарушения системы защиты и повлекший «изменение, уничтожение либо блокирование информации, а равно вывод из строя компьютерного оборудования либо

[121] Трофимцева, С.Ю. Международное противодействие киберпреступности: сравнительный анализ рекомендаций Будапештской конвенции и законодательства СНГ в области уголовного права. С.49.

[122] Соглашение «О сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», Минск, 01.06.2001 [Электронный ресурс] // СПС «Гарант». – Режим доступа: https://base.garant.ru/12123778/, ограниченный (дата обращения: 11.02.2021).

иной значительный ущерб»[123], что предполагает, в отличие от рекомендаций Будапештской конвенции, оставление безнаказанным злоумышленника, вошедшего с компьютерную систему, пребывающего в ней без прав или превысившего права доступа. Кроме того, в Модельном кодексе рекомендуется к криминализации данное деяние, совершённое по неосторожности.

Предумышленное воздействие на компьютерные данные в Модельном кодексе разделено по ст. 287 «Модификация компьютерной информации», ст. 288 «Компьютерный саботаж» и ст. 289 «Неправомерное завладение компьютерной информацией», а в Конвенции воздействие на данные как умышленное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных, объединяется в одну статью (ст. 4)[124]. В Кодексе вводятся разные составы по модификации как изменению информации, но к этому присоединён компьютерный подлог (ст. 287), а копирование информации соединено с её перехватом и (ст. 289) (последнее не может быть компьютерным преступлением), а изменение, уничтожение, блокирование может считаться преступлением только при совершении по его неосторожности в случае доказанности факта несанкционированного доступа[125] (далее – НСД) (ст. 286)[126], а при наличии намерения в наступлении указанных последствий при НСД данное деяние, вероятно, общественно опасным не является, что у исследователей вызывает недоумение в адекватности нормы реалиям[127].

Совершение указанных действий с информацией без факта НСД Модельным кодексом рекомендуется к криминализации в ст. 288, которая поче-

---

[123] Модельный уголовный кодекс СНГ. (Рекомендательный законодательный акт для СНГ) (Постановление № 7-5 от 17.02.1996) [Электронный ресурс] // Консорциум-кодекс: Электронный фонд правовой и нормативной документации. – Режим доступа: http://docs.cntd.ru/document/901781490 (дата обращения: 20.02.2021).

[124] Convention Committee on Cybercrime ETS No 185, Budapest, 23/11/2001.

[125] Модельный уголовный кодекс СНГ.

[126] Оба состава без подлога и перехвата объединены в п. а) ст. 3 Минского соглашения, при этом рекомендуется криминализация только при наличии прямого умысла.

[127] Трофимцева, С.Ю. Международное противодействие киберпреступности: сравнительный анализ рекомендаций Будапештской конвенции и законодательства СНГ в области уголовного права. – С.48.

му-то называется «Компьютерный саботаж»[128]. По поводу объединения копирования информации с её перехватом во время передачи по каналам связи, то, по мнению специалистов, с одной стороны, два этих деяния объединяет сходный результат, а с другой, различается способ совершения деяния[129]. Что касается перехвата, то, как указывают специалисты, такое действие предполагает вмешательство в канал связи[130], а съёма электромагнитных излучений и наводок (ПЭМИН) в принципе нет законодательстве СНГ, чем открывается ещё одна возможность для злоумышленника остаться безнаказанным[131].

Рекомендация по криминализации создания (разработке), использованию и распространению вредоносных программ содержится в ст. 291 Модельного кодекса и п. б) ст. 3 Минского соглашения, что имеет некоторые параллели с рекомендациями Будапештской конвенции. Однако, как указывают специалисты, в Модельном кодексе есть диспозиция, включающая в себя изготовление и использование специальных средств для НСД к компьютерной системе (ст. 290). В ст. 5, 6 Будапештской конвенции, во-первых, рекомендуются к криминализации не указанные выше только деяния, но и в ст. 5 умышленное создание серьезных помех функционированию компьютерной системы путём введения данных или воздействия на данные[132], поскольку вследствие этих деяний выступает не непосредственное нарушение статуса компьютерной информации (как следует из рекомендаций Модельно-

[128] Анализ данной рекомендации см. подробнее: Трофимцева, С.Ю., Илюшин, Д.А. Некоторые аспекты квалификации компьютерных преступлений в Российской Федерации и Республике Казахстан / С.Ю. Трофимцева, Д.А. Илюшин // Құқықтық жүйенің қазіргі кездегі дамуының негізгі бағыттары және болашағы: Қазақстан тәуелсіздігінің 25-жылдығына арналған халықаралық ғылыми-тәжірибелік конференцияның материалдары (Алматы, «Тұран» университеті, 1 қараша 2016ж.). – Алматы, «СаГа», 2017. – С.142.

[129] Трофимцева, С.Ю. Международное противодействие киберпреступности: сравнительный анализ рекомендаций Будапештской конвенции и законодательства СНГ в области уголовного права. – С.47.

[130] Трофимцева, С.Ю. Международное противодействие киберпреступности: сравнительный анализ рекомендаций Будапештской конвенции и законодательства СНГ в области уголовного права. – С.47.

[131] Трофимцева, С.Ю. Международное противодействие киберпреступности: сравнительный анализ рекомендаций Будапештской конвенции и законодательства СНГ в области уголовного права. – С.48.

[132] Convention Committee on Cybercrime ETS No 185.

го кодекса), а сбой в работе компьютерной системы, что в законодательстве СНГ не отражено[133]. Следует также отметить, что рекомендации ст. 6 Будапештской конвенции намного шире, в том числе, включающие использование «компьютерных паролей, кодов доступа или иных аналогичных данных» для получения неправомерного доступа к системе[134]. При этом специалисты обращают внимание на то, что в Конвенции содержатся ссылки на случаи, исключающие преступный характер деяния, чего нет в рекомендациях компьютерного законодательства СНГ.

При этом анализ показывает, что в модельное законодательство СНГ был введён состав, рекомендующий криминализировать нарушение правил эксплуатации компьютерной системы или сети (ст. 292 Модельного кодекса, п. в) ст. 3 Минского соглашения), то аналогично ст. 274 УК РФ. Данная диспозиция достаточно давно вызывает критику у специалистов. Как считает Н.П. Яблоков, в организации должны существовать два основных вида правил эксплуатации компьютеров, которыми должны руководствоваться в своей деятельности лица, работающие с компьютерами: инструкции по работе с компьютерами и машинными носителями информации, разработанные изготовителем ЭВМ и периферийных технических устройств, поставляемых вместе с данным экземпляром ЭВМ; правила, установленные собственником или владельцем информационных ресурсов, информационных систем, технологий и средств их обеспечения, определяющие порядок пользования ЭВМ, системы ЭВМ и сети ЭВМ, а также иными машинными носителями информации[135]. По мнению У.В. Зининой, даже если такие документы существуют в организации, при приеме на работу никто сотрудника не знакомит, поэтому,

---

[133] Трофимцева, С.Ю. Международное противодействие киберпреступности: сравнительный анализ рекомендаций Будапештской конвенции и законодательства СНГ в области уголовного права. – С.47.

[134] Convention Committee on Cybercrime ETS No 185.

[135] Convention Committee on Cybercrime ETS No 185.

как утверждает У.В. Зинина, субъекту нельзя вменить в вину нарушение каких-либо правил, поскольку лицо даже не знало о их существовании[136].

Из преступлений, связанных с компьютерами, в Кодексе рекомендуется к криминализации хищение, совершённое с использованием компьютерной техники (ст. 243)[137], отсутствующее в Будапештской конвенции. Данную рекомендацию можно рассматривать как квалифицированный состав соответствующих уголовных норм, криминализирующих хищений (вероятнее всего, кражу), где компьютер, сети, системы и технологии выступают в качестве средства совершения хищения. Аналогичное заключение можно дать в отношении рекомендации ст. 269 Модельного кодекса «Незаконное получение информации составляющей коммерческую или банковскую тайну».

Ст. 250 Модельного кодекса вызывает вопросы к формулировке диспозиции, поскольку рекомендует криминализовать «причинение значительного имущественного ущерба собственнику или иному владельцу имущества путём обмана или злоупотребления доверием» либо путём модификации компьютерной информации, но при этом должны отсутствовать признаки хищения или иного завладения чужим имуществом[138]. Данную диспозицию можно рассматривать как частичный аналог ст. 8 Будапештской конвенции «Мошенничество с использованием компьютерных технологий», поскольку в уголовной практике (что нашло отражение и в УК РФ) мошенничество предполагает как причинение имущественного ущерба, так и «хищение чужого имущества или приобретение права на чужое имущество»[139].

А весьма приблизительным аналогом ст. 10 «Правонарушения, связанные с нарушением авторского права и смежных прав» Будапештской конвенции является рекомендация п. г) ст. 3 Минского соглашения, поскольку ре-

---

[136] Зинина, У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. – С.26.

[137] Модельный уголовный кодекс СНГ.

[138] Модельный уголовный кодекс СНГ. (Рекомендательный законодательный акт для СНГ).

[139] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 30.04.2021).

комендации Минского соглашения сужены, и предметом посягательств выступают компьютерные программы и базы данных[140], тогда как в диспозиции ст. 10 Конвенции содержится бланкетная норма, и предметом преступных посягательств выступает любой объект авторских или смежных прав, защищаемый международным законодательством[141].

Таким образом, проделанный анализ делает очевидным тот факт, что рекомендации Будапештской конвенции в области материального права являются более адекватными реальному совершению киберпреступлений, и использование её рекомендаций государствами мира позволит эффективнее гармонизировать их законодательство.

### 2.3.2. Особенности процесса гармонизации уголовного законодательства стран - членов СНГ

Итак, как было рассмотрено выше, действующие в СНГ на настоящий момент документы – это Модельный уголовный кодекс СНГ (1996 г.) и Минское соглашение о сотрудничестве, и государства, ратифицировавшие их, должны внести изменения во внутреннее уголовное право, включая Украину (член СНГ по 2018 г.) и Грузию (член СНГ с 1996 по 2009 г.). В этой связи необходимо провести анализ процесса гармонизации.

По мнению исследователей, членов СНГ можно разделить на группы от стран, максимально реализовавших рекомендации, до стран, практически абсолютно их проигнорировавших[142].

К первой группе исследователи относят Белоруссию, Армению и Таджикистан, аргументируя тем, что они наиболее полно воплотили рекомендации по криминализации компьютерных преступлений (гл. 30 разд. XII Мо-

[140] Соглашение «О сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации».

[141] Vid.: Convention Committee on Cybercrime ETS No 185.

[142] Трофимцева, С.Ю. Проблемы гармонизации уголовного законодательства стран СНГ в области противодействия киберпреступности / С.Ю. Трофимцева // Евразийский юридический журнал. – 2020. – №10(149). – С.31.

дельного кодекса[143] и ч. 1 ст. 3 Минского соглашения[144]). Так, реализация ст. 286 Кодекса реализована почти полностью в ст. 349-355 УК Белоруссии[145]. А ст. 289 Кодекса реализована частично: в ст. 352 не включены квалифицирующие обстоятельства, связанные с шантажом, что свидетельствует о немеханическом копировании рекомендаций законодательства СНГ. Армянский законодатель проигнорировал лишь рекомендацию только ст. 286 Модельного кодекса: диспозиция ст. 251 УК Армении[146] превращена в аналог ст. 2 Будапештской конвенции. Таджикский законодатель расширил диспозицию рекомендованной Кодексом ст. 286 в ст. 298 УК Таджикистана, где общим составом стали несанкционированные воздействия на информацию в результате НСД, а материальные последствия вынесены в квалифицированный состав ст. 298[147], что оптимальнее рекомендаций законодательства СНГ.

В ст. 181 уголовного закона Армении нашла отражение ст. 243 Модельного кодекса. В УК Белоруссии в ст. 212 по объективной стороне соединяется хищение с помощью изменения компьютерной информации (ст. 243 Кодекса) и хищение посредством компьютерного подлога (ст. 287 Кодекса) без криминализации компьютерного мошенничества (ст. 250 Модельного кодекса). УК Таджикистана, игнорируя рекомендации ст. 243 и ст. 250 Модельного кодекса, в ст.277 включил (аналогично ст. 199 УК Армении) рекомендацию ст. 269 Модельного кодекса[148]. Этой нормы в УК Белоруссии нет.

---

[143] Модельный уголовный кодекс СНГ.

[144] Соглашение «О сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации».

[145] Уголовный кодекс Республики Беларусь, 9 июля 1999 г. № 275-З [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=Hk9900275 (дата обращения: 25.11.2020).

[146] Уголовный кодекс Республики Армения от 29.04.2003 г. ЗР-528 [Электронный ресурс]. – Режим доступа: https://www.legislationline.org-download-id-8237-file-Armenia_CC_am2016_ru.pdf (дата обращения: 25.12.2020).

[147] Уголовный кодекс Республики Таджикистан от 13.11.1998 г. № 684 [Электронный ресурс]. – Режим доступа: https://www.legislationline.org-download-id-8601-file-Tajikistan_CC_1998_am2020_ru.pdf (дата обращения: 25.12.2020).

[148] Уголовный кодекс Республики Таджикистан от 13.11.1998 г.

По мнению исследователей, вторую группу составляют Казахстан, Киргизия, Туркмения и Узбекистан[149]. В их уголовных законах рекомендации реализованы фрагментарно, при этом нормы этих государств содержат ряд сходных норм, не представленных в рекомендациях для СНГ – это факт гармонизации «снизу»[150], хотя норма ст. ч. 1 ст. 304 УК Киргизии[151], ч. 1, 2 ст. 298 УК Таджикистана[152] очень близки по формулировке к ст. 286 Кодекса. В ст. 278.3 УК Узбекистана запрещается не только неправомерный доступ к информации, находящейся во всей компьютерной системе, но также и в её частях[153], что шире, чем предложенный Модельным кодексом вариант. Уголовное законодательство Казахстана и Туркменистана сближает то, что криминализируется сам факт НСД без ссылки на наступление материальных последствий. При этом ч. (1) ст. 333 УК Туркменистана НСД рассматривается как преступный, если имело место нарушение прав и законных интересов субъектов[154], и схожа формулировка представлена в ч. 1 ст. 205 УК Казахстана[155]. В ч. 1 ст. 304УК Киргизии[156] НСД криминализируется при наличии материальных последствий, но при этом их законодатель (как и ч. 1 ст. 287.2 УК Узбекистана) и устанавливает только прямую форму вины, что отличается от рекомендаций ст. 286 Кодекса. В ч. 1 ст. 287.2 УК Узбекистана[157] от-

---

[149] Трофимцева, С.Ю. Проблемы гармонизации уголовного законодательства стран СНГ в области противодействия киберпреступности. – С.31.

[150] Трофимцева, С.Ю. Проблемы гармонизации уголовного законодательства стран СНГ в области противодействия киберпреступности. – С.31.

[151] Уголовный кодекс Кыргызской Республики от 22.12.2016 г. [Электронный ресурс]. – Режим доступа: https://www.legislationline.org-download-id-8264-file-Kyrgyzstan_CC_2016_am2019_ru.pdf (дата обращения: 25.12.2020).

[152] Уголовный кодекс Республики Таджикистан от 13.11.1998 г.

[153] Уголовный кодекс Республики Узбекистан от 22.09.1994 г. [Электронный ресурс]. – Режим доступа: https://www.legislationline.org-download-id-8565-file-Uzbekistan_CC_1994_am012020_ru.pdf (дата обращения: 25.12.2020).

[154] Уголовный кодекс Туркменистана от 12.06.1997 г. [Электронный ресурс]. – Режим доступа: https://www.legislationline.org-download-id-8316-file-Turkmenistan_CC_2010_am2019_en.pdf (дата обращения: 25.12.2020).

[155] Уголовный кодекс Республики Казахстан от 03.07.2014 г. [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/m/document?doc_id=31575252 (дата обращения: 25.12.2020).

[156] Уголовный кодекс Кыргызской Республики, 22.12.2016 г.

[157] Уголовный кодекс Республики Узбекистан от 22.09.1994 г.

дельным составом идёт НСД к сети и неправомерное использование такой системы, включая пропуск трафика (ст. 287.6), что представляет интерес для государств[158]. Это позволит убрать недоработку Кодекса.

Рекомендации ст. 290 и ст. 291 Кодекса реализованы в ст. 210 УК Казахстана, ст. 305 УК Киргизии, ст. 335 УК Туркмении, ст. 278.6 УК Узбекистана. Ст. 287 Кодекса нашла частичное (без подлога) отражение в ст. 206 УК Казахстана, ст. 287.4 УК Узбекистана, ст. 334 УК Туркмении. В ст. 334 УК Туркмении есть значимое дополнение – «изменения формата» компьютерной информации, что, с одной стороны, разновидность изменения информации, но с другой, облегчает работу по квалификации преступления следователем.

Рекомендация ст. 289 Модельного кодекса была учтена в Казахстане и Туркмении. В УК Казахстана состав разделён на две: в ч. 1 ст. 208 получение информацией путём копирования, перехвата и т. д., при этом обязательным является нарушение прав потерпевших, и ст. 209, где криминализирован шантаж потерпевших с целью получения компьютерной информации[159], что более рационально, чем УК Туркмении, где указанные деяния представляют собой общий и квалифицированный состав ст. 334.2[160]. Весьма позитивным является вариант в УК Казахстана и УК Узбекистана нормы компьютерного саботажа: в отличие от ст. 288 Модельного кодекса, где термин «саботаж» употреблён в несвойственном языку значении как несанкционированные воздействия на информацию и компьютерную систему (аналог только ст. 306 УК Киргизии), под компьютерным саботажем здесь понимается умышленное действие (бездействие), направленное на нарушение работы (вывод из строя) системы или сети (ст. 207 УК Казахстана, ст. 287.5 УК Узбекистана).

Нормы ст. 290 и ст. 292 Кодекса, а также пп. в), г) ст. 3 Минского соглашения в УК этой группы государств не представлены (ст. 287.3 кроме УК Узбекистана, близкой к ст. 290 Кодекса). В отношении ст. 292 Модельного

---

[158] Трофимцева, С.Ю. Проблемы гармонизации уголовного законодательства стран СНГ в области противодействия киберпреступности. – С.31.

[159] Уголовный кодекс Республики Казахстан от 03.07.2014 г.

[160] Уголовный кодекс Туркменистана от 12.06.1997 г.

кодекса эту ситуацию можно считать рациональной. Но игнорирование рекомендаций ст. 290 Кодекса вряд ли будет рациональным и обоснованным.

Следует отметить, что региональная гармонизация уголовного законодательства данных государств привела к появлению в их УК норм, не имеющих аналогов в модельном законодательстве СНГ. К примеру, в ст. 211 УК Казахстана и ст. 335.1 УК Туркмении есть состав по запрету распространения персональных данных ограниченного доступа. Ст. 188.1 УК Узбекистана, ст. 214 УК Киргизии запрещает незаконное привлечение денег или организацию финансовых пирамид, ст. 278 УК Узбекистана, ст. 212 УК Киргизии – азартных игр с использованием информационных технологий, что обусловлено спецификой криминальной ситуации. Избыточны нормы ст. 213 УК Казахстана и ст. 353.3 УК Туркмении в связи с устареванием технологий[161].

Третью группу государств образуют значительно или почти полностью проигнорировавшие рекомендации законодательства СНГ: Молдавия, Азербайджан, Грузия и Украина[162]. По мнению исследователей, это может быть связано с тем, что данные государства ратифицировали Будапештскую конвенцию, и по этой причине процесс гармонизации законодательства был направлен именно в эту область.

В Уголовном кодексе Российской Федерации, несмотря на то, что именно она инициировала и Модельный кодекс, и Минское соглашение, из рекомендаций модельного законодательства СНГ не учтена ни одна. Сходными по составу со ст. 291 и ст. 292 Модельного кодекса и п. г) ст. 3 Минского соглашения являются ст. 273 и ст. 274 соответственно, однако они были введены в российское уголовное законодательство до принятия Модельного кодекса СНГ. Статья 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» была введена в УК до принятия Модельного кодекса СНГ, действует в редакции Федерального за-

[161] См. подробнее: Трофимцева, С.Ю., Илюшин, Д.А. Некоторые аспекты квалификации компьютерных преступлений в РФ и Республике Казахстан. – С. 144.

[162] Трофимцева, С.Ю. Проблемы гармонизации уголовного законодательства стран СНГ в области противодействия киберпреступности. – С.31.

кона от 07.12.2011 №420-ФЗ и устанавливает санкции за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации[163].

Исходя из диспозиции, объективная сторона состоит в создании вредоносной компьютерной программы и в её использовании и распространении. Эта формулировка вызывает вопросы у специалистов. Прежде всего, введение в УК понятия «вредоносная компьютерная программа» требует ссылки на нормативный акт, определяющий границы между обычной и «вредоносной» программой. Сейчас в РФ подобных актов нет. С субъективной стороны, по мнению большинства исследователей, преступление совершается по прямому умыслу. Но, по мнению В.С. Пущина, речь идёт о двух формах вины: как умышленной, так и неосторожной[164]. С данной позицией нельзя согласиться, т. к. в диспозиции на деяние по неосторожности не указано, речь может идти только об прямой вине. В единственном Постановлении Пленума Верховного суда РФ, как-то касающимся киберпреступлений, от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» указано, что, когда эти деяния «сопряжены с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для электронно-вычислительных машин, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по статье 159 УК РФ, а также, в зависимости от обстоятельств дела, по статьям 272 или 273 УК РФ, если в результате неправомерного доступа к компьютерной информации произошло уничтожение, блокирование, модификация либо копирование информации, наруше-

[163] Уголовный Кодекс Российской Федерации.

[164] Пущин, В.С. Преступления в сфере компьютерной информации [Электронный ресурс] / В.С. Пущин (дата обращения: 14.01.2021).

ние работы ЭВМ, системы ЭВМ или их сети»[165]. Исходя из данного разъяснения, можно заключить, что если деяние совершено из корыстной заинтересованности, но признаков состава преступления по ст. 159.6 или, к примеру, по ст. 183 (что несколько проще) не обнаружено, деяние следует квалифицировать по ч. 2 ст. 272 УК РФ. Разъяснения Пленума Верховного суда о порядке правоприменительной практики именно по ст.273 отсутствуют.

Статья 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» действует в редакции Федерального закона от 07.12.2011 №420-ФЗ и устанавливает санкции за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо инфотелекоммуникационных сетей и оконечного оборудования и правил доступа к инфотелекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб[166]. Данную статью, как уже указывалось выше, специалисты и сами сотрудники правоохранительных органов, в частности, отдела «К» считают «мёртвой», поскольку дела по ней не возбуждаются. Нормативных правил эксплуатации компьютера в России нет, сопроводительная документация и технические регламенты предприятия, согласно ст.8 Трудового кодекса РФ[167], нормативными актами не являются, поэтому найти признаки состава преступления не представляется возможным.

Частично в УК РФ реализована рекомендация ст. 250 Модельного кодекса СНГ – в 2012 г. в уголовный закон была введена ст. 159.6 «Мошенничество в сфере компьютерной информации». Однако её диспозиция значительно шире, нежели чем в рекомендациях Модельного кодекса: ч. 1 ст.159

---

[165] Постановление Пленума Верховного Суда РФ, касающимся компьютерных преступлений, от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. – 2008. – 12 января. – Вып.4.

[166] Уголовный Кодекс Российской Федерации.

167 Трудовой кодекс Российской Федерации от 30.12.2001 # 197-ФЗ (ред. от 30.04.2021) (с изм. и доп., вступ. в силу с 01.05.2021) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 13.05.2021).

компьютерным мошенничеством считает именно хищение чужого имущества или приобретение права на чужое имущество[168].

Остальные рекомендации как Модельного кодекса СНГ, так и, тем более, Минского соглашения, Россия игнорирует в полном объёме, что, по мнению исследователей, может быть причиной отказа стран - членной СНГ не только подписать, но и даже рассматривать предложенный Россией в 2011 г. проект Конвенции об обеспечении международной информационной безопасности, правда, не содержащий ни одной нормы уголовного права[169].

## Выводы по 2 главе

Итак, на основе проделанного анализа в настоящей работе было доказано, что экспонентный рост злонамеренных общественно опасных деяний в киберсфере вкупе с осознанием их транснационального характера привели уже не только внутреннего законодателя, но и международное сообщество к необходимости начать процесс гармонизации уголовного права. При этом, как было показано в работе, на уровне ООН был установлен статус защищаемой информации и возложена ответственность на государства по углублению международного сотрудничества в области противодействия киберпреступности, а МОУП Интерпол была разработана первая официальная классификация киберпреступлений.

Наиболее эффективными и адекватными общественной опасности киберпреступлениям можно считать принятую Советом Европы Будапештскую конвенцию по киберпреступлениям (2001 г.), поскольку, как было рассмотрено в работе, она содержит рекомендации по гармонизации, прежде всего, норм уголовного права, позволяющие адекватно противостоять киберпреступности в начале XXI века, которые, после ратификации Будапештской

[168] Уголовный кодекс Российской Федерации.

[169] Трофимцева, С.Ю. Проблемы гармонизации уголовного законодательства стран СНГ в области противодействия киберпреступности. – С.31.

конвенции (на настоящий момент – 66 государствами всего мира), обязаны быть инкорпорированы во внутреннее законодательство.

Однако проделанный анализ показал, что, несмотря на реальность общественной опасности киберпреступности, во-первых, затянулся процесс её подписания и ратификации как со стороны европейских государств, так и со стороны неевропейских стран. Тем не менее, анализ уголовного законодательства в киберсфере европейских стран показал, что ратификация Будапештской конвенции далеко не всегда ускоряет процесс работы внутреннего законодателя над гармонизацией уголовных норм. Очевидно, что процесс недостаточно быстро, но движется, что позитивно влияет на повышение уровня уголовно-правового противодействия транснациональной киберпреступности, и процесс приведения национального законодательства к международным стандартам может быть вполне успешным.

Анализ модельного законодательства СНГ (Модельного кодекса СНГ и Минского соглашения) показал, что модельное законодательство не содержит часть составов, имеющих место в Будапештской конвенции (ст. 2, 5, 7, 9), что уже можно считать реальной уязвимостью. Кроме того, формулировки части составов вызывают некоторое недоумение (ст. 287, 289, 250 Модельного кодекса), или содержат заведомо неисполнимые требования (ст. 292 Модельного кодекса).

Анализ реализации рекомендаций модельного законодательства СНГ был проведён по трём основным группам государств СНГ, где в первой группе (Белоруссию, Армения и Таджикистан) рассматривались государства, максимально инкорпорировавшие рекомендации в своё внутренне уголовное право, во второй группе (Казахстан, Киргизия, Туркмения и Узбекистан) государства учли рекомендации лишь частично, при этом провели региональную гармонизацию уголовных норм в области противодействия киберпреступности. Государства третьей группы (Молдавия, Азербайджан, Грузия (по 2009 г.), Украина (по 2018 г.) и Россия) значительно или почти полностью проигнорировали рекомендации законодательства СНГ.

Таким образом, как показал анализ, в законодательстве западных стран, права субъектов информационных отношений можно считать более защищёнными, чем в государствах СНГ, где ряд действий злоумышленников по посягательствам на компьютерную информацию, остаются безнаказанными по причине наличия пробелов как в модельном законодательстве СНГ, так и в российском законодательстве.

В этой связи российскому законодателю рекомендуется ратифицировать Будапештскую конвенцию, в результате чего, возможно, в уголовное законодательство России, наконец, будут введены новые составы по компьютерным преступлениям и преступлениям, связанным с компьютерами.

# ГЛАВА 3. ОСОБЕННОСТИ АДМИНИСТРАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРОЦЕССА ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ НА МЕЖГОСУДАРСТВЕННОМ УРОВНЕ

## 3.1. Сравнительный анализ административно-правовых мер европейского законодательства и законодательства СНГ

Итак, как показало проведённое в настоящей работе исследование, киберпреступления относятся к наиболее сложным в плане квалификации деяниям, при этом киберпреступления относятся и к наиболее сложным и в плане расследования. Согласно некоторым данным, в ведущих зарубежных странах в 80-90-е гг. раскрывалось только 10% из зарегистрированных преступлений: в Великобритании из 270 зарегистрированных киберпреступлений за 5 лет были расследованы только 6; в ФРГ в 1987 г. было выявлено 2777 случаев аналогичных преступлений, расследовано только 170[170]. В начале XXI века ситуация принципиально в позитивном направлении пока не развивается, что связано как с отставанием уголовного законодательства от спектра злоумышленных посягательств, так и рядом проблем, возникших перед следственными органами государств.

Если рассматривать меры административного характера при уголовно-процессуальном противодействии киберпреступности, то в настоящей работе представляется необходимым проведение сравнительного анализа рекомендаций Будапештской конвенции и Минского соглашения СНГ.

Осознавая проблемы при расследовании транснациональных киберпреступлений, ст. 22 Будапештской конвенции устанавливает *юрисдикцию* каждой стороны: её территория, борт судна под её флагом, борт воздушного судна, зарегистрированного по её законам, совершение уголовно наказуемого в месте его совершения преступления одним из её граждан, или если это правонарушение совершено за пределами территориальной юрисдикции какого-

[170] Вехов, В.Б. Компьютерные преступления. способы совершения методики расследования [Электронный ресурс] / В.Б. Вехов. – М., 1996. – Режим доступа: http://www.pravo.vuzlib.org/book_z404_page_1.html (дата обращения: 27.12.2020).

либо государства (пп. a-d) ч. 1 ст. 22)[171]. Аналогичные рекомендации в Минском соглашении отсутствуют.

*Печень мер* по противодействию киберпреступности можно разделить на *две группы*: меры внутреннего характера (обязательства, соблюдаемые при проведении внутренних расследований), меры в области международного сотрудничества сторон.

Первая группа мер. Минское соглашение требует составить *перечень компетентных органов* и передать его другим сторонам (ч. 2 ст. 4)[172]. П. c) ч. 2 ст. 27 Будапештской конвенции вводит сходную норму, а также требует передачу списка Генеральному секретарю Совета Европы, который, на основании п. d) ч. 2 ст. 27, постоянно обновляет реестр таких органов[173].

Следует отметить, что европейское сообщество при составлении рекомендаций в области процессуального права исходило из осознания того, что в виртуальной среде следы преступления не сохраняются, в связи с чем ст. 16 Конвенции ввела требование об *оперативном обеспечении* в течение 90 дней (ч. 2 ст. 16) *сохранности компьютерных данных* и данных о потоках информации, поскольку такие данные подвержены риску утраты или изменения (ч. 1 ст. 16)[174], при этом ст. 17 требует обеспечения такой сохранности от всех поставщиков услуг (п. a) ч. 1 ст. 17) для оперативного раскрытия информации при расследовании киберпреступления (п. b) ч. 1 ст. 17)[175]. Для реализации этого каждая сторона должна принять законодательные акты, закрепляющие за компетентными органами полномочия отдавать распоряжения на её территории лицу (п. a) ч. 1 ст. 18) или поставщику услуг (п. b) ч. 1 ст. 18), а на основе таких данных должна быть возможность установить: a) вид используемой коммуникационной услуги (п. a) ч. 3 ст. 18), личность пользова-

[171] Convention Committee on Cybercrime ETS No 185.

[172] Соглашение «О сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», Минск, 01.06.2001.

[173] Convention Committee on Cybercrime ETS No 185.

[174] Convention Committee on Cybercrime ETS No 185.

[175] Convention Committee on Cybercrime ETS No 185.

теля, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание (п. b) ч. 3 ст. 18), любые другие сведения о месте установки коммуникационного оборудования, имеющиеся в соглашении или договоре на обслуживание (п. c) ч. 3 ст. 18)[176]. Аналогичных рекомендаций в Минском соглашении нет.

Кроме того, Будапештская конвенция требует принять *меры по наделению компетентных органов полномочиями по перехвату компьютерных данных*: собирать или записывать данные на своей территории, с применением технических средств (п. a) ч. 1 ст. 21), и обязать поставщика услуг в пределах его технических возможностей: собирать или записывать с использованием технических средств компьютерные данные и сотрудничать с компетентными органами и помогать им в сборе или записи в режиме реального времени данных о содержании указанных сообщений на её территории, передаваемых с помощью компьютерных систем (п. b) ч. 1 ст. 21)[177].

Кроме того, как было неоднократно отмечено, в том числе, в рамках настоящей работы, следы преступления в виртуальной среде быстро исчезают, Будапештская конвенция предлагает сторонам принять *меры по созданию возможности сбора информации с применением технических средств в реальном времени*, предполагающие фиксирование компетентными органами информации на своей территории (п. a) ч. 1 ст. 20), а также наложение обязанностей на поставщика услуг собирать или записывать информацию на территории стороны и сотрудничать с компетентными органами, помогать им собирать или записывать в реальном режиме времени данные о потоках информации, но, что следует подчеркнуть, только связанные с конкретными сообщениями на этой территории (п. b) ч. 1 ст. 20)[178] (с оговорками, связанными с особенностями формирования и применения внутригосударственного

[176] Convention Committee on Cybercrime ETS No 185.
[177] Convention Committee on Cybercrime ETS No 185.
[178] Convention Committee on Cybercrime ETS No 185.

права – ч. 1 ст. 20[179]). В Минском соглашении подобных требований нет, лишь содержится общая декларация о принятии сторонами необходимых организационных и правовых мер для выполнения положений Соглашения (ч. 2 ст. 2)[180]. А Будапештская конвенция требует от сторон оказания друг другу максимальной правовой помощи для проведения расследований или судебного разбирательства, а также сбора доказательств по преступлению[181].

Кроме того, в Минском соглашении не содержится ещё ряд требования по гармонизации процессуальных процедур, имеющихся в Будапештской конвенции. Так, например, Конвенция требует от сторон принять законодательные *меры по облегчению и оперативному производству обысков и выемки компьютерных данных или их носителей* (с. 19) на территории своего государства при сохранении компьютерных данных, их целостности и конфиденциальности для лиц, не относящихся к сотрудникам органов[182]. Подобные рекомендации в Минском соглашении отсутствуют.

Основные *меры* в области *международного сотрудничества* следующие. Если Минское соглашение в ст. 5 перечисляет *формы международного сотрудничества* (обмен информацией, исполнение запросов, планирование и проведение скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию киберпреступлений, и прочее[183]); то в Будапештской конвенции этому вопросы посвящена *вся глава III*, где, в частности, в ч. 5 ст. 25 предусматривается *возможность признания деяния преступным обеими сторонами* независимо от его конкретной квалификации, степени тяжести и разницы в терминологии[184].

---

[179] Convention Committee on Cybercrime ETS No 185.

[180] Соглашение «О сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», Минск, 01.06.2001.

[181] Convention Committee on Cybercrime ETS No 185.

[182] Convention Committee on Cybercrime ETS No 185.

[183] Соглашение «О сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», Минск, 01.06.2001.

[184] Convention Committee on Cybercrime ETS No 185.

Сходным мерой обоих документов является установление непосредственного сотрудничества между компетентными органами (ч. 1 ст. 4 Минского соглашения, п. b) ч. 2 ст. 27 Будапештской конвенции).

В Будапештской конвенции предусмотрено *сотрудничество* между компетентными органами *не только в форме обмена данными* (см. п. а) ст. 5 Минского соглашения), но и *взаимной правовой помощи по сбору данных* о потоках в режиме реального времени (ст. 33) и взаимной помощи *по перехвату данных* (ст. 34). Подобных рекомендаций в Минском соглашении нет.

К *мерам* международного сотрудничества также относится *форму запроса о передаче данных* одной стороной *о совершённом киберпреступлении* другой стороне, *о порядке и сроках выполнения запроса*. В пп. а-е ч. 4 ст. 6 Минского соглашения устанавливается порядок направления *письменного* запроса, по определённой форме, *подписанного* руководителем компетентного органа (или его заместителем) и скреплённого *гербовой печатью* (ч. 5 ст. 6)[185]. Само составление подобного запроса требует временных затрат, и, по мнению специалистов, вряд ли является адекватным специфике киберпреступлений по причине несохранности следов: средства хранения и передачи компьютерной информации уничтожают «цифровые следы» автоматически, фиксируя новую информацию[186].

*Меры*, предлагаемые Будапештской конвенцией в области *формирования и исполнения запроса* координально отличаются. Прежде всего, как было уже указано выше, стороны Будапештской конвенции обязаны принять меры по сохранности компьютерной информации на своей территории и меры по её оперативной выемке и перехвату. Запрос другой стороне отправляется, согласно ч. 3 ст. 25, с использованием *любого способа оперативной связи*, факсимильной связи, электронной почты, с соблюдением мер защиты информа-

[185] Соглашение «О сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», Минск, 01.06.2001.

[186] Трофимцева, С.Ю. Организация противодействия киберпреступности: сравнительный анализ процессуальных рекомендаций Будапештской конвенции и законодательства СНГ. – С.246.

ции, включая шифрование (криптографическую защиту), и ответ на запрос принимается в аналогичной форме[187].

Кроме передачи другой стороне информации, ч. 1 ст. 30 Будапештской конвенции в качестве ещё одной *меры* предусматривает возможность направления *запроса о компьютерных потоках для идентификации поставщика услуг и пути, по которому было передано сообщение*[188]. Подобные рекомендации в Минском соглашении отсутствуют.

*Время* на *исполнение* подобного *запроса* другой стороне Минское соглашение отводит, согласно ст. 7, до *30 суток* с даты поступления, а при некоторых обстоятельствах, согласно ч. 4 ст. 7, исполнение запроса можно отложить[189]. Результат при реализации подобной процедуры может быть приближен только к нулевому. Что касается *времени исполнения запроса* в Будапештской конвенции, ст. 35 обязывает подписантов создать *контактный центр 24/7*[190] (7 дней в неделю 24 ч.), что даёт возможность компетентным органам направить запрос в тот момент времени, когда информация им понадобилась, не тратя усилия на оформлении бумаг, что является адекватной мерой, способствующей повышению раскрываемости киберпреступлений.

Кроме того, ст. 26 Будапештской конвенции разрешает *направление информации другой стороне без предварительного запроса*, если это требуется для проведения расследования при совершении транснационального киберпреступления[191].

*Отказать в выполнении запроса*, согласно ч. 4 ст. 27 Будапештской конвенции, сторона может, если запрос касается правонарушения, рассматриваемого как политическое преступление или связанное с политическим преступлением (п. a) ч. 4 ст. 27) или выполнение запроса, вероятно, приведет к подрыву её суверенитета, безопасности, общественного порядка (п. b) ч. 4

---

[187] Convention Committee on Cybercrime ETS No 185.

[188] Convention Committee on Cybercrime ETS No 185.

[189] Соглашение «О сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации».

[190] Convention Committee on Cybercrime ETS No 185.

[191] Convention Committee on Cybercrime ETS No 185.

ст. 27), но при этом сохраняется возможность частичного удовлетворения запроса (ч. 6 ст. 27)[192], что Минским соглашением не предусмотрено.

Кроме того, ч. 1 ст. 31 Будапештской конвенции разрешает одной стороне направить *просьбу о произведении обыска или аналогичных действий*, обеспечивающих доступ к информации, выемке или раскрытия компьютерных данных, в том числе данных, сохраненных, в системе, находящейся *на территории другой стороны*, если есть основания полагать, что соответствующие данные особо уязвимы для потери или изменения (п. а ч. 3 ст. 31), при этом другая сторона может правомерно отказать.

Основные претензии России к мерам административного характера, предлагаемым Будапештской конвенцией, сводятся к следующим.

1. Согласно п. b ст. 32 Конвенции, сторона без согласия другой может «получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получать их»[193]. По мнению России, «такая формулировка» может «нанести ущерб суверенитету и национальной безопасности государств-участников, правам и законным интересам их граждан и юридических лиц»[194]. Претензия выглядит странной, т. к. в абзаце 2 п. b ст. 32 указано, что получение данных без согласия другой стороны возможно тогда, когда запрашивающая «сторона имеет законное и добровольное согласие лица», обладающего компьютерными данными, а оно «имеет законные полномочия раскрывать эти данные»[195]. Т. е., для получения запрашиваемых данных или данных о потоках у лиц на территории другой стороны, такие лица должны иметь право передавать данные в соответствии с нормами внутригосударственного права[196].

---

[192] Convention Committee on Cybercrime ETS No 185.

[193] Convention Committee on Cybercrime ETS No 185.

[194] Распоряжение президента Российской Федерации «О подписании конвенции о киберпреступности» от 15 ноября 2005 г. №557-рп [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/23081 (дата обращения:02.12.2020).

[195] Convention Committee on Cybercrime ETS No 185.

[196] Трофимцева, С.Ю. Организация противодействия киберпреступности: сравнительный анализ процессуальных рекомендаций Будапештской конвенции и законодательства СНГ. – С.246.

2. Согласно ч. 2 ст. 16 Будапештской конвенции, каждая сторона должна внести во внутригосударственное право нормы, обязывающие провайдеров хранить информацию и данные о потоках до 90 дней. Российская сторона сочла требование избыточным, а сроки – завышенными.

Однако в течение 2000-х гг. в федеральное законодательство о связи были внесены изменения, обязавшие провайдеров хранить информацию о фактах коммуникации сначала до 30 дней, а, согласно 374-ФЗ, принятому в июле 2016 г. (один из двух законов так называемого «пакета Яровой»), с июля 2017 г. провайдер обязан хранить данные о фактах пользовательской активности до года, а с июля 2018 г. данные о содержании виртуальной коммуникации до шести месяцев[197] (затем срок был перенесен на 1.11.2018 г.), что значительно больше требований Будапештской конвенции.

3. Согласно п. а) ст. 32 Будапештской конвенции, другой стороне предоставляется право «получать доступ к общедоступным (открытому источнику) компьютерным данным»[198]. По мнению П. Ливадного, это неприемлемо, поскольку «всё-таки мы должны учитывать интересы нашей национальной безопасности»[199]. Данная претензия также вызывает недоумение, т. к. Интернет не предполагает как наличия государственных границ, так и ограничения доступа к открытым ресурсам официальным органам любого государства, и согласие официальных государственных правоохранительных структур на доступ к открытым для всего мира виртуальным ресурсам с юридической точки зрения абсурдно[200].

---

[197] Федеральный закон РФ «О внесении изменений в федеральный закон "О противодействии терроризму" и отдельные законодательные акты российской федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» от 06.07.2016 г. № 374-ФЗ [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/41108, свободный (дата обращения: 13.12.2020).

[198] Convention Committee on Cybercrime ETS No 185.

[199] Россия отказалась ратифицировать конвенцию СЕ о киберпреступности: Новости Интерфакса [Электронный ресурс]. – Режим доступа: http://vz.ru/news/2010/11/9/445958.html (дата обращения: 02.11.2020).

[200] Трофимцева, С.Ю. Организация противодействия киберпреступности: сравнительный анализ процессуальных рекомендаций Будапештской конвенции и законодательства СНГ. – С.247.

4. Последняя претензия в представлении главы департамента по вопросам международной информационной безопасности МИД РФ А. Крутских состоит в том, что Будапештская конвенция «не включает фундаментальный принцип «либо выдай, либо суди»[201]. Эта претензия также вызвала недоумение у специалистов, поскольку в ст. 24 Будапештской конвенция рассматривается порядок выдачи лица за совершение киберпреступлений: согласно п. а) ч. 1 ст. 24, «при условии, что согласно законам обеих заинтересованных сторон за них предусматривается наказание в виде лишения свободы на максимальный срок не менее одного года или более суровое наказание», а, согласно ч. 6 ст. 24, если лицо не может быть выдано по правовым причинам, то запрашиваемая сторона передаёт дело своим компетентным органам «в целях осуществления судебного преследования»[202]. Следует отметить, что подобные нормы в Минском соглашении не предусмотрены вообще.

Исходя из рассмотренного выше, очевидно, что меры административно-правового характера, содержащиеся в международном законодательстве в области противодействия киберпреступности, инициированном Советом Европы, намного по объёму и содержанию превышают рекомендации Минского соглашения, что можно рассматривать как систему более адекватных мер по административно-правовому противодействию международной киберпреступности.

## 3.2. Порядок направления запросов об оказании правовой помощи Российской Федерации в предоставлении информации из зарубежных стран и стран СНГ при расследовании киберпреступлений

Итак, как было рассмотрено выше, в начале XXI века наблюдается экспонентный рост транснациональных киберпреступлений, в связи с чем всем государствам мира, в том числе, Российской Федерации, необходимо осу-

[201] «Без договоренностей глобального характера эту проблему не решить»: Глава нового департамента МИД РФ Андрей Крутских о конфронтации в интернете.

[202] Convention Committee on Cybercrime ETS No 185.

ществлять сотрудничество в сфере обмена информацией при расследовании преступлений в киберсфере.

Дела по киберпреступлениям в Российской Федерации возбуждаются в соответствии с ч. 1 ст.140 УПК РФ, или по заявлению граждан, или по заявлению юридических лиц, либо следователем в процессе расследования других преступлений при обнаружении признаков состава преступления (поскольку ситуация явки с повинной в практике расследования данных дел, как утверждают сами сотрудники полиции РФ, практически не возникает), либо согласно постановлению прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании[203].

В случае если заявление в правоохранительные органы всё-таки поступило, в соответствии с ч. 1 ст. 144 УПК РФ, проводятся оперативно-разыскные мероприятия на предмет выявления признаков состава преступления. В РФ данные мероприятия по киберпреступлениям, отнесены к компетенции Управления «К» Бюро специальных технических мероприятий МВД[204]. Оперативные сотрудники отдела «К» БСТМ территориальных управлений МВД имеют право на проведение опроса потерпевшего, свидетелей и осмотр места происшествия. После проведения необходимых оперативно-разыскных мероприятий, в соответствии со ст. 146 УПК РФ, дело передаётся по подследственности по месту жительства подозреваемого в районный отдел оперуполномоченному для рассмотрения вопроса о возбуждении уголовного дела. В случае если подозреваемый изначально не очевиден (подозреваемый не устанавливается посредством запроса провайдеру и оператору связи, как в случае с удалённым НСД, когда отсутствует круг лиц, имеющих явный мотив совершения данного преступления, или имеет место

---

[203] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 30.04.2021, с изм. от 13.05.2021) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 30.04.2021).

[204] Официальный сайт МВД. – Режим доступа: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (дата обращения: 30.04.2021).

сетевая DDos-атака либо вирусная атака), то для определения подследственности, в соответствии с ч. 3 ст. 146 УПК РФ, дело направляется прокурору, который определяет территориальный следственный орган управления МВД, поскольку согласно п. 3) ч. 2 ст. 151 УПК РФ, ведение дел по ст. 159.6 и ст. 272-274 отнесено к компетенции следственных органов МВД[205].

В порядке, предусмотренном п. 3 ч. 2 ст. 151 УПК РФ, следствие по ст. 159.6 и ст. 272-274.1 в Российской Федерации осуществляется следователями органов внутренних дел[206]. В случае если в процессе расследования киберпреступления следователю требуется оказание содействия в получении информации, представленной в компьютерных системах, расположенных на территории другой страны, то в порядке ст. 453 УПК РФ следователь имеет право внести запрос о производстве на территории осмотра, выемки, обыска, судебной экспертизы или иных процессуальных действий компетентным органом или должностным лицом иностранного государства[207].

В настоящей работе представляется необходимым конкретизировать алгоритм порядка направления запроса о предоставлении органу Министерства внутренних дел Российской Федерации компьютерной информации компетентными органами: государств - членов СНГ, государств - членов МОУП Интерпол, не являющихся членами СНГ.

Итак, запрос в компетентные органы государства - члена СНГ, составляется в соответствии с чч. 3, 4 ст. 453 УПК РФ в порядке, предусмотренном ст. 454 УПК РФ и ч. 2 ст.6 Минского соглашения. Запрос о производстве процессуальных действий должен быть: составлен в письменной форме на языке государства, куда направляется запрос; подписан руководителем органом Министерства внутренних дел, его направляющим (или заместителем руководителя); удостоверен гербовой печатью соответствующего органа.

Запрос должен содержать: наименование органа Министерства внутренних дел, от которого исходит запрос; наименование и место нахождения

[205] Уголовно-процессуальный кодекс Российской Федерации.
[206] Уголовно-процессуальный кодекс Российской Федерации.
[207] Уголовно-процессуальный кодекс Российской Федерации.

органа, в который направляется запрос в иностранном государстве; наименование уголовного дела и характер запроса; указание цели и обоснование запроса; содержание запрашиваемого содействия; изложение подлежащих выяснению обстоятельств, а также перечень запрашиваемых документов, носителей информации и других доказательств; сведения о фактических обстоятельствах совершенного преступления, его квалификация, текст соответствующей статьи Уголовного кодекса РФ, а при необходимости также сведения о размере вреда, причиненного преступлением; желательные сроки исполнения запроса.

В случае если запрос направляется в государство, не являющееся членом СНГ, то на основании ст. 453 УПК РФ, Устава МОУП Интерпол, Указа президента Российской Федерации об участии Российской Федерации в деятельности Международной организации уголовной полиции – Интерпола от 30.07.1996 г. № 1113, Положения о Национальном центральном бюро Интерпола, утвержденного Постановлением правительства РФ от 14.10.1996 г. № 1190. Порядок составления и направления запроса определяется ст. 454 УПК РФ и Приказом МВД РФ № 786 от 06.10.2006 г.

Запрос следователя, ведущего уголовное дело по киберпреступлению, в соответствии со ст. 16 Приказа МВД РФ № 786: направляется в филиал Национального центрального бюро (НЦБ) МОУП Интерпол[208]; составляется в письменной форме на английском, французском или испанском языке; подписывается руководителем органом Министерства внутренних дел, его направляющим (или заместителем руководителя), если он в порядке ст. 22 Приказа МВД РФ № 786 уполномочен на подписание подобных документов; удостоверяется гербовой печатью соответствующего органа; проставляется степень срочности «Urgent» / «Срочно» (в течение 24 часов) или «Non-

[208] Приказ МВД РФ «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» № 786 от 06.10.2006 г. (ред. от 22.09.2009 г.) (Зарегистрировано в Минюсте РФ 03.11.2006 № 8437) [Электронный ресурс]. – Режим доступа: https://legalacts.ru/doc/prikaz-mvd-rf-n-786-miniusta-rf/ (дата обращения: 10.05.2021).

urgent» / «Не срочно» (в течение периода, не превышающего 30 суток) и ссылочный номер документа; указывается код киберпреступления, разработанный МОУП Интерпол.

В соответствии с кодификацией киберпреступлений Интерпола, приведённой выше, предполагается, что: преступление, квалифицированное по ст. 272 УК РФ, может иметь код: QAZ&QDZ (прочие виды несанкционированного доступа и прочие виды изменения данных); преступление, квалифицированное по ст. 273 УК РФ, может иметь код: QDT / QDV / QDW («троянский конь», «компьютерный вирус», «компьютерный червь»); преступление, квалифицированное по ст. 159.6 УК РФ, может иметь код: QFZ (прочие компьютерные мошенничества); преступление, квалифицированное по ч. 1 ст. 274.1 УК РФ, может иметь код: QDZ (прочие виды изменения данных) или общий код QD (изменение компьютерных данных); преступление, квалифицированное по ч. 2 ст. 274.1 УК РФ, может иметь код: QAZ & QDZ (несанкционированный доступ и перехват вкупе с прочими видами изменения данных); преступления, квалифицированные по ст. 274 и ч. 3 ст. 274.1 УК РФ, код в классификации Интерпола не имеет, следовательно, запрос о предоставлении информации или её носителей исполняться не будет.

В случае если в МВД, ГУВД, УВД по субъекту РФ филиал НЦБ Интерпола отсутствует, документы в порядке ст. 16 Приказа МВД РФ № 786, направляются взаимодействующим органом в НЦБ Интерпола через центральный аппарат федерального министерства внутренних дел[209].

В порядке, предусмотренном ст. 19 Приказа МВД РФ № 786, обмен информацией между НЦБ Интерпола и органами Министерства внутренних дел РФ осуществляется: по каналам единой сети электросвязи (ЕСЭ России); по каналам мультисервисной телекоммуникационной сети МВД России; по сети почтовой связи Российской Федерации; по сети федеральной фельдъ-

[209] Приказ МВД РФ «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» № 786.

егерской связи[210]. По действующим международным документам по деятельности Интерпола, документы, поступающие в НЦБ Интерпола по каналам связи телекоммуникационной сети Интерпола I-24/7, круглосуточно принимаются и обрабатываются дежурной сменой сотрудников НЦБ Интерпола.

Практика, в том числе, и российская, показывает, что при определённых ситуациях правоохранительные органы открыты для сотрудничества. К примеру, по сообщению начальника БСТМ генерал-майора полиции А. Мошкова, сотрудниками Управления «К» в 2012 г. была проведена операция «Сорняк» по выявлению пользователей пиринговых сетей в различных странах мира, распространяющих видеоматериалы, содержащие детскую порнографию[211]. Но это, скорее, исключения.

По информации, полученной от сотрудников от сотрудников отдела «К» Бюро специальных технических мероприятий ГУ МВД по Самарской области при прохождении практики в процессе написания настоящей работы, в случае, если следователю отдела полиции ГУ МВД по Самарской области, расследующего преступления, квалифицированные по ст. 159.6 и ст. 272-274.1 УК РФ, необходима информация, предоставляемая в рамках международного сотрудничества компетентными органами другого государства, то время прохождения документов по соответствующим структурам МВД РФ до отправки запроса за пределы России занимает от 30 до 60 дней. С учётом времени выполнения запроса государством - членом СНГ – до 30 дней (а в определённых ч. 4 ст. 7 Минским соглашением случаях исполнение запроса может быть отложено[212]), а государством, не являющимся членом СНГ – в соответствии с его внутренним законодательством, результат исполнения запроса может быть либо отрицательным, либо уже не актуальным в силу специфики киберпреступлений.

---

[210] Приказ МВД РФ «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» № 786.

[211] Национальный форум информационной безопасности обсуждает проблемы противодействия киберпреступности.

[212] Соглашение «О сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации».

Исходя из всего выше сказанного, основной рекомендацией по результатам проделанной работы является предложение Российской Федерации ратифицировать Будапештскую конвенцию Совета Европы. В плане расследования киберпреступлений ратификация Конвенции позволит России (кроме модификации её уголовного законодательства по киберпреступлениям) напрямую отправлять запросы о выдаче компьютерных данных и информации о потоках в киберсфере непосредственно после актуализации необходимости для следствия данной информации, а запрашиваемая сторона будет обязана предоставить России запрошенную информацию, что позволит повысить долю раскрытых киберпреступлений в Российской Федерации и увеличить степень эффективности международного противодействия киберпреступности.

## Выводы по 3 главе

Итак, поскольку киберпреступления являются одними из наиболее серьёзных общественно опасных деяний в силу своего транснационального характера и высокой латентности, как показано в данной главе, для их эффективного расследования требуется реализация адекватных мер административно-правового характера.

Проведённый в настоящей работе сравнительный анализ предлагаемых Минским соглашением о сотрудничестве стран - членов СНГ в киберсфере и Будапештской конвенцией по киберпреступности позволит объединить административные меры по противодействию киберпреступности в две группы: меры внутреннего характера, закрепляющие за сторонами обязательства, соблюдаемые при проведении внутренних расследований, и меры в области международного сотрудничества сторон.

К первой группе мер были отнесены: составление перечня компетентных органов, ответственных за обмен информацией по киберпреступности; требование об оперативном обеспечении сохранности компьютерных дан-

ных, в том числе, данных о потоках информации, хранимых в компьютерной системе; требования о наделении компетентных органов полномочиями по перехвату компьютерных данных; меры по созданию возможностей сбора информации с применением технических средств в реальном времени, меры по облегчению и оперативному производству обысков и выемки компьютерных данных или их носителей.

Ко второй группе мер были отнесены: конкретизация форм международного сотрудничества, включая обмен данными, взаимную правовую помощь по сбору данных о потоках в режиме реального времени и взаимную помощь по перехвату данных; определение формы запроса о передаче данных одной стороной о совершённом киберпреступлении другой стороне, включая информацию о компьютерных потоках для идентификации поставщика услуг и пути, по которому было передано сообщение о порядке формирования и сроках выполнения такого запроса; определение порядка направления информации другой стороне без предварительного запроса; просьбу другой стороне о произведении обыска или аналогичных действий, обеспечивающих доступ к информации, выемке или аналогичного обеспечения сохранности и раскрытия компьютерных данных, в том числе данных, сохраненных, в системе, находящейся на территории другой стороны. На основании проведённого анализа претензий российской стороны к рекомендациям Будапештской конвенции выявлена несущественность данных претензий.

Был рассмотрен порядок формирования запросов в рамках международного сотрудничества России о компьютерных данных при проведении расследований по киберпреступлениям следователями отделов территориальных органов Министерства внутренних дел на основании законодательства Российской Федерации и ратифицированных Россией международных документов. Был выявлен неадекватный времени сохранения следов киберпреступления в виртуальном пространстве срок от направления запроса до получения ответа. В связи с этим был сделан вывод о необходимости присоединения России к Будапештской конвенции.

# ЗАКЛЮЧЕНИЕ

Итак, как было показано в настоящей работе, прогресс информационных технологий, приведший к трансформации общественных отношений и появлению их нового вида – информационных отношений, возникающих по поводу информационного обмена, привёл к появлению нового вида общественно опасных деяний – киберпреступлений, характеризующихся высокой степенью латентности, предполагающих наличие у сотрудников органов следствия специальной компетенции, требующих проведения оперативного расследования по причине исчезновения следов преступления в виртуальной среде, и наличия в ряде преступлений транснационального характера, формирующего проблемы при определении подследственности и обмене данными между правоохранительным органами государств, что в совокупности, как показано в работе, резко снижает уровень их раскрываемости.

На основе проделанного в настоящей работе анализа под киберпреступлениями понимаются виновные общественно опасные деяния, совершаемые в инфотелекоммуникационной среде и посягающие на безопасность информационных отношений, определяемых как общественные отношения, возникающие в процессе взаимодействия субъектов для удовлетворения их интересов в информационном процессе, протекающем в киберпространстве.

В качестве основных классов киберпреступлений выделяются: компьютерные преступления, преступления, связанные с компьютерами, и преступления, связанные с данными.

Под компьютерными преступлениями в настоящей работе понимаются совершаемые в инфотелекоммуникационной среде виновные общественно опасные деяния, непосредственно направленные против конфиденциальности, целостности и доступности данных, что приводит к нарушению законно установленного статуса информации компьютерных систем и нормального функционирования компьютерной системы и сети.

Под преступлениями, связанными с компьютерами, в настоящей работе понимаются виновные общественно опасные деяния, совершённые при помощи компьютерных систем, где компьютер как программно-аппаратное устройство, компьютерные технологии использовались злоумышленником как орудие или средство совершения преступления.

Под преступлениями, связанными с данными, в настоящей работе понимаются виновные общественно опасные деяния, состоящие в распространении в киберсфере негативной информации, запрещённой внутригосударственным и международным законодательством.

Как показано в работе, зарождение киберпреступности и её эскалация в условиях создания инфотелекоммуникационных сетей, особенно Интернета, свидетельствовало о реальной общественной опасности злонамеренных деяний, совершаемых в киберсфере, создавая тем самым, реальную угрозу национальной безопасности государств, в связи с чем, сначала на уровне внутреннего права, затем на международном уровне начался процесс принятия уголовных норм по противодействию киберпреступности.

В настоящей работе на основе анализа рекомендаций резолюций Генеральных ассамблей ООН, Кодификатора киберпреступлений МОУП Интерпол, рекомендаций Комитета Министров стран - членов Совета Европы, Будапештской Конвенции СДСЕ № 185 о киберпреступлениях с изменениями Страсбургского протокола, Модельного кодекса СНГ и Минского соглашения были выявлены основные тенденции по гармонизации внутреннего права государств мира.

В целях анализа было выделено две группы государств: страны, ратифицировавшие Будапештскую конвенцию, и страны - члены СНГ.

Проделанный в рамках настоящей работы процесс гармонизации норм внутреннего права государств, ратифицировавших Будапештскую конвенцию показал, что за прошедшие двадцать лет в уголовное законодательство ряда государств были внесены новые, криминализирующие злонамеренные деяния в киберсфере, которые, в частности, отсутствуют в российском законода-

тельстве: несанкционированный доступ к компьютерным данным или несанкционированное пребывание в систем, перехват информации, включая ПЭМИН, противозаконное использование программ и устройств, компьютерный подлог и нарушение авторских прав с помощью компьютерных технологий. Тем не менее, проведённый в работе анализ уголовного законодательства в киберсфере европейских стран показал, что ратификация Будапештской конвенции далеко не всегда ускоряет процесс работы внутреннего законодателя над гармонизацией уголовных норм. Однако очевидно, что процесс недостаточно быстро, но движется, что позитивно влияет на повышение уровня уголовно-правового противодействия транснациональной киберпреступности.

Анализ модельного законодательства СНГ (Модельного кодекса СНГ и Минского соглашения) показал, что, во-первых, модельное законодательство не содержит часть составов, имеющих место в Будапештской конвенции, что уже можно считать реальной уязвимостью, создающей возможность для злоумышленника остаться безнаказанным, совершая общественно опасное деяние. Кроме того, формулировки части составов вызывают некоторое недоумение или содержат заведомо неисполнимые требования.

Анализ реализации рекомендаций модельного законодательства СНГ был проведён по трём основным группам государств СНГ, где в первой группе (Белоруссию, Армения и Таджикистан) рассматривались государства, максимально инкорпорировавшие рекомендации модельного законодательства СНГ в своё внутренне уголовное право, во второй группе (Казахстан, Киргизия, Туркмения и Узбекистан) государства учли рекомендации лишь частично, при этом провели региональную гармонизацию уголовных норм в области противодействия киберпреступности. Государства третьей группы (Молдавия, Азербайджан, Грузия (по 2009 г.), Украина (по 2018 г.) и Россия) значительно или почти полностью проигнорировали рекомендации законодательства СНГ. А случае с Молдавией, Азербайджаном, Грузией и Украиной это, по всей вероятности, связано с ратификацией ими Будапештской кон-

венции, ситуацию с Россией логично объяснить не представляется возможным.

Таким образом, как показал анализ, в законодательстве стран Европы и США, права субъектов информационных отношений можно считать более защищёнными, чем в государствах СНГ, где ряд действий злоумышленников по посягательствам на компьютерную информацию, системы и сети её хранения, обработки и передачи, остаются безнаказанными.

Проведённый в настоящей работе сравнительный анализ предлагаемых Минским соглашением о сотрудничестве стран - членов СНГ в киберсфере и Будапештской конвенцией по киберпреступности позволит объединить административные меры по противодействию киберпреступности на европейском уровне и уровне СНГ в две группы: меры внутреннего характера, закрепляющие за сторонами обязательства, соблюдаемые при проведении внутренних расследований, и меры в области международного сотрудничества сторон.

К первой группе мер были отнесены: составление перечня компетентных органов, ответственных за обмен информацией по киберпреступности; требование об оперативном обеспечении сохранности компьютерных данных, в том числе, данных о потоках информации, хранимых в компьютерной системе; требования о наделении компетентных органов полномочиями по перехвату компьютерных данных; меры по созданию возможностей сбора информации с применением технических средств в реальном времени, меры по облегчению и оперативному производству обысков и выемки компьютерных данных или их носителей.

Ко второй группе мер были отнесены: конкретизация форм международного сотрудничества, включая обмен данными, взаимную правовую помощь по сбору данных о потоках в режиме реального времени  и взаимную помощь по перехвату данных; определение формы запроса о передаче данных одной стороной о совершённом киберпреступлении другой стороне, включая информацию о компьютерных потоках для идентификации постав-

щика услуг и пути, по которому было передано сообщение о порядке формирования и сроках выполнения такого запроса; определение порядка направления информации другой стороне без предварительного запроса; просьбу другой стороне о произведении обыска или аналогичных действий, обеспечивающих доступ к информации, выемке или аналогичного обеспечения сохранности и раскрытия компьютерных данных, включая данные, сохраненные в системе, находящейся на территории другой стороны.

На основании проведённого анализа претензий российской стороны к рекомендациям Будапештской конвенции выявлена несущественность данных претензий.

Был рассмотрен порядок формирования запросов в рамках международного сотрудничества России о компьютерных данных при проведении расследований по киберпреступлениям следователями отделов территориальных органов Министерства внутренних дел на основании законодательства Российской Федерации и ратифицированных Россией международных документов. Был выявлен неадекватный времени сохранения следов киберпреступления в виртуальном пространстве срок от направления запроса до получения ответа.

В связи с этим был сделан вывод о необходимости присоединения России к Будапештской конвенции, что позволит России:

– гармонизировать своё уголовное законодательство в соответствии с рекомендациями международного права, введя в него новые составы, криминализирующие ряд злонамеренных деяний в киберсфере;

– ускорить время прохождения запроса и получения компьютерных данных, включая данные о потоках, что может сократить срок ведения следствия и повысить уровень раскрываемости киберпреступлений.

## Библиографический список

### Нормативные правовые акты

1. Интерпол: Резолюция AG№/64/P.RES/19 «Компьютерно-ориентированная преступность». Принята Генеральной ассамблеей Интерпола (4–10 октября 1995 г.). [Электронный ресурс]. – Режим доступа: http://www.№ewasp.omskreg.ru/bekryash /app1.htm#6 (дата обращения: 12.01.2021).

2. Модельный уголовный кодекс СНГ. (Рекомендательный законодательный акт для СНГ) (Постановление № 7-5 от 17.02.1996) [Электронный ресурс] // Консорциум-кодекс: Электронный фонд правовой и нормативной документации. – Режим доступа: http://docs.cntd.ru/document/901781490 (дата обращения: 20.02.2021).

3. ООН: Резолюция ООН 55/63 «Борьба с преступным использованием информационных технологий». Принята Генеральной Ассамблеей по докладу Третьего комитета (A/55/593) 22.01.2001 г. [Электронный ресурс] // Официальный сайт ООН. – Режим доступа: https://www.un.org/ru/ga/third/55/third_res.shtml (дата обращения: 22.11.2020).

4. ООН: Резолюция ООН 56/121 «Борьба с преступным использованием информационных технологий». Принята Генеральной Ассамблеей по докладу Третьего комитета (A/55/593) 22.01.2001 г. [Электронный ресурс] // Официальный сайт ООН. – Режим доступа: https://www.un.org/ru/ga/third/56/third_res.shtml (дата обращения: 22.11.2020).

5. Соглашение «О сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», Минск, 01.06.2001 [Электронный ресурс] // СПС «Гарант». – Режим доступа: https://base.garant.ru/12123778/, ограниченный (дата обращения: 11.02.2021).

6. Трудовой кодекс Российской Федерации от 30.12.2001 # 197-ФЗ (ред. от 30.04.2021) (с изм. и доп., вступ. в силу с 01.05.2021) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 13.05.2021).

7. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 30.04.2021).

8. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 30.04.2021, с изм. от 13.05.2021) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 30.04.2021).

9. О внесении изменений в федеральный закон "О противодействии терроризму" и отдельные законодательные акты российской федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Федеральный закон РФ от 06.07.2016 г. № 374-ФЗ [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/41108 (дата обращения: 13.12.2020).

10. О подписании конвенции о киберпреступности: Распоряжение президента Российской Федерации от 15 ноября 2005 г. №557-рп [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/23081 (дата обращения:02.12.2020).

11. О признании утратившим силу распоряжения президента Российской Федерации от 15 ноября 2005 г. №557-рп «О подписании конвенции о киберпреступности»: Распоряжение президента РФ 22 марта 2008 г. №144-рп [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=417185;fld=134;dst=100006;rnd=0.6502687247211727 (дата обращения: 23.07.2020).

12. Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола: Приказ МВД РФ № 786 от

06.10.2006 г. (ред. от 22.09.2009 г.) (Зарегистрировано в Минюсте РФ 03.11.2006 № 8437) [Электронный ресурс]. – Режим доступа: https://legalacts.ru/doc/prikaz-mvd-rf-n-786-miniusta-rf/ (дата обращения: 10.05.2021).

13. Уголовный кодекс Республики Казахстан от 03.07.2014 г. [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/m/document?doc_id=31575252 (дата обращения: 25.12.2020).

14. Уголовный кодекс Кыргызской Республики от 22.12.2016 г. [Электронный ресурс]. – Режим доступа: https://www.legislationline.org-download-id-8264-file-Kyrgyzstan_CC_2016_am2019_ru.pdf (дата обращения: 25.12.2020).

15. Уголовный кодекс Республики Армения от 29.04.2003 г. ЗР-528 [Электронный ресурс]. – Режим доступа: https://www.legislationline.org-download-id-8237-file-Armenia_CC_am2016_ru.pdf (дата обращения: 25.12.2020).

16. Уголовный кодекс Республики Беларусь, 9 июля 1999 г. № 275-З [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=Hk9900275 (дата обращения: 25.11.2020).

17. Уголовный кодекс Республики Таджикистан от 13.11.1998г. № 684 [Электронный ресурс]. – Режим доступа: https://www.legislationline.org-download-id-8601-file-Tajikistan_CC_1998_am2020_ru.pdf (дата обращения: 25.12.2020).

18. Уголовный кодекс Республики Узбекистан от 22.09.1994 г. [Электронный ресурс]. – Режим доступа: https://www.legislationline.org-download-id-8565-file-Uzbekistan_CC_1994_am012020_ru.pdf (дата обращения: 25.12.2020).

19. Уголовный кодекс Туркменистана от 12.06.1997 г. [Электронный ресурс]. – Режим доступа: https://www.legislationline.org-download-id-8316-file-Turkmenistan_CC_2010_am2019_en.pdf (дата обращения: 25.12.2020).

20. Convention on Cybercrime, ETS No 185, Budapest, 23/11/2001 [Electronic resource].– Mode access: http://conventions.coe.int/Treaty/EN/Treaties /Html/185.htm (data access: 06/10/2020).

21. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems ETS No 189, Strasbourg, 28/01/2003 [Electronic resource] // Council of Europe. – Mode access: https://rm.coe.int/090000168008160f free (data access: 06/10/2020).

22. België: Strafwetboek 1867 [Elektronische bron]. − Toegangsmodus: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1867060801&table_name=wet, gratis (datum beroep: 23/02/2021).

23. Die BRD: Das Strafgesetzbuch der BRD 1881 [Elektronisches Resurs]. – Das Regime des Zugang: http://www.gesetze-im-internet.de/stgb/, freies (Datum der Beschwerde: 11/03/2021).

24. Danmark: Straffeloven 1997 [Elektronisk ressource]. − Adgangstilstand: https://danskelove.dk/straffelovengratis (adgangsdato: 09/01/2021).

25. España: Código Penal 1995 [Recurso electrónico]. − Modo de acceso: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html, gratuito (fecha de acceso: 10/01/2021).

26. France: Code pénal 1994 [Ressources électroniques]. – Mode d'accès: http://www.legifrance.gouv.fr/affichCode.do;jsessionid=ACAD58662A3CECCA88A42F6142A3DBCF.tpdjo12v_1?idSectionTA=LEGISCTA000006149839&cidTexte=LEGITEXT000006070719&dateTexte=20140405 (date d'appel: 24/03/2021).

27. Nederlanden: Wetboek van Strafrecht 1881 [Elektronische bron]. − Toegangsmodus: http://www.wetboek-online.nl/wet/Sr.html, gratis (datum beroep: 23/02/2021).

28. Norge: Straffeloven 1902 [Elektronisk ressurs]. − Tilgangsmodus: https://lovdata.no/dokument/NLO/lov/1902-05-22-10?q=straffeloven (anke dato: 10/02/2021).

29. Österreich: Das Strafgesetzbuch der Österreich 1974 [Elektronisches Resurs]. – Das Regime des Zugang: https://www.ris.bka.gv.at/GeltendeFassung. w xe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (Datum der Beschwerde: 11/03/2021).

30. Schwitzerland: Das Strafgesetzbuch 1937 [Elektronisches Resurs]. – Das Regime des Zugang: http://www.admin.ch/opc/de/classified-compilation/19370083/index.html, freies (Datum der Beschwerde: 20/02/2021).

31. Sverige: Straffbalken 1864 [Elektronisk resurs]. − Åtkomstläge: https://riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/ brottsbalk-1962700_sfs-1962-700 (datum för åtkomst: 29/02/2021).

32. UK: The Computer Misuse Act (1990) [Electronic resource]. – Mode access: http://www.legislation.gov.uk/ukpga/1990/18 (data access: 06/10/2020).

33. USA: U.S. Code. Title 18. Part I. Chapter 47. §1030 [Electronic resource]. Mode access: http://www.law.cornell.edu/uscode/text/18/1030 (data access: 06/10/2020).

34. Recommendation No R(89)9 of the Committee of ministers to member states on computer-related crime [Electronic resource]. – Mode access: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlob Get&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 (data access: 06/10/2020).

35. Recommendation No R (95)13 of the Committee of ministers to member states concerning problems of criminal procedural law connected with information technology [Electronic resource]. – Mode access: http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp (data access: 06/10/2020).

**Научные, учебные, справочные издания**

36. Батурин, Ю.М. Проблемы компьютерного права [Текст] / Ю.М. Батурин. –М.: Юридическая литература, 1991. – 221 с.

37. Вехов, В.Б. Компьютерные преступления. способы совершения методики расследования [Электронный ресурс] / В.Б. Вехов. – М., 1996. – Режим доступа: http://www.pravo.vuzlib.org/book_z404_page_1.html (дата обращения: 27.12.2020).

38. Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М.: ООО «Издательство «Юрлитинформ», 2001. – 245 с.

39. Каспаров, А.А. Создание, использование и распространение вредоносных программ для ЭВМ: уголовно-правовые аспекты: Лекция. - М.: МГУ, 2003. – 89 с.

40. Кубышкин, А.В. Международно-правовые проблемы обеспечения информационной безопасности государства / А.В. Кубышкин. – М.: Юристъ, 2002. – 267 с.

41. Пущин, В.С. Преступления в сфере компьютерной информации [Электронный ресурс] / В.С. Пущин (дата обращения: 14.01.2021).

42. Скоромников, К.С. Компьютерное право Российской Федерации / К.С. Скоромников. - М.: Юристъ, 2000. – 256 с.

43. Панфилова, Е.И., Попов, А.Н. Компьютерные преступления. (Серия: Современные стандарты в уголовном праве и уголовном процессе) / Е.И. Панфилова, А.Н. Попов / Науч. редактор проф. Б.В. Волженкин. - СПб., 1998. – 123 с.

44. Фентон, Б. Интерпол / Б. Фентон. - М., 1996. – 230 с.

**Материалы периодической печати**

45. Илюшин, Д.А. Особенности возбуждения уголовных дел о преступлениях, совершаемых в сфере предоставления услуг «Интернет» / Д.А. Илюшин // Вестник Самарского государственного университета. – 2007. – № 1 (51). – С. 9-16.

46. Карпов, Н, Вертузаев, М. К вопросу о борьбе с компьютерными преступлениями в Украине / Н. Карпов, М. Вертузаев // Закон и жизнь. – 2004. - №7. – С.29-32.

47. Смирнова, Т.Г. Преступления в сфере компьютерной информации и некоторые особенности их совершения организованными преступными группами / Т.Г. Смирнова // Проблемы повышения эффективности борьбы с организованной преступностью: Сборник научных трудов / Отв. ред. А.Ф. Токарев. - М.: Юристъ, 1998. - С. 127-131.

48. Тропина, Т.Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? / Т.Л. Тропинина // Международное правосудие. – 2012. – № 3. – С.86-95.

49. Трофимцева, С.Ю., Илюшин, Д.А. Некоторые аспекты квалификации компьютерных преступлений в Российской Федерации и Республике Казахстан / С.Ю. Трофимцева, Д.А. Илюшин // Құқықтық жүйенің қазіргі кездегі дамуының негізгі бағыттары және болашағы: Қазақстан тәуелсіздігінің 25-жылдығына арналған халықаралық ғылыми-тәжірибелік конференцияның материалдары (Алматы, «Тұран» университеті, 1 қараша 2016ж.) / з.ғ.д., профессор Л.Т. Жанузаковаңың, з.ғ.к., доцент Н.А. Жұманбаеваның жалпы редакциясымен. – Алматы, «СаГа», 2017. – С.139-146.

50. Трофимцева С.Ю., Илюшин, Д.А. Некоторые аспекты определения места и времени совершения киберпреступлений в Российской Федерации / С.Ю. Трофимцева, Д.А. Илюшин // Евразийский юридический журнал. – №9(100). – С.246-247.

51. Трофимцева, С.Ю. Запрет на несанкционированный доступ к компьютерной информации как мера противодействия киберпреступности: международные рекомендации и уголовное законодательство стран СНГ / С.Ю. Трофимцева // Евразийский юридический журнал. – 2020. – № 8 (135). – С. 335-337.

52. Трофимцева, С.Ю. Международное противодействие киберпреступности: сравнительный анализ рекомендаций Будапештской конвенции и

законодательства СНГ в области уголовного права / С.Ю. Трофимцева // Евразийский юридический журнал. – 2020. – С.47-49.

53. Трофимцева, С.Ю. Международное уголовно-правовое противодействие киберпреступности: к вопросу об «устаревании» Будапештской конвенции / С.Ю. Трофимцева // Сборник докладов II Всерос. научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации», 28-30 октября, Ставрополь. – Ставрополь: изд-во: Сев.-Кавк. федер. ун-т, 2020. – С. 22-27.

54. Трофимцева, С.Ю. Организация противодействия киберпреступности: сравнительный анализ процессуальных рекомендаций Будапештской конвенции и законодательства СНГ / С.Ю. Трофимцева // Евразийский юридический журнал. – 2020. – №11(150). – С.245-247.

55. Трофимцева, С.Ю. Проблема выделения дефиниций базовых терминов при анализе киберпреступности / С.Ю. Трофимцева // Евразийский юридический журнал. – 2017. – № 7 (110). – С.75-77.

56. Трофимцева, С.Ю. Проблемы гармонизации уголовного законодательства стран СНГ в области противодействия киберпреступности / С.Ю. Трофимцева // Евразийский юридический журнал. – 2020. – №10(149). – С.30-31.

57. Ястребов, Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового сравнительного анализа) / Д.А. Ястребов // Государство и право. – 2005. – №1. – С.52-63.

**Диссертации и авторефераты**

58. Жмыхов, А.А. Компьютерная преступность за рубежом и ее предупреждение / А.А. Жмыхов. Дисс. …канд. юр. наук. Спец. 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право». – М., 2003. – 192 с.

59. Зинина, У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве / У.В. Зинина. Автореф. дисс. … канд. юр. наук. Спец. 12.00.08 – угол. право и криминология; уголовно-исполнительное право. – М.: Инст-та государства и права РАН, 2007. – 32 с.

60. Карпов, В.С. Уголовная ответственность за преступления в сфере компьютерной информации / В.С. Карпов. – Автореф. дисс. … канд. юр. наук. Специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право». – Красноярск: КрГУ, 2002. – 28 с.

61. Сафонов, О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. ... канд. юрид. наук / О.М. Сафронов. – М., 2015. – 186 с.

## Материалы юридической практики

62. Постановление Пленума Верховного Суда РФ, касающимся компьютерных преступлений, от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. – 2008. – 12 января. – Вып. 4.

## Электронные ресурсы

63. «Без договоренностей глобального характера эту проблему не решить»: Глава нового департамента МИД РФ Андрей Крутских о конфронтации в интернете [Электронный ресурс] // Газета «Коммерсантъ». – 2020. – 25.02. – №33. – С. 6. – Режим доступа: https://www.kommersant.ru/doc/4267456 (дата обращения: 27.10.2020).

64. Бекряшев, А.К., Белозеров, И.П. Теневая экономика и экономическая преступность [Электронный ресурс] / А.К. Бекряшев, И.П. Белозёров. - Режим доступа:

http://sbiblio.com/biblio/archive/bekryashev_belozerov_tenevaya_economica/3.aspx (дата обращения: 23.11.2020).

65. Васильев, В. Расследование компьютерных преступлений как компонент обеспечения ИБ [Электронный ресурс] / В. Васильев // ИТ-безопасность. – 2001. – Май. – Режим доступа: http://www.pcweek.ru/security/article/detail.php?ID=131239 (дата обращения: 12.12.2020).

66. Ворошилова, Т.П. Киберпреступления (преступления в сфере компьютерной информации) в санкциях статей уголовного кодекса российской федерации [Электронный ресурс]. – Режим доступа: http://www.rusnauka.com/26_NII_2011/Pravo/5_92099.doc.htm (дата обращения: 24.11.2020).

67. Дубко, М. О понятии компьютерного преступления [Электронный ресурс] / М. Дубко. – Режим доступа: http://marketing2013.ucoz.ru/blog/o_ponjatii_kompjuternogo_prestuplenija/2013-01-19-632 (дата обращения: 24.11.2020).

68. Козлов, В. «Computer crime»? Что стоит за названием? (криминалистический аспект) [Электронный ресурс] / В. Козлов. – Режим доступа: http://www.crime-research.ru/library/CCrime.html (дата обращения: 24.11.2020).

69. Концепция проекта Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информатизации» [Электронный ресурс]. – Режим доступа: http://referatdb.ru/informatika/3504/index.html?page=2 (дата обращения: 12.12.2020).

70. Мамедов, Н. Криминалистические проблемы расследования преступлений в сфере компьютерной информации [Электронный ресурс] / Н. Мамедов // Специализированный ежемесячный журнал «ЮРИСТ». – 2008. – Сентябрь. - № 9 – Режим доступа: http://journal.zakon.kz/203375-kriminalisticheskie-problemy.html (дата обращения: 23.12.2020).

71. Мосин, О.В. Компьютерная преступность и Интернет [Электронный ресурс] / О.В. Мосин. – Режим доступа: http://www.ibil.ru/index.php?Type=review&area=1&p=articles&id=1140 (дата обращения: 24.11.2020).

72. Национальный форум информационной безопасности обсуждает проблемы противодействия киберпреступности [Электронный ресурс] // Опубликовано: официальный сайт МВД, 05 Февраля 2013 15:00.– Режим доступа: http://mvd.ru/news/item/830615/ (дата обращения: 11.11.2020).

73. Осипенко, А.Л. Борьба с преступностью в глобальных компьютерных сетях Интернет: Монография [Электронный ресурс] / А.Л. Осипенко. – Режим доступа: http://www.s-quo.com/content/articles/335/949/ (дата обращения: 02.11.2020).

74. Официальный сайт МВД. – Режим доступа: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (дата обращения: 30.04.2021).

75. Россия отказалась ратифицировать конвенцию СЕ о киберпреступности: Новости Интерфакса [Электронный ресурс]. – Режим доступа: http://vz.ru/news/2010/11/9/445958.html (дата обращения: 02.11.2020).

76. Таблица подписей и ратификации договора 185 «Конвенция о компьютерных преступлениях». Статус на 15/05/2021 [Электронный ресурс] // Сайт Совета Европы. – Режим доступа: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=TVQJuVZx (дата обращения: 15.05.2021).

77. Широков, В.А., Беспалова, Е.В. Киберпреступность: история уголовно-правового противодействия [Электронный ресурс]. – Режим доступа: http://www.gosbook.ru/node/29398 (дата обращения: 13.01.2021).

78. Эмм, Д. Киберпреступность и закон: обзор положений законодательства Великобритании, касающегося компьютерных преступлений [Электронный ресурс]. – Режим доступа:

http://www.comprice.ru/articles/detail.php?ID=232278 (дата обращения: 25.03.2021).

79. Яблоков, Н.П. Криминалистика: Теоретические, методологические и науковедческие основы криминалистики [Электронный ресурс] / Н.П. Яблоков. – Режим доступа: http://www.be5.biz/pravo/k012/223.htm (дата обращения: 23.12.2020).

80. Urbanovich, P. Information protection. Part 1: introduction to the subject area [Electronic resource]. – Mode access: https://elib.belstu.by/bitstream/123456789/293/1/Informationprot_Part201-introduction.pdf (data access: 01/02/2021).