Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Юридический институт
институт
Деликтологии и криминологии
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ И.А. Дамм
подпись инициалы, фамилия
« _____» _____ 2019 г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01 – Юриспруденция

Криминологический анализ и предупреждение преступлений в отношении персональных данных, совершаемых в сети Интернет

Руководитель _____ доцент, к.ю.н. С.И. Гутник
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ А.С. Синякова
подпись, дата инициалы, фамилия

Красноярск 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ……...3

ГЛАВА 1. Особенности персональных данных как вида информации: возникновение и развитие ……6

§ 1. Персональные данные как вид информации ……..6

§ 2. Возникновения института персональных данных: российский и зарубежный опыт
…….25

ГЛАВА 2. Криминологический анализ преступлений в отношении персональных данных, совершаемых в сети Интернет……..37

§ 1. Преступления в отношении персональных данных, совершаемые в сети Интернет…….37

§ 2. Анализ механизма преступных посягательств в отношении персональных данных, совершаемых в сети Интернет……..44

§ 3. Личность преступника, совершающего преступления в отношении персональных данных в сети Интернет……52

§ 4. Предупреждение преступлений в отношении персональных данных, совершаемых в сети Интернет…….....58

ЗАКЛЮЧЕНИЕ…….....65

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ……..69

ВВЕДЕНИЕ

Проблема обеспечения информационной безопасности актуальна с тех пор, как люди стали обмениваться информацией, накапливать ее и хранить. Во все времена возникала необходимость надежного сохранения наиболее важных достижений человечества с целью передачи их потомкам. Аналогично возникала необходимость обмена конфиденциальной информацией и надежной ее защиты.

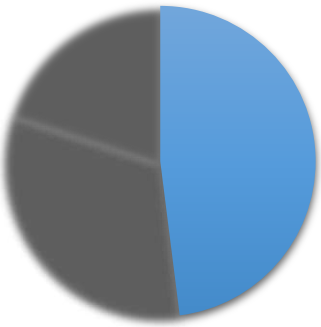
В современном обществе проблема информационной безопасности особенно актуальна, поскольку информация стала частью жизни. Быстро развивающиеся информационные технологии вносят заметные изменения в жизнь общества. Информация стала товаром, который можно приобрести, продать, обменять. От степени безопасности информационных технологий зависит благополучие, а порой и жизнь многих людей.

С повышением значимости и ценности информации соответственно растет и важность ее защиты. С одной стороны, информация стала товаром, и ее утрата или несвоевременное раскрытие наносит материальный ущерб. С другой стороны, информация - это сигналы управления процессами в обществе, а несанкционированное вмешательство в процессы управления может привести к катастрофическим последствиям.

Актуальность данной работы диктуется невероятным вовлечением людей в социальные сети по всему миру. По данным аналитического агентства Statista в России на 2018 год использование социальных сетей оценивается в 47% от количества всего населения, аккаунты в них имеют 67,8 млн россиян[1]. Для

[1] Социальные сети в 2018 году: глобальное исследование. [Электронный ресурс] : WebCanape. Социальные сети в 2018 году: глобальное исследование. – Режим доступа: https://www.web-canape.ru

более подробного изучения вовлечения населения в социальные сети было проведено статистическое исследование в виде анкетирования, в котором приняли участие 50 человек в возрасте от 15 до 52 лет. В результате чего стало известно, что более половины респондентов имеют три и более аккаунта в



социальных сетях, что говорит о том, что социальные сети невероятно сильно внедрились в жизнь каждого из нас и сопровождают ее изо дня в день (Рис. 1). Такое быстрое распространение сети Интернет повлекло появление новых способов нарушения законного обмена информацией, а как следствие нарушения конституционных прав и свобод.

Рисунок 1 – количество аккаунтов в социальных сетях на одного человека

Объектом данной работы выступает комплекс общественных отношений, связанных с криминологическими особенностями и предупреждением преступлений в современных правовых условиях Российской Федерации.

Предметом работы являются нормы действующего законодательства Российской Федерации, уголовного законодательства России советского периода, регулирующего правоотношения по обеспечению правовой охраны персональных данных, общепризнанные принципы и нормы международного права и международные договоры в области правового регулирования и охраны оборота персональных данных, ведомственные нормативные правовые акты, данные статистических исследований, уголовные дела, публикации по

указанной проблематике, электронные ресурсы всемирной информационно коммуникационной сети Интернет.

Целью работы является проведение криминологического анализа и изучение механизма предупреждения преступлений в отношении персональных данных в сети Интернет.

Для достижения указанной цели были поставлены следующие задачи:

1. Изучить персональные данные как особый вид информации;
2. Изучить становление института персональных данных в России, сравнить с зарубежным опытом;
3. Исследовать динамику преступлений против персональных данных в сети Интернет за 2016-2018 годы;
4. Изучить механизм преступных посягательств;
5. Изучить личность преступника, виктимологические особенности данных преступлений;
6. Изучить меры по предупреждению преступлений в отношении персональных данных в сети Интернет, определить необходимость профилактических мероприятий.

Нормативную базу исследования составляют: Конституция Российской Федерации, Уголовный кодекс Российской Федерации, законодательные акты Российской Федерации, регулирующие оборот персональных данных, а также уголовное законодательство, осуществляющее правовое регулирование охраны персональных данных в зарубежных странах.

Теоретической базой работы выступили работы следующих авторов: (запишу после).

Структура работы включает введение, две главы, которые объединяют шесть параграфов, заключение и список использованных источников. Данная структура работы обусловлена поставленными задачами и направлена на их реализацию.

Глава 1. Особенности персональных данных как вида информации: возникновение и развитие

1.1. Персональные данные как вид информации

Исследование правовой регламентации оборота персональных данных следует начать с понимания самого феномена «персональные данные». Для ясности необходимо определить место персональных данных в огромном потоке информации, выделив существенные признаки и черты. Это важно еще и потому, что в действующем законодательстве нет единого подхода к пониманию такого вида информации, что добавляет проблем правоприменителю.

Сегодня человечество живет в обществе, где информация является важнейшим ресурсом и основополагающим инструментом развития. Любая наша деятельность пронизана информационными отношениями, они важнейший регулятор нашей жизни. Признание информации ценностью общества создало потребность в формировании правового механизма защиты информации.

С каждым годом нормативная база регулирования информационных правоотношений усиливается и дополняется. В 1993 году Конституция РФ закрепила принцип приоритета прав и свобод человека и гражданина, право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиты чести и доброго имени[2]. В мае 2017 года Указом Президента Российской Федерации была утверждена Стратегия развития информационного

[2] Конституция Российской Федерации [Электронный ресурс] : федер. закон от 25.12.1993 ред. от 21.07.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

общества в Российской Федерации на 2017 - 2030 годы, которая установила необходимость законодательной регламентации доступа организаций к данным о гражданах и юридических лицах, в том числе содержащимся в государственных информационных системах, порядка обработки данных, а также порядок государственной защиты персональных данных граждан на территории Российской Федерации. Кроме того, Стратегия закрепила необходимость обеспечить защиту данных от несанкционированной и незаконной трансграничной передачи иностранным организациям[3]. Таким образом, персональные данные, получившие законодательную защиту относительно недавно, уже стали важным элементом безопасности всей информационной системы.

Учитывая важность таких понятий, как «конфиденциальная информация», «персональные данные», «идентификация личности», единого подхода к их пониманию нет. Между тем, представляется невозможным законодательное обеспечение безопасности персональных данных без понимания сущности такого вида информации. Таким образом, необходимо определить место персональных данных в сфере информационных правоотношений, исходя из понятия и их признаков.

Итак, персональные данные–в первую очередь, являются информацией. Именно информация является родовым понятием, от которого необходимо отталкиваться, изучая отдельные её разновидности.

Обыденное понимание информации нашло отражение в словарях русского языка. Само слово «информация» восходит к латинскому «informatio» и означает буквально «разъяснение, изложение, сообщение, осведомление о чем-либо». В русский язык это слово пришло во времена Петра I, будучи заимствованным из польского, однако в речевой практике оно практически не

[3] Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы (утв. Указом Президента РФ 09.05.2017 № 203) [Электронный ресурс] : информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

использовалось вплоть до XX в[4]. В качестве синонимов к слову «информация» в словаре синонимов называются «сведения», «данные», «материал»[5]. В «Большом толковом словаре русского языка» С.А. Кузнецова под информацией понимается «сообщение о положении дел где-либо, о каких-либо событиях» или «сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальными устройствами»[6].

В середине двадцатого века Клод Шеннон ввел термин «информация» в узком техническом смысле, применительно к теории связи или передачи кодов (которая получила название «Теория информации»). Математическая теория информации К. Шеннона утверждала, что «информация есть снятая неопределенность» и позволяла определять количество информации, передаваемой по каналам связи, абстрагируясь от ее семантики, смысла[7]. Для уяснения специфики такого понимания информации А.Д. Иванников, А.Н. Тихонов и В.Я. Цветков приводят три фразы: 1) «казнить нельзя, помиловать»; 2) «казнить, нельзя помиловать»; 3) «нить, ватьнепомльзя казило». Из этих трех фраз первая и вторая противоположны по смыслу, третья бессмысленна, но с позиции теории информации К. Шеннона они несут одинаковое количество информации, имеют равное количество бит[8]. Таким образом, теория информации К. Шеннона полностью игнорирует содержание информации. Вопрос о ее ценности в этой теории вообще не ставится. Как пишет И.В. Мелик-Гайказян, «рассчитывая пропускную способность канала связи, бессмысленно принимать во внимание содержание телеграмм»[9].

---

[4] Лысак, И. В. Информация как общенаучное и философское понятие: основные подходы к определению / И. В. Лысак // Философские проблемы информационных технологий и киберпространства. – Пятигорск, 2015. – С. 9 - 26.

[5] Словарь синонимов русского языка [Электронный ресурс] : З. Е. Александрова. Практический справочник. М.: Русский язык, 2001. — Режим доступа: https://alleng.org.

[6] Большой толковый словарь русского языка [Электронный ресурс] : коллекция словарей и энциклопедий сост. и гл. ред. С.А. Кузнецов. СПб. — Режим доступа: https://gufo.me.

[7] Шеннон, К. Работы по теории информации и кибернетике. / К. Шеннон // Издательство иностранной литературы. – Москва, 1963. – С. 263.

[8] Иванников, А. Д., Тихонов, А. Н., Цветков, В. Я. Основы теории информации / А. Д. Иванников, А. Н. Тиханов, В. Я. Цветков // МАКС Пресс. – Москва, 2007. – С. 163.

[9] Мелик-Гайказян, И. В., Мелик-Гайказян, М. В., Тарасенко, В. Ф. Методология моделирования нелинейной динамики сложных систем / И. В. Мелик-Гайказян, М. В. Мелик-Гайказян, В. Ф. Тарасенко // Физматлит. – Москва, 2001. – С. 96.

Абсолютно противоположную идею высказывал один из самых известных теоретиков информации Норберт Винер, с работами которого советские читатели познакомились в конце 50-х годов XX века. Норберт Винер утверждал, что «информация – это обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспосабливания к нему наших чувств»[10]. Данная идея считается более верной, несмотря на то, что ценность информации - очень спорный вопрос, содержании все же является именно тем элементом, который позволяет снять неопределенность в понимании чего-либо. Информацию нельзя путать с коммуникацией в целом, ведь именно это явление является «каналом связи», описанным И.В. Мелик-Гайказян, а сама информация всегда несет в себе содержательный элемент, воспринимаемый людьми по-разному.

Исходя из вышеперечисленного, можно уже найти общие признаки. Итак, информация - это некие знания об окружающем нас мире, помогающие восполнить недостающую осведомленность. К этому можно добавить очевидный признак – существование информации исключительно внутри общества как следствие взаимодействия людей и осуществления ими различной деятельности.

Информация необходима обществу как условие коммуникации, без нее общество не сможет функционировать, а значит, такому важному элементу нашей жизни просто необходима четкая правовая регламентация и особый режим защиты. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ определяет информацию весьма просто: это сведения (сообщения, данные) независимо от формы их представления[11]. Закон при этом никаким образом не конкретизирует, что понимается под сведениями, а отождествляет их с

[10] Винер Н. Кибернетика и общество / Н. Виннер // Издательство иностранной литературы. – Москва, 1958. – С. 31.

[11] Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ ред. от 18.03.2019 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

сообщениями и данными. Законодательное закрепление достаточно узкое и не отражает сути информации, представленной выше. В данном определении не ясно, какими признаками обладает информация, и для чего она вообще нужна.

Можно ли отождествлять понятия сведения и информация либо информация шире и включает в себя что-то еще? Во всех случаях, когда идет речь о сведениях, следует понимать, что говорится об информации осмысленной, преобразованной человеческим сознанием. Ставя знак «равно» между фактами и сведениями, мы придерживаемся сути антропоцентрического подхода. Этот подход в настоящее время применяется наиболее широко и, в частности, в российском законодательстве. До последнего времени антропоцентрический подход удовлетворительно работал в области правовых и общественных наук[12]. Однако его минусы стали появляться все чаще и чаще в процессе активного развития технологий.

Во-первых, антропоцентрический подход подразумевает понимание информации как сведений, осмысленных человеком, соответственно, возникает проблема описания информационных процессов между компьютерами, различными технологическими системами. Во-вторых, в рамках антропоцентрического подхода невозможно найти адекватного объяснения генетической информации живой природы.

В связи с этим возникла потребность в изменении трактовки понятия информации. Оно было расширено и включило обмен сведениями не только между человеком и человеком, но также между человеком и автоматом, автоматами, обмен сигналами в животном и растительном мире, передачу признаков между клетками. Получается, что информация тождественна сведениям, которые передаются во всей живой природе, а не только от человека к человеку, она может быть и не осмысленная человеком, но информацией быть

[12] Абдулгалимов, Г. Л., Кугель, Л. А. Обучение проектированию информационных систем и анализу данных / Г. Л. Абдулгалимов, Л. А. Кугель // Профессиональное образование. Столица. – Москва, 2013. – № 4. – С. 31-33.

от этого не перестанет. Такое понимание стало необходимым при развитии технологий и человеческого сознания в целом.

На основе вышеизложенного можно выделить несколько признаков информации:

1) Информация является совокупностью сведений (знаний) и коммуникации (канала передачи содержания информации).

2) Информация подвержена субъективному восприятию, которое зависит от обстановки, личности и еще многих факторов.

3) Информация всегда существует внутри общества, является связующим звеном в информационных отношениях, пронизывающих жизнь каждого.

4) Информация не всегда может быть ценна здесь и сейчас, цель получения информации – стать осведомленным, приобрести знание, вне зависимости от получения пользы здесь и сейчас.

5) Информацией можно считать также обмен сигналами в животном и растительном мире, передачу признаков от клетки к клетке, передачу сведений от автомата автомату.

Итак, любые сведения независимо от их оформления, являются информацией - материальным или нематериальным объектом, участвующим в любых отношениях. Современное развитие общества, в котором возможна невероятно быстрая передача информации, выделило ее в особый предмет экономических, социальных и культурных правоотношений.

Персональные данные и есть разновидность информации, они дают познаваемому субъекту сведения о конкретном человеке. Но также у персональных данных есть особый признак, который присущ не любой информации. Персональные данные не всегда общедоступны, их оборот в большей части ограничен, и для того, чтобы исследовать сам феномен

персональных данных, необходимо понять суть конфиденциальности информации.

С появлением социальных сетей человек стал более открыт для общения с другими людьми, стал более доверительно относиться к сети Интернет, а значит информация о нем стала более уязвима. В 1993 году в журнале New Yorker была опубликована карикатура, изображающая двух собак, сидящих перед дисплеем компьютера, одна из которых говорит другой: В Интернете никто не знает, что ты собака[13]. Сегодняшняя реальность существенно отличается от этой картины. Пользуясь социальными сетями, кто-то осознано, а кто-то нет распространяет информацию о себе, а иногда это может повлечь неблагоприятные последствия. Мы так переживаем за утечку данных о нашей банковской карте, адреса квартиры, но вряд ли кто-то задумывался что и фотографии, и переписку, и номер автомобиля можно использовать в преступных целях. Все это говорит о том, что информация не всегда должна быть открыта, а с развитием сети Интернет к конфиденциальной информации должно быть приковано особое внимание.

Согласно Конституции Российской Федерации каждый имеет право свободно искать, получать, передавать, производить информацию любым законным образом[14]. Европейская конвенция о защите прав человека и основных свобод также закрепляет свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны органов публичной власти и независимо от государственных границ, фиксирует возможные запреты и ограничения для защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия[15]. Несмотря на то, что свобода обмена информацией провозглашена многими государствами,

[13] Jones, C. R. Nobody knows you’re a dog / C. R. Jones // Education in Cyberspace. — New York, 2004.

[14] Конституция Российской Федерации [Электронный ресурс] : федер. закон от 25.12.1993 ред. от 21.07.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[15] Европейская конвенция о защите прав человека и основных свобод ETS №005 [Электронный ресурс] : конвенция о защите прав человека и основных свобод (Заключена в г. Риме 04.11.1950) (с изм. от 13.05.2004) // Информационно-правовой портал «Гарант.ру». — Режим доступа: https://www.garant.ru.

существуют обстоятельства, при которых такой обмен может повлечь нарушение прав человека либо подорвать безопасность государства в целом.

Итак, для того, чтобы обозначить информацию, ограниченную в доступе, в мировой практике появилось понятие конфиденциальной информации. Например, в модельном законе о международном информационном обмене конфиденциальная информация понимается как документированная информация, доступ к которой ограничивается в соответствии с законодательством[16]. В законодательстве России существует понятие конфиденциальности информации как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя[17]. Существует также перечень информации, отвечающей признаком конфиденциальности в Указе Президента РФ от 06 марта 1997 №188 «Об утверждении перечня сведений конфиденциального характера», который был редактирован в 2015 году. Данный перечень включает в себя, помимо прочего, сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные). Установление такого перечня, несомненно, в перспективе должно было упростить защиту оборота информации, но Конституция Российской федерации предусматривает ограничение прав и свобод человека и гражданина только на основе федерального закона, а Указ президента таковым не является[18].

Итак, до этого момента мы применяли понятие конфиденциальности информации, что является особым режимом, требованием по обращению с ней. Ранее, в Федеральном законе «Об информации, информатизации и защите информации» 1995 года содержалось понятие «конфиденциальной

---

[16] О международном информационном обмене [Электронный ресурс] : модельный закон от 26.03.2002 № 19-7 // Информационно-правовой портал «Гарант.ру». — Режим доступа: https://www.garant.ru.

[17] Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ ред. 18.03.2019 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[18] Конституция Российской Федерации [Электронный ресурс] : федер. закон от 25.12.1993 ред. от 21.07.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

информации». Это понятие подразумевало под собой информацию, которая изначально была ограничена в обороте в силу прямого указания на это в законе, то есть существовал особый вид информации. Именно такое определение дает и модельный закон о международном информационном обмене[19]. Сейчас же понятие «конфиденциальности информации» подразумевает условия, согласно которым информация будет носить признак конфиденциальности.

Суть конфиденциальности информации в ее ограниченном доступе, который заключается в усложненной процедуре обмена такой информацией. Получатель такой информации не может распространять ее без согласия обладателя, что и отличает ее от общедоступной. Такой режим существует для защиты прав и свобод тех субъектов правоотношений, оборот информации о которых может нанести ущерб их деятельности, прибыли или безопасности. Но и тут есть особенности, субъект может сделать любую информацию о себе общедоступной, распространив ее для открытого пользования, то есть конфиденциальность проявляется не в силу особого предписания на это в законе, а в силу воли самого субъекта такой информации.

Заслуживает внимания мнение Е. К. Волчинской, которая полагает, что можно выделить несколько условий, необходимых и достаточных для установления режимов конфиденциальности:

– заинтересованность субъекта в ограничении доступа к информации, свидетельствующая о том, что конкретная информация представляет для него ценность (в моральном, материальном аспекте);

– наличие интереса (права) других субъектов на получение и/или использование этой информации, т. е. обладатель, реализуя свой интерес, не должен нарушать законные права других субъектов на получение информации;

– информация, доступ к которой ограничивается, не должна быть общеизвестной;

[19] О международном информационном обмене [Электронный ресурс] : модельный закон от 26.03.2002 № 19-7 // Информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

– обладатель информации, к которой он хочет ограничить доступ, должен обеспечить необходимые меры защиты этой информации – установить режим тайны[20].

Исходя из предложенных выше определений, можно выделить главный критерий конфиденциальности информации - возможность быть переданной третьим лицам только с согласия её обладателя, что и будет отличием от информации общего доступа. Таким образом, наступление режима конфиденциальности зависит от решения самого обладателя информации, но это не единственный вариант.

Так, Федеральный закон «О персональных данных» устанавливает, что операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законом[21]. Данный закон устанавливает перечень оснований, при которых получение согласия субъекта на обработку персональных данных, а, как следствие, обеспечение их конфиденциальности, не требуется. Среди них, в частности, указываются такие, как: необходимость защиты жизни и здоровья субъекта персональных данных; всероссийская перепись населения; необходимость установления или осуществления прав субъекта персональных данных, а равно и в связи с осуществлением правосудия и т.д.

Подводя итог определению понятия конфиденциальности информации, можно прийти к выводу, что под данным режимом понимаются особые условия оборота необщедоступной информации, имеющей значение для его владельца, заключающиеся в получении согласия на передачу ее третьим лицам. Законодательного перечня такой информации, на основе которой возможно было бы ограничить права других людей на получения информации, не

[20] Волчинская, Е. К. Место персональных данных в системе информации ограниченного доступа / Е. К. Волчинкская // Право. Журнал Высшей школы экономики. – Москва, 2014. – С. 195.

[21] О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 №152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

существует. Также необходимо понимать, что не всегда требуется согласие обладателя на передачу информации третьим лицам, исключения существуют для прямо предписанных в законе случаев, некоторые из них были приведены в качестве примера выше.

Как уже упоминалось, Указ Президента от 06 марта 1997 года №188 одним из видов конфиденциальной информации называет персональные данные. В доктрине персональные данные определяются как информация (зафиксированная на любом материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним[22].

Статья 2 Конвенции № 108 Совета Европы «О защите личности в связи с автоматической обработкой персональных данных» содержит определение персональных данных как информации, касающееся конкретного или могущего быть идентифицированным лица («субъекта данных»). Это определение достаточно широкое и дает возможность странам, ратифицировавшим Конвенцию, возможность для трактовки и трансформации его для применения в национальном законодательстве.

Еще до принятия конвенции Федеральным законом от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» (далее Закон № 24) впервые на законодательном уровне было закреплено понятие «персональные данные». Согласно статье 2 упомянутого закона к персональным данным относились «сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность»[23]. Важно понимать, что персональные данные могут относиться не только к не известному ранее человеку, но и к уже идентифицированному. Примером может служить Апелляционное определение от 22 мая 2014 г. по

[22] Алямкин С. Н. Персональные данные как объект правового регулирования: понятие и способы защиты / С. Н. Алямкин // Мир науки и образования. – Саранск, 2016. – № 4(8).

[23] Собрание законодательства Российской Федерации [Электронный ресурс] : собрание законодательства РФ 1995 №8 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

делу № 33–14709[24]. Гражданин подал заявление мировому судье в порядке частного обвинения, в связи с чем запросил в отделе МВД РФ по району Соколиная гора по г. Москве паспортные данные граждан, в отношении которых заявление было подано. В данном случае необходимое лицо уже идентифицировано и требуется лишь заполучить нужную информацию. Практика по таким случаям достаточно однозначна — запрашивающим отказывают в предоставлении данных на основании того, что они являются персональными и защищены Федеральным законом № 152-ФЗ «О персональных данных». В таких ситуациях информация может быть предоставлена только с согласия лица, чьи персональные данные подлежат разглашению. Исключением являются случаи, когда соответствующие данные уже находятся в свободном доступе или принадлежат должностному лицу и связаны с его деятельностью по осуществлению своих полномочий.

Более верный и разумный подход избрали авторы принятого 27 июля 2006 года Федерального закона № 152-ФЗ «О персональных данных» (далее Закон № 152), где в статье 3 постарались дополнить и конкретизировать понятие персональных данных по сравнению с ранее существующими. Если говорить обобщенно об этом законе, а не только об исследуемой дефиниции, можно сказать, что его принятие относится к первой попытке установления комплексного правового регулирования защиты персональных данных. Причиной его принятия, в частности, послужили имевшиеся на тот момент многочисленные факты краж баз персональных данных в государственных и коммерческих структурах, их повсеместная продажа[25].

Итак, российское законодательство также дает необоснованно широкое определение понятия «персональные данные». В понимании Федерального закона от 27.07.2006 № 152-ФЗ персональные данные - это любая информация,

---

[24] Апелляционное определение Московского городского суда от 22.05.2014. № 33-14709 [Электронный ресурс] : справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=RAMSMARB&n=719253#02431987170781642.

[25] Симонова, Е. В. Определение понятия персональных данных в Российской Федерации / Е. В. Симонова // Молодой ученый. – Казань, 2017. – №10. – С. 323-326.

относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[26]. Одна из предыдущих редакций данного закона содержала конкретный и в то же время открытый перечень персональных данных: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Исключение перечня конкретных видов информации стало результатом приведения понятийного аппарата в соответствие с Конвенцией № 108 Совета Европы, что нельзя, на наш взгляд, назвать удачным решением. Данная конвенция закрепила самое широкое определение, которое государства могут конкретизировать для включения в свое законодательство, что и было сделано в предыдущей редакции Закона №152. Новая редакция позволяет относить к персональным данным почти любую информацию, которая хотя бы косвенно сопровождает жизнь определенного человека, что не позволяет качественно защищать ее от преступных посягательств, а также порождает множество проблем в судебной практике.

Для выявления проблем, встречающихся при толковании понятия «персональные данные», было проанализировано 50 решений судов общей юрисдикции, включая решения судебных коллегий по гражданским делам, а также решения мировых судей по делам об административных правонарушениях. Решения подобраны с учетом возможной разнообразности в понимании судами понятия «персональные данные» за период 2017–2018 годов. По итогу, не было выявлено ни одного судебного решения, в котором бы у суда или сторон возникал вопрос о том, является ли некоторая информация персональными данными или нет. Суды достаточно уверенно относят всё, что прямо или косвенно относится к определенному или определяемому физическому лицу, к персональным данным. Например: фотоизображения[27];

[26] О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 №152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[27] Приговор № 1-53/2018 от 24 сентября 2018 г. по делу № 1-53/2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/JHBHzJUXOmWW/.

детализация соединений абонентов операторов сотовой связи[28]; содержание личной переписки[29]; абонентские номера[30]; адреса почтовых ящиков зарегистрированных пользователей и пароли к этим почтовым ящикам[31]; паспортные данные[32]; ФИО, дата рождения[33]; сведения о должнике, просроченной задолженности и ее взыскании[34]; нетрудоспособность[35]; кредитная задолженность перед банком[36] и т. п. Нельзя сделать вывод, говорящий о том, что суды уверенно и обоснованно толкуют легальное определение персональных данных, так как каждый суд использует свои способы толкования. При этом, нынешнее толкование судами понятия персональных данных в большинстве своём представляет не что иное как цитирование устаревшей редакции Закона № 152. Исходя из этого, представляется логичным вывод о том, что осуществлённое законодателем изменение (внесение в текст закона поправок) практически не повлияло на практику судов в части толкования понятия персональных данных, так как фактически бывшая легальная часть определения теперь стала частью толкования.

Тем не менее, в доктрине и в СМИ поднимаются некоторые вопросы отнесения тех или иных данных к персональным. Например, существуют проблемы при идентификации личности по полученным данным. Можно ли отнести к персональным данным, например, знания об увлечениях человека, его

---

[28] Приговор № 1-389/2017 1-6/2018 от 2 октября 2017 г. по делу № 1-389/2017 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/kN7MkWMrBlUK/.

[29] Приговор № 1-22/2017 1-378/2016 от 13 февраля 2017 г. по делу № 1-22/2017 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/uFVINSkG4CHZ/.

[30] Приговор № 1-218/2018 от 15 октября 2018 г. по делу № 1-218/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/BTGs3iNkWxUw/.

[31] Приговор № 1-211/2018 от 27 июля 2018 г. по делу № 1-211/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/zUJ8vvZC2Udq/.

[32] Решение № 2-2438/2018 от 23 октября 2018 г. по делу № 2-2438/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/fRg7fDCcbjWK/.

[33] Решение № 2-2193/2018 от 19 октября 2018 г. по делу № 2-2193/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/3BLhkoppApQX/.

[34] Решение № 2-5812/2018 от 5 октября 2018 г. по делу № 2-5812/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/lwgoHBIpJK51/.

[35] Решение № 2-1-547/2018 от 3 октября 2018 г. по делу № 2-1-547/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/n8suO3Gne2Qc/.

[36] Решение № 2-3620/2018 от 27 сентября 2018 г. по делу № 2-3620/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/cFgxlKrkoBV5/.

музыкальном вкусе, или IP адреса? Должны ли персональные данные в совокупности идентифицировать человека или достаточно получения отдельных данных? По данному вопросу существует интересная зарубежная практика, в том числе Европейского Суда по правам человека, в которой Суд признал IP адрес персональными данными, на которые, соответственно, распространяется режим конфиденциальности информации. В своём решении Европейский Суд по правам человека постановил, что динамические IP-адреса могут рассматриваться как персональные данные, даже если они не относятся конкретно к одному человеку, но с оговоркой — если веб-сайт «имеет правовые средства, позволяющие ему идентифицировать посетителя с помощью дополнительной информации, которую имеет о посетителе его Интернет-провайдер[37]». Совершенно очевидно, что в подавляющем большинстве случаев с помощью IP-адресов можно идентифицировать устройство, с которого выполнялся выход Интернет, и круг пользователей, а также их взаимосвязь, если пользователи выходили в сеть с одного IP-адреса. В ситуации, когда устройство принадлежит конкретному человеку и достоверно известно, что никто иной им не пользуется, то имея IP-адрес, идентифицировать человека будет легко. То есть данные, которые не всегда точно могут самостоятельно идентифицировать человека, также можно признавать персональными данными, если они могут отождествиться с конкретным человеком при наличии дополнительной информации. И это раскрывает один из признаков персональных данных – возможность по ним идентифицировать человека, либо по их совокупности. К тому же, 25 мая 2018 года вступил в силу новый европейский регламент GDPR (General Data Protection Regulation). В частности, пункт 30 преамбулы к закону обращает внимание на то, что к персональным данным относятся онлайн-идентификаторы, поскольку они ассоциируются с конкретными физическими лицами, к которым относятся адреса интернет-протоколов (IP-адреса), идентификаторы cookies и другие следы,

[37] Case of Benedik v. Slovenia. The European Court of Human Rights. Application no. 62357/14. 24.04.2018 2018 [Электронный доступ] : The European Court of Human Rights. – Режим доступа: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}.

радиочастотные метки, предпочтения по выбору сайта и так далее[38]. Особое отношение к персональным данным в сети «Интернет» говорит о том, что они безусловно, «валюта» современной жизни.

Относительно адреса электронной почты такой же однозначной позиции не существует. Согласно решению по делу № 12-253/2015 от 26.05.2015. Калининского районного суда (города Санкт-Петербурга) адрес электронной почты обладает режимом конфиденциальности и является персональным данным владельца почты. Но при этом Роскомнадзор считает, что фамилия в совокупности с электронным адресом (а иногда и электронный адрес) могут рассматриваться как персональные данные, только если корпоративные правила компании предусматривают формирование электронной почты в виде сочетания полного имени, фамилии сотрудника и названия компании (например, ivanov.ivan@it-grad.ru)[39]. Такие данные с большой вероятностью позволяют определить конкретного человека. Следовательно, персональные данные считаются таковыми, когда имеются какие-либо признаки или идентификаторы, позволяющие установить конкретное лицо, к которому они относятся.

По поводу передачи персональных данных по электронной почте существует практика Конституционного Суда РФ о конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации»[40]. Оспоренная норма являлась предметом рассмотрения, потому что понимается в правоприменительной практике как позволяющая считать лицо, оказывающее услуги электронной почты, обладателем информации, которая содержится в электронных сообщениях, что служит основанием для оценки действий гражданина, осуществившего

---

[38] General Data Protection Regulation. Wikipedia. [Электронный доступ] : Wikipedia. The Free Encyclopedia. – Режим доступа : https://en.wikipedia.org/wiki/General_Data_Protection_Regulation.

[39] Ответы на вопросы в сфере защиты прав субъектов персональных данных. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный доступ] : Официальный сайт РОСКОМНАДЗОР. – Режим доступа : https://rkn.gov.ru/treatments/p459/p468/.

[40] Постановление КС РФ от 26.10. 2017 № 25-П [Электронный доступ] : Российская газета - Федеральный выпуск № 259(7425) . – Режим доступа : https://rg.ru/2017/11/16/ks-dok.html.

передачу информации с адреса электронной почты, контролируемой лицом, как нарушение им установленного правовыми актами и (или) договорами запрета на такую передачу и, соответственно, для определения правовых последствий этих действий. Оспоренное положение было признано не противоречащим Конституции Российской Федерации, поскольку оно не может рассматриваться как наделяющее правообладателя интернет-сервиса, с помощью которого осуществляются передача электронных сообщений и хранение информации, статусом обладателя информации в отношении сведений, содержащихся в сообщениях, или в отношении информации, которую пользователи хранят с помощью данного интернет-сервиса.

Трудовые отношения работника и работодателя также пронизаны обменом персональных данных. Каждый, кто приходит устраиваться на работу обязан предоставить работодателю ряд сведений о себе. Когда в организациях широко используются автоматизированные информационные системы и их технологии, информация о любом работнике, состоящем с работодателем в трудовых отношениях, может стать в той или иной мере открытой и привести к ущемлению прав и законных интересов работника, причинить ему материальный ущерб и (или) моральный вред. Действующая редакция ТК РФ не содержит 85 статью, которая ранее закрепляла определение персональных данных работника информации, необходимой работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Данное определение было основано на положениях Конвенции Совета Европы «О защите личности в связи с автоматической обработкой персональных данных» и было значительно уже общего определения персональных данных.

Несмотря на то, что действующее законодательство не содержит ни понятие, ни перечень персональных данных работника, можно принимать во внимание статью 85 ТК РФ в ранее действующей редакции и понимать персональные данные работника как любую информацию о нем, необходимую работодателю для принятия на работу и дальнейшего сотрудничества. В пример

можно привести сведения из трудовой книжки, состояние здоровья, сведения о воинской обязанности, образовании или квалификации и т. д., и конечно же важным является тот факт, что эти данные работодатель должен получить добровольно от работника, например, предоставляя документы или заполняя анкеты. Судебная практика так же признает данные о работнике персональными, и активно защищает права работника, в случае, если данные о нем были переданы третьему лицу без его согласия, например, в решении Ачинского городского суда Красноярского края от 06 июля 2016 года[41] или в решении Черноморского районного суда Республики Крым 23 мая 2018 года[42] персональными данными работника были признаны сведения об образовании и воинской обязанности.

Неудачность нынешнего легального понятия состоит также в том, что оно настолько широко, что может включать в себя как данные, являющиеся информацией ограниченного доступа о субъекте, так и данные, по сути, не являющиеся персональными данными ввиду каких-либо особенностей. Такое широкое толкование, часто используемое судами, далеко не всегда свидетельствует о повышении уровня защиты прав субъекта персональных данных, поскольку формальное обращение к защите таких сведений способно привести к существенному нарушению прав, гарантированных другими законодательными актами, зачастую более важными, нежели право на защиту персональных данных. Всё же несмотря на достаточно смелое отнесение судами той или иной информации к персональным данным, у судов существуют некоторые критерии, по которым можно распознать персональные данные. Самым важным и часто встречающимся критерием является возможность идентификации по соответствующим данным конкретного лица. Не можем согласиться с тем, что данный критерий всегда работает и позволяет судам делать логичные выводы, потому что зачастую данные выводят на

[41] Решение № 2-3188/2016 от 6 июля 2016 г. по делу № 2-3188/2016 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа : https://sudact.ru/regular/doc/PbeMmON8wmZP/.

[42] Решение № 2-209/2018 от 23 мая 2018 г. по делу № 2-209/2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа : https://sudact.ru/regular/doc/TtSMpYKDwfor/.

совокупность людей, а не конкретное лицо, в этом случае иногда суд не признает это персональными данными.

Подводя итог вышеизложенному, можно сказать, что при отнесении той или иной информации к персональным данным важно учитывать следующее:

1) Эта информация относится к жизни определенного человека, анализируя которую можно идентифицировать человека.

2) Идентификация человека зачастую происходит при анализе совокупности хотя бы двух данных.

3) Данные о человеке могут находиться в открытом доступе, в связи с чем они потеряют режим конфиденциальности и станут общедоступны.

4) Для передачи персональных данных третьим лицам необходимо получить согласие субъекта этих данных, за исключением случаев, указанных в законодательстве.

На основе этих критериев можно сделать вывод, что персональные данные - это информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу, которая если носит режим конфиденциальности, то требует согласия субъекта для передачи ее третьим лицам за исключением случаев, установленных в законе. Важно учесть, что персональные данные не всегда могут идентифицировать человека по отдельности, часто это можно сделать по совокупности двух - трех данных. Также следует отметить, что отсутствие конкретного перечня персональных данных является существенным пробелом в российском законодательстве. Все же, необходимо установить открытый перечень, что повлечет за собой более разумную судебную практику и более качественный уровень защиты персональных данных.

1.2. Возникновения института персональных данных: российский и зарубежный опыт

Предпосылки возникновения института персональных данных связаны с объективными тенденциями развития общества, а так же с потребностями каждого человека в наличии у него личной информации, которая была бы недоступна для иных лиц, без его согласия на это. Все исторической развитие данного института можно разделить на два обширных этапа. Первый этап связан с довольно фиктивным установлением защиты персональных данных, когда государство, закрепляя некоторые правовые нормы в этой сфере не рассчитывало на их реальное применение, а главным оставался публично-правовой интерес с возможностью вмешательства в частную жизнь любого человека. Конституция Российской Федерации 1993 года стала точкой отсчета второго этапа развития института персональных данных, в котором права и свободы личности были не просто услышаны государственными органами, а получили статус наивысшей ценности. Именно на этом этапе в связи с небывалым темпом развития информационных технологий возникла необходимость охраны персональных данных в сети «Интернет».

Первый этап становления охраны персональных данных можно начать с 1845 года, когда был принят первый закон об уголовной ответственности – Уложение о наказаниях уголовных и исправительных, который упорядочил в себе различные наказания за посягательства на объекты, считающиеся наиболее важными для государства. В первоначальной редакции Уложения, информация о частной жизни никак не охранялась, но в 1866 году были внесены некоторые изменения, касающиеся именно введения ответственности за распространение порочащих сведений о частной жизни, которые составляют тайну: «Оглашение в печати о частном или должностном лице, или обществе, или установление такого обстоятельства, которое могло повредить их чести, достоинству и

доброму имени»[43]. Несмотря на то, что, создавая данную норму государство не рассчитывала исполнять ее, не создавался правовой механизм наказания за оглашение перечисленных сведений, именно она положила начало возникновению охраны персональных данных, совершенствующийся до сих пор.

В качестве дополнения к Уложению, был принят Устав о наказаниях уголовных и исполнительных, налагаемых мировыми судьями, который установил ответственность за оскорбление чести, путем оглашения «сведений, сообщенных в тайне», либо если эти сведения было получены незаконным путем[44].

В 1903 году было принято «Уголовное уложение», ознаменовавшее закрепление новых охраняемых объектов, а также совершенствование охраны уже имеющихся. В нем появились целые главы, посвященные защите лиц от оскорбления и оглашении тайн личной жизни, что позволило законодательству встать на новую ступень в защите личности. Так, в ст. 531 Уголовного уложения содержалась норма об уголовной ответственности за опозорение разглашением, хотя бы в отсутствие опозоренного, обстоятельства, его позорящего[45]. Таким образом, устанавливалась уголовная ответственность за разглашение сведений, которые, по существу, носили позорящий характер для потерпевшего и представляли для него сведения, не подлежащие разглашению.

Интересно отметить, что наступление ответственности за разглашение тайны было только в том случае, если обвиняемый не докажет, что сведения были истинны, либо если есть в этом сомнения, но деяние совершилось для общественной пользы либо для охраны общественного порядка[46]. Существовало и исключение из правила об освобождении от наказания,

---

[43] Лазарев, В. В. Теория государства и права : учебник для академического бакалавриата / В. В. Лазарев, С. В. Липень // 5-е изд., испр. и доп. Издательство Юрайт. – Москва, 2017.

[44] Устав о наказаниях, налагаемых мировыми судьями [Электронный доступ] : Русская энциклопедия Традиция. – Режим доступа : https://traditio.wiki/Устав_о_наказаниях,_налагаемых_мировыми_судьями.

[45] Уголовное Уложение 22 марта 1903 года / Издание Н.С. Таганцева. – СПб., 1904. С. 731.

[46] Там же.

касалось оно разглашения сведений о главе иностранного государства, иностранного посла, поверенного в делах, либо если оглашение произошло в местах скопления людей, в массовой печати или иным образом, рассчитанное на восприятие многими людьми. В таких случаях освобождения от наказания при совершенном преступлении не могло быть ни при каких обстоятельствах.

В противоречие с действующим Уголовным кодексом Российской Федерации, согласно которому наказуемым является любое распространение тайны, относящейся к частной жизни, в Уголовном уложении 1903 года таковым являлось только распространение тайны, порочащей имя либо оскорбляющей другое лицо[47]. На наш взгляд, более верным решением необходимо признать незаконным любое оглашение личной тайны, потому что сам по себе такой факт нарушает права человека на личную и семейную тайну, на неприкосновенность частной жизни.

Все вышеперечисленные нормы были несовершенны, что влияло на применение их в жизни. Не был устроен механизм привлечения к ответственности за такие деяния, не известно было как собирать доказательственную базу, к тому же, в законе существовали оценочные понятия. Например, наличие «достойных уважительния причин» как причина освобождения от наказания за распространение порочащих лицо сведений. В законе не конкретизировано кто именно освобождается от ответственности, в таком случае, и что можно считать достойных уважена наш взгляд, что такое оценочное примечание не давало права на освобождение в принципе из-за широких возможностей усмотрения при назначении виновным лицам наказания.

Следующей исторической ступенью развития института персональных данных, стал Уголовный кодекс РСФСР, принятый в 1922 году. Никакого развития института не происходило, потому что данный период в истории характеризуется защитой лишь публичных интересов государства. Данный

[47] Уголовное Уложение 22 марта 1903 года / Издание Н.С. Таганцева. – СПб., 1904. С. 752.

Уголовный кодекс РСФСР содержал в себе лишь одну статью, предусматривающую ответственность за разглашение должностным лицом не подлежащих оглашению сведений[48]. Это означало, что лишь должностное лицо могло быть субъектом преступления и, вероятнее всего, только при разглашении профессиональной либо государственной тайны. Личная информация других людей, в связи с отсутствием соответствующих норм, никак законодательно не защищалась даже после принятия Уголовного кодекса 1926 года.

Некоторым прорывом в развитии института персональных данных стало принятие Конституции СССР в 1936 году. Она впервые закрепила неприкосновенность частной жизни, тайну переписки, телефонных переговоров, почтовых и телеграфных сообщений[49]. Но нельзя утверждать, что накануне массовых репрессий 1937-1938гг. защите частной жизни уделялось должное внимание. В теоретическом плане это было серьезным достижением советского права, а в практическом – всего лишь формальностью.

Начиная с 1940-х годов проблема нарушений прав человека исчезла в связи с установлением тоталитарного режима. Несмотря на то, что в мировой практике институт персональных данных развивался и уже приспосабливался к новым техническим методам охраны сведений, в СССР была уничтожена вся та законодательная база, которая так долго формировалась.

В 80-х годах прошлого столетия, когда резко повысился рост преступности, началось активное развитие инфраструктуры и рыночных отношений, все подразумевало активное изменение законодательства. Исключением не стала и охрана личной информации, и несмотря на то, что Уголовный кодекс РСФСР 1960 года не предусматривал такой объект охраны, позже в него внеслись изменения, в результате которых введены нормы о

[48] Уголовный кодекс РСФСР [Электронный ресурс] : федер. закон от 01.06.1922 // Федеральный правовой портал Юридическая Россия. – Режим доступа: http://www.law.edu.ru.

[49] Конституция Российской Федерации [Электронный ресурс] : федер. закон от 25.12.1993 ред. от 21.07.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

нарушении тайны переписки, а также о разглашении тайны усыновления. Иные сведения не подлежали охране со стороны государства, но данный кодекс можно считать началом переломного момента, когда государство стало принимать во внимание частноправовые интересы своих граждан.

Точкой отсчета второго этапа развития института персональных можно считать появление Конституции РФ в 1993 году. Она стала первой и единственной за всю российскую историю конституцией, включавшей в отдельном разделе стандартный для развитых европейских стран комплекс гражданских, политических, экономических, социальных и культурных прав. Развитие общества создало доступную среду для обмена информацией, в том числе в сети «Интернет», где огромные потоки информации ежедневно собираются, накапливаются и передаются, что обеспечивает плодородную почву для различного рода преступлений. Повышение риска утечек информации с последующим несанкционированным ее использованием обусловило необходимость создания действующего механизма защиты информации.

Всем известно, что информация всегда была необходимым элементом государственного управления. Во все времена государство собирало информацию о населении, как с помощью государственных органов, так и с помощью церкви. С оглашения демократического пути развития России государству становится все сложнее и сложнее обрабатывать информацию о населении и всему виной возросшие потребности людей в сохранении своей личной информации и обеспечении неприкосновенности частной жизни. И государство, и общество понимает, что обеспечение частноправовых интересов личности встает на место более приоритетное, чем это было в СССР и более ранние периоды.

Таким образом, три объективных фактора - потребность государства в полной и достоверной информации о населении, потребность индивида в неприкосновенности частной жизни на фоне стремительной интеграции и

глобализации и прорывное развитие информационных технологий - обусловили появление в правовой науке специальной юридической категории, получившей название «персональные данные».

Термин «институт» часто употребляется в неопределенно широком смысле: говорят, например, о социальных, политических, экономических институтах общества. При этом могут подразумеваться самые разнообразные и разнородные явления. Однако в данном случае речь идет о сугубо юридическом понятии института, которое традиционно рассматривается как совокупность правовых норм, составляющих часть отрасли права и регулирующих определенный вид или сторону однородных общественных отношений[50].

Перечисленные в Конституции РФ гарантии подкреплялись некоторыми нормативно-правовыми актами, например, 20 февраля 1995 г. был принят Федеральный закон № 24-ФЗ «Об информации, информатизации и защите информации», непосредственно регулирующий права граждан в сфере информации, а 4 июля 1996 г. - Федеральный закон № 85-ФЗ «Об участии в международном информационном обмене». Эти Федеральные законы стали первыми актами, содержащими в себе понятия и принципы в области охраны персональных данных. В них персональные данные относились к конфиденциальной информации и им обеспечивался особый режим охраны. Соответственно, физические и юридические лица должны были нести ответственность за разглашение сведений о третьих лицах, но данные нормы так и не были воплощены в жизнь в связи с отсутствием ответственности за их нарушение.

Первые законодательные попытки по охране персональных данных были достаточно стихийны и неконкретны, например, оставалось не ясно какую именно информацию относить к персональным данным. Первым же шагом в создании комплексного правового регулирования института персональных

[50] Лазарев, В. В. Теория государства и права : учебник для академического бакалавриата / В. В. Лазарев, С. В. Липень. – 5-е изд., испр. и доп. – Москва : Издательство Юрайт, 2017.

данных личности являлась ратификация Россией Конвенции о защите физических лиц при автоматизированной обработке данных личного характера[51]. Она содержит определения основных понятий в сфере персональных данных и устанавливает общие принципы, например, добросовестность, законность, целевое соответствие, точность получения и обработки данных, их защита от несанкционированного использования, усиленный режим охраны особых категорий сведений. Именно данная Конвенция подтолкнула российского законодателя на создание Закона о персональных данных, в котором было раскрыто большинство положений Конвенции. Тем более, к моменту подготовки российского законопроекта в странах Совета Европы уже давно действовали соответствующие законы и был накоплен определенный нормотворческий опыт, который частично был учтен российскими законодателями. В результате был принят Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», вступивший в силу 26 января 2007 г. (далее - Закон о персональных данных).

В Законе даны определения таких понятий, как «персональные данные», «оператор», «обработка персональных данных», «конфиденциальность персональных данных» и др.; закреплен достаточно эффективный механизм противодействия нарушениям прав физических лиц в сфере оборота персональных данных. Закон обеспечивает правовую защищенность личности в условиях информационного общества и создает предпосылки для укрепления внешнеполитических позиций нашего государства.

Вместе с тем Закон о персональных данных имеет и недостатки. Так, нельзя не отметить, что основное внимание в нем уделено техническим вопросам обработки персональных данных и порядку деятельности операторов. Значительно хуже разработаны исходные общетеоретические положения о

[51] О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс] : закон РФ от 19.12.2005 № 160 // Информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

целях и задачах Закона, о статусе персональных данных как таковых, об общих принципах оборота персональных данных в Российской Федерации.

Во-первых, упущения в теоретическом плане в совокупности с доминирующим описанием технических и технологических проблем проявляет пренебрежительное отношение к основополагающим вопросам защиты прав и свобод человека, расставляя приоритет на более специальные проблемы обработки и оптимального использования информации в различных целях.

Во-вторых, в рассматриваемом Законе не слишком удачно применен термин «обработка персональных данных». Согласно тексту Закона он обозначает все возможные действия (операции) с персональными данными, а именно: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение[52]. Однако в русском языке слово «обработка» обычно используется в более узком значении и семантически обозначает только одно - действие от глагола «обрабатывать», «обработать»[53]. По нашему мнению, для обозначения всех вышеперечисленных действий с персональными данными идеально подходит термин «оборот», который к тому же достаточно широко используется в российском законодательстве[54]. Слово «оборот» обычно означает «полный повторяющийся цикл в каком-либо процессе, употреблении, применении, использовании»[55].

На основе Закона о персональных данных стали приниматься различные приказы и инструкции, касающиеся, например, обработки данных средствами автоматизации или охраняющих лишь сведения, составляющие государственную тайну. Одним из таких приказов является Приказ ФСТЭК

---

[52] О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 №152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[53] Словарь синонимов русского языка [Электронный ресурс] : З. Е. Александрова. Практический справочник. М.: Русский язык, 2001. – Режим доступа: https://alleng.org.

[54] Об обороте земель сельскохозяйственного назначения [Электронный ресурс] : федер. закон от 24.07.2002 ред. 01.05.2019 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[55] Словарь синонимов русского языка [Электронный ресурс] : З. Е. Александрова. Практический справочник. М.: Русский язык, 2001. – Режим доступа: https://alleng.org.

России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Он представляет интерес в связи с закреплением мер по обеспечению безопасности персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий. Среди таких мер указана антивирусная защита, выявление инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и реагирование на них, обеспечение целостности информационной системы и персональных данных.

Защиту персональных данных он несанкционированного использования может обеспечить, например, их обезличивание, чему и посвящен приказ Роскомнадзора от 05.09.2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных». В нём дается понятие обезличивания как действия в результате которого становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных[56]. Достаточно действенным методом можно считать введение идентификаторов (замена части сведений идентификаторами с созданием таблицы соответствия идентификаторов исходным данным). Такой метод позволяет провести процедуру деобезличивания, а также структурировать данные в любой автоматизированной системе, что не влечет за собой потерю идентификации с определенным лицом.

Анализируя развитие законодательства об охране персональных данных можно с уверенностью сказать, что Россия совершила огромный шаг к созданию демократического государства, где приоритетом является частноправовой интерес личности. Принятие Конституции РФ 1993 года и

[56] Об утверждении требований и методов по обезличиванию персональных данных [Электронный ресурс] : приказ Роскомнадзора от 05.09.2013 № 996 // Сайт «Законы, кодексы и нормативно-правовые акты в Российской Федерации». – Режим доступа: http://legalacts.ru.

объявление прав и свобод человека и гражданина высшей ценностью потребовало создание нормативно-правовой базы охраны личной жизни каждого. На смену декларативным нормам пришел Закон о персональных данных, хоть и содержащий оценочные понятия, но ставший мощным фундаментом для появления других нормативных актов. Вместе они создают единую правовую базу, позволяющую каждому человеку чувствовать защищенность и неприкосновенность частной жизни. Но не стоит игнорировать и международный опыт становления института персональных данных, ведь все же Россия основывается на уже проверенном опыте других стран, заимствовав те или иные идеи, уже проверенные на практике.

Юридические предпосылки с охране персональных данных впервые появились в США. Известные американские юристы Сэмюэль Уоррен и Луис Брандейс уже в 1890 году сформулировали понятие «privacy» как право быть оставленным в покое или право быть предоставленным самому себе[57]. В своей статье «Право на приватность» в Гарвардском правовом журнале они утверждали, что приватность подвергается опасности со стороны новых изобретений и методов ведения бизнеса, и обосновывали необходимость создания специального «права приватности». В наши дни мы понимаем, что американские юристы смотрели далеко вперед, предполагая технический прорыв, когда защита частной жизни будет зависит от множества технологий, не всем людям подвластных.

Огромную роль в становлении и формулировании права на частную жизнь сыграла деятельность американских судов. Так, в 1965 г. в деле Griswold v. Connecticut судья Верховного суда США Дуглас признав, что право приватности «охраняет различные аспекты неприкосновенности частной жизни». Широко известны слова, которые он произнес, резюмируя решение

[57] Важорова, М. А. История возникновения и становления института персональных данных / М. А. Важорова // Государство и право: теория и практика: материалы Междунар. науч. конф. – Челябинск, 2011. – С. 33.

суда: «Мы имеем дело с правом на неприкосновенность частной жизни, которое старше, чем Билль о правах[58]».

10 декабря 1948 года на Генеральной Ассамблеи ООН была утверждена Всеобщая Декларация прав человека, в статье 12 которой устанавливалось, что никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность жилища, тайну его корреспонденции или на его честь и репутацию; каждый человек имеет право на защиту закона от такого вмешательства и таких посягательств[59]. В 1950 году аналогичная норма была закреплена в статье 8 Европейской конвенции о защите прав человека и основных свобод в следующей формулировке: «каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции»[60]. Благодаря данным документам право на неприкосновенность частной жизни получило признание в качестве неотъемлемого права каждого человека.

Впоследствии в Директиве Европейского парламента и Совета Европейского союза от 24 октября 1995 г. №95/46ЕС о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных были заложены основы общеевропейской системы защиты персональных данных[61]. В 2000 году в Хартии Европейского союза об основных правах право на защиту персональных данных было сформулировано в качестве самостоятельного фундаментального[62].

---

[58] Важорова, М. А. История возникновения и становления института персональных данных / М. А. Важорова // Государство и право: теория и практика: материалы Междунар. науч. конф. – Челябинск, 2011. – С. 34.

[59] Всеобщая декларация прав человека [Электронный доступ]: всеобщая декларация прав человека принятая Генеральной Ассамблеей ООН 10.12.1948 // Информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

[60] Европейская конвенция о защите прав человека и основных свобод ETS №005 [Электронный ресурс] : Конвенция о защите прав человека и основных свобод (Заключена в г. Риме 04.11.1950) (с изм. от 13.05.2004) // Информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

[61] Директива Европейского Парламента и Совета Европейского Союза [Электронный доступ]: директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24.10.1995 // Информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

[62] Хартия Европейского Союза об основных правах [Электронный доступ]: хартия Европейского Союза об основных правах от 12.12.2007 // Информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

Таковы основные этапы формирования нормативного механизма о защите персональных данных на европейском континенте. Заключительным этапом его формирования стало принятие национальных законов стран - участниц Европейского союза, направленных на регулирование вопросов защиты персональных данных. Первый в мире специальный Закон о защите персональных данных был принят германской землей Гессен в 1970 году[63]. До этого подобных законов нигде в мире не было. За последние года более чем в 20 европейских государствах были приняты нормативные акты по защите персональных данных, в которых были закреплены реальные механизмы правового регулирования оборота персональных данных.

Сравнивая же развитие международного законодательства с российским можно заметить, что наша страна достаточно поздно стала учитывать частноправовые интересы личности по сравнению с другими странами. В то время, когда СССР создавал декларативные нормы, на международной арене право человека на охрану персональных данных стало уже фундаментальным и это крайне важно, учитывая развитие технологий и все новые способы несанкционированного использования данных. Учитывая глобальный характер проблемы, России необходимо учитывать опыт других стран и совершенствовать свое законодательство в сфере охраны персональных данных.

[63] Важорова, М. А. История возникновения и становления института персональных данных / М. А. Важорова // Государство и право: теория и практика: материалы Междунар. науч. конф. – Челябинск, 2011. – С. 37.

Глава 2. Криминологический анализ преступлений в отношении персональных данных, совершаемых в сети Интернет

2.1 Преступления в отношении персональных данных, совершаемые в сети Интернет

Общеизвестно, что уголовная ответственность самая суровая среди всех видов наказаний. Она назначается за посягательства на самые основные объекты жизни всего общества, и только при наличии состава преступления, предусмотренного Особенной частью УК РФ. Согласно законодательству Российской Федерации, к лицам, совершившим виновные деяния в отношении персональных данных уголовная ответственность применяется при квалификации по четырем статьям УК РФ. Уголовный кодекс РФ не дает понятие, что такое персональные данные и не содержит составов преступлений, где бы они были записаны как объект преступления. Но, тем не менее, из всего ряда статей кодекса можно выделить некоторые, касающиеся преступлений в отношении того или иного вида персональных данных (Ст. ст. 137, 138, 140, 272 УК РФ).

Для общего понимания всех посягательств в отношении персональных данных в сети Интернет считаем необходимым ознакомиться с каждым из преступлений, оценить их динамику за последние годы. Начнем со ст. 137 УК РФ, а именно «нарушение неприкосновенности частной жизни». Возникает закономерный вопрос: тождественны ли понятия «частная жизнь» и «персональные данные»? Определения первого понятия в законодательстве нет, как и нет перечня явлений, входящий в частную жизнь, что естественно затрудняет применение данной нормы.

В настоящее время, доктринально понятие частной жизни хорошо изучено, например, М. В. Баглай понимает частную жизнь как суверенитет личности, неприкосновенность тех сторон его жизни, которые она не желает

делить с другими[64]. Г. Б. Рамоновский придерживается той же позиции, только еще конкретизирует, что частная жизнь включает в себя убеждения, хобби, привычки, симпатии, религиозные убеждения, то есть внутренний мир человека, а также его связи с другими людьми, например, знакомства, беседы или запись на прием к стоматологу[65]. Однако, существует определение Конституционного суда, в котором наиболее точно и полно отражается суть понятия «частная жизнь», как области жизнедеятельности человека, которая относиться к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер[66]. Получается, что «частная жизнь» гораздо шире понятия «персональные данные», ведь включает в себя не только информацию идентифицирующую человека, и ее можно определить, как «данные о человеке и мера его возможного поведения, не попадающее под прямое воздействие государственных органов и являющиеся суверенитетом личности при взаимодействии с окружающим миром».

Исходя из вышесказанного, получается, что персональные данные являются важнейшим элементом частной жизни человека, тем самым, нарушение режима неприкосновенности частной жизни нарушает права человека в области защиты его персональных данных. Применительно к теме нашего исследования, суть данного преступления можно выразить в: незаконном собирании или распространении персональных данных без согласия субъекта этих данных в сети Интернет. Данную норму можно назвать самой общей, и именно ее чаще всего суды применяют к деяниям, нарушающим оборот персональных данных. Согласно статистическим исследованиям, за 2018 год в России по ст. 137 УК РФ было осуждено 127 человек, из них только 11 были приговорены к лишению свободы, а в основном

---

[64] Баглай, М. В. Конституционное право Российской Федерации / М. В. Баглай // Норма. – Москва, 2009. – С. 181.

[65] Романовский, Г. Б. Право на неприкосновенность частной жизни / Г. Б. Романовский // МЗ – Пресс. – Москва, 2001. – С. 63-65.

[66] Определение Конституционного Суда РФ от 09.06.2005 г. № 248-О [Электронный доступ]: информационно-правовой портал «Гарант.ру». – Режим доступа: https://base.garant.ru/1354478/.

суды в качестве мер наказания использовали штраф. Если же поглядеть на статистику прошлых лет, то можно увидеть явное увеличение с каждым годом числа осужденных по данной статье, например, в 2017 году виновных было 86 человек, а в 2016 году всего 59 по всей России[67]. Такая динамика вполне очевидна в современном обществе, где государство становится на защиту частноправовых интересов человека, выявляя подобные преступления, а люди развивают свое правосознание, замечая нарушения своих прав и стремятся сделать все, чтобы защитить себя. Вероятно, увеличение числа преступлений в данном случае зависит от уменьшения латентности, опять же, благодаря правосознанию людей и уже сложившейся судебной практики, в связи с чем, такая тенденция сохранится и в последующие годы. К тому же, как было сказано выше, ст. 137 УК РФ является самой общей среди охраняющих персональные данные, благодаря чему, суды выбирают именно данную норму при наличии сомнений при квалификации.

Следующей нормой, касающейся охраны персональных данных является ст. 138 УК, она закрепляет ответственность за преступление, объектом которого является тайна переписки, телефонных и иных переговоров. Посягательство в данном случае происходит в виде ознакомления с сообщениями или телефонными разговорами, содержащие персональные данные, без согласия на то субъекта информации и без законных на то оснований. Количество осуждённых по данной статье за 2018 год 41 человек, из них только 9 были приговорены к лишению свободы, а большинство к обязательным работам. Если сравнивать данные показатели с предыдущими годами, то можно увидеть, что состояние преступности по ст. 138 УК РФ в России является стабильным, в 2017 году осуждено было 48 человек, а в 2016 году 42 человека[68]. Не известно, какое количество преступлений было совершено в сети Интернет, но такая судебная практика существует, например, Калужский районный суд

[67] Агентство правовой информации. Статистика [Электронный доступ]: Агентство правовой информации. – Режим доступа: http://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17.

[68] Агентство правовой информации. Статистика [Электронный доступ]: Агентство правовой информации. – Режим доступа: http://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17.

приговорил у уголовному наказанию виновное лицо, которое ознакомилось с перепиской потерпевшего с иными пользователями электронной почты без его согласия на это[69]. Также, примером является приговор Федерального суда общей юрисдикции Дзержинского района г. Новосибирска, в котором суд признал виновным лицо, которое, имея доступ к информационно-телекоммуникационной сети Интернет, узнавало номера исходящих и входящих соединений абонентов, после чего предоставлял указанные данные другому лицу для получения полных персональных данных абонентов[70]. Исходя из современной ситуации повсеместного распространения сети Интернет, можно предположить, что подобные деяния будут совершаться все чаще и чаще, ведь не все ответственно относятся к сохранности сообщений, информации о звонках в мессенджерах и социальных сетях, а получить эту информацию, пользуясь доверием очень просто. Необходимо поднимать уровень правосознания людей, ведь пока подобные нарушения охраны персональных данных будут латентными, их количество будет только возрастать, а судебная практика не будет развиваться в данном направлении.

Статья 140 УК РФ тоже затрагивает тему оборота персональных данных, а именно неправомерного отказа должностного лица гражданину в доступе к своим персональным данным, содержащихся в картотеках государственных органов. К тому же, возможно привлечение к уголовной ответственности по ст. 140 УК РФ в связи с неисполнением оператором обязанности, указанной в ст. 18 Закона о персональных данных, а именно непредставление информации о процедуре обработки данных гражданина. К сожалению, данная норма в России является недействующей, ведь согласно статистики за последние три года судами не было вынесено ни одного обвинительного приговора[71].

---

[69] Приговор № 1-878/1/2017 1-878/2017 от 15 декабря 2017 г. по делу № 1-878/1/2017 [Электронный доступ]: Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/1KmWTdMX4qHo/.

[70] Приговор № 1-389/2017 1-6/2018 от 2 октября 2017 г. по делу № 1-389/2017 [Электронный доступ]: Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/kN7MkWMrBlUK/.

[71] Агентство правовой информации. Статистика [Электронный доступ]: Агентство правовой информации. – Режим доступа: http://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17.

Заключительной статьей, содержащей запрет на незаконный оборот персональных данных можно назвать ст. 272 УК РФ, а именно за неправомерный доступ к компьютерной информации, повлекший уничтожение, блокирование, модификацию либо копирование компьютерной информации. Под такой информацией можно понимать в том числе персональные данные лица или группы лиц, к которой неправомерно получили доступ третьи лица.

В современном мире преступления с компьютерным аспектом совершаются все чаще, в том числе, требующие значительную подготовку и специальные знания. Поскольку в большинстве случаев деятельность операторов систем персональных данных автоматизирована и зависима от компьютерного оборудования, то неправомерные доступы к таким системам будут только учащаться в связи с развитием технологий и разработки новых способов «взламывания» систем. Данная норма играет в том числе и важную превентивную роль в отношении людей, которые «взламывают» компьютерные сети различных учреждений, банков ради спортивного интереса, а не ради доступа к данным. Несмотря на кажущуюся распространенность неправомерного доступа к компьютерной информации с последствиями, описанными в норме, статистика показывает, что за 2018 год только 50 человек по всей России были осуждены за данное преступление, из них 19 приговорены к лишению свободы. Если же учитывать предыдущие годы, то нельзя выявить какую-либо закономерность, потому что в 2017 году осуждено было 74 человека, а в 2016 году 62 человека по всей России[72].

На практике существует проблема квалификации деяний по ст. 137 УК РФ и 272 УК РФ, связанная с вменением только одной из этих статей при посягательстве на частную жизнь в сфере компьютерной информации. Например, Ставропольский краевой суд установил, что Ю. признан виновным в незаконном собирании сведений о частной жизни лица, составляющих его личную и семейную тайну, без его согласия. Преступление совершено путем

[72] Агентство правовой информации. Статистика [Электронный доступ]: Агентство правовой информации. – Режим доступа: http://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17.

неправомерного доступа к информации, содержащейся на её персональном компьютере, а именно в аккаунте социальной сети «Вконтакте»[73]. Сравнимые статьи имеют некоторое отличие, если ст. 137 УК РФ охраняет персональные данные в качестве частной жизни, и здесь важен содержательный аспект, то ст. 237 УК РФ охраняет персональные данные в сфере оборота компьютерной информации, то есть важен аспект формальный. В вышеизложенном примере как раз проявляется нарушение оборота персональных данных, являющихся частной жизнью, и, в то же время, компьютерной информацией, но суд, квалифицируя деяние только по ст. 137 УК РФ не учел факт неправомерного доступа именно к компьютерной информации. В то же время, Городецкий городской суд Нижегородской области квалифицировал деяние П., а именно, «взлом» электронной почты с последующим ознакомлением и удалением фотографий, сообщений только как неправомерный доступ к охраняемой законом компьютерной информации, без учета того, что информация являлась элементом частной жизни[74]. Суды не учитывают, что посягательство на компьютерную информацию может быть элементом посягательства на персональные данные, составляющие частную жизнь человека. Например, Ю. В. Гаврилин пишет о том, что «в тех случаях, когда неправомерный доступ к компьютерной информации выступает способом совершения другого умышленного преступления, а электронно-вычислительная техника используется как орудие для достижения преступной цели, содеянное должно быть квалифицировано по совокупности преступлений»[75]. Р. Р. Гайфутдинов указывает, что «подобного рода преступные деяния будут являться двухобъектным посягательством. При уголовно-правовой оценке действия лица будут образовывать разнообъектную идеальную совокупность преступлений, квалифицируемых соответственно по ст. 137 и ст. 272 УК РФ. Субъект

[73] Апелляционное постановление № 22-6353/2018 от 15 ноября 2018 г. по делу № 22-6353/2018 [Электронный доступ]: Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/60mfkd1UoDQr/.

[74] Приговор № 1-133/2018 от 25 июля 2018 г. по делу № 1-133/2018 [Электронный доступ]: Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/tHIOr1LSy3Ya/.

[75] Научно-практический комментарий к ст. 272 УК РФ [Электронный доступ]: Образовательный портал Geum.ru. – Режим доступа: http://geum.ru/lav/index-42778.php.

осуществляет посягательство, с одной стороны, на отношения по поводу обеспечения целостности и сохранности компьютерной информации, а с другой – на конституционные права неприкосновенности частной жизни, личной и семейной тайны»[76]. И с этими двумя точками зрения нельзя не согласиться. Рассматриваемые статьи наиболее часто избираются судами при квалификации деяний, при этом санкция у них различна. Предлагается использовать идеальную совокупность с. 137 УК РФ и 272 УК РФ при назначении наказания за нарушение неприкосновенности частной жизни, которая была выражена в незаконном доступе к компьютерной информации. Только так можно отразить посягательство сразу на два объекта, повлекшее два разных последствия, охватывающих две статьи Особенной части УК РФ.

Подводя итог, следует отметить, что законодательство и судебная практика по преступлениям, связанным с оборотом персональных данных в сети Интернет не совершенно. Также, такие преступления составляют незначительную часть от всего объема преступлений, что является в большей части признаком латентности в связи с нежеланием субъектов данных регистрировать нарушения их прав. Согласно результатам проведенного нами анкетирования, ни один человек из тех, чьи персональные данные подвергались незаконному воздействию не обращался в правоохранительные органы. Также значительного увеличения обвинительных приговоров по ст. ст. 137, 138, 140, 272 УК РФ в последний год не наблюдается, за исключением нормы за нарушение неприкосновенности частной жизни, но для более объективной оценки посягательств на персональные данные необходимо пересмотреть судебную практику, отметив возможную идеальную совокупность ст. 137 УК РФ и 272 УК РФ в ряде случаев.

[76] Гайфутдинов, Р. Р. Уголовно-правовая характеристика посягательства на персональные данные, обрабатываемые в автоматизированных системах / Р. Р. Гайфутдинов // Учёные записки Казанского университета. Серия: Гуманитарные науки №4. – Казань, 2014. – С. 159.

2.2 Анализ механизма преступных посягательств в отношении персональных данных, совершаемых в сети Интернет

Все люди, живущие сейчас, наблюдают за очередным прорывом человека в информационной сфере. Такой уровень развития технологий казался немыслимым еще двадцать лет назад, в связи с чем и образ жизни людей существенно изменился. Информационно-телекоммуникационная сеть Интернет, прочно закрепив свое положение в повседневной жизни человека, стала не только сферой для общения, сотрудничества, образования, но и для конкуренции, противоправных действий. В криминологическом исследовании важно изучить взаимодействие свойств личности и конкретной жизненной ситуации, называемое механизмом преступного поведения. Основные элементы данного механизма – психические процессы и состояния, а также факторы внешней среды, то есть причины и условия конкретного преступления. А. И. Долгова разделяет криминальное поведение человека на четыре этапа: формирование мотивации, принятие решения о совершении преступления и планирование его, исполнение решения и посткриминальное поведение. Последний этап достаточно неоднозначен в связи с тем, что не все его выделяют как значимый в криминальном поведении, например, Л. М. Прозументов и Л. В. Шеслер ограничивают свое исследование тремя первыми этапами, описанными А. И. Долговой[77].

Мотивация содержит в себе процесс возникновения, формирования преступного поведения и его цели. Мотивы выполняют функции возбудителя преступного поведения личности, начала формирования решения о совершении преступления. Наиболее характерными мотивами лиц, совершающих преступления в сфере оборота персональных данных, можно считать: корыстные, хулиганские, игровые, исследовательский интерес, потребность в самоутверждении, месть. Мотивами преступных действий несовершеннолетних обычно являются исследовательский интерес, самоутверждение и жажда славы,

[77] Долгова, А. И. Криминология. Учебник для вузов /Под общ. ред. д. ю. н.,проф. А. И. Долговой // — 3-е изд., перераб. и доп. – М.: Норма. – Москва, 2005. – С. 365 - 366.

возможность проверки своих способностей на практике. С развитием социальных сетей информация о частной жизни граждан, размещаемая там, все чаще становится объектом преступных посягательств. Наиболее распространенным мотивом в данном случае является ревность со стороны близких и знакомых пострадавших. Так, по делу № 1-678/2018 Советского районного суд г. Казани, К., имея доступ к персональным данным абонентов, содержащих охраняемую законом тайну, из личной заинтересованности, в связи с раннее сложившейся конфликтной ситуацией, вызванной ревностью, решила получить сведения о телефонных переговорах абонентов потерпевших без их согласия и в отсутствие на то законных оснований[78]. В качестве цели преступник желает видеть конфиденциальную информацию об интересующем его человеке для удовлетворения личного интереса либо получения денежных средств от передачи этой информации третьи лицам.

Второй этап характеризуется принятием решения и планированием поведения. Здесь у человека возникает внутренняя борьба с самим собой, внутренний самоконтроль может удержать от совершения преступления даже при точно сформулированном мотивое на предыдущем этапе. При принятии решения о совершении преступления важную роль играет анализ последствий, соотношение всех «за» и «против» преступного поведения и возможности достижения цели. Например, если человек обдумывает получение материальной выгоды после доступа к персональным данным и знает, что обычно за подобное деяние назначается незначительный штраф, то получается, что совершить преступление выгодно. После принятия решения лицо начинает избирать средства достижения цели, в нашем случае это может быть получение доверия от третьего лица с просьбой поделиться паролем от аккаунта в социальной сети или электронной почте, приискание оператора персональных данных, способного допустить к ним за вознаграждение и т. п.

[78] Постановление № 1-678/2018 от 13 сентября 2018 г. по делу № 1-678/2018 2018 [Электронный доступ]: Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/JGUHXNS8aBd8/.

После принятия решения наступает стадия его исполнения. Фактический ход совершения преступления может отличаться от задуманного, например, целью могло быть ознакомление с перепиской третьего лица, а по факту удалось получить доступ еще и к другой информации, либо же в процессе совершения преступления могут возникнуть дополнительные трудности. Для оценки действий важно знать с помощью каких средств было совершено преступление, ведь как мы уже выяснили, нарушение оборота персональных данных может квалифицироваться по ст. 137 УК РФ, а может образовывать совокупность со ст. 272 УК РФ, если присутствовал неправомерный доступ к компьютерной информации.

Распространение совершения изучаемых преступлений среди несовершеннолетних позволяет выделить их особенность, а именно свернутый характер преступного поведения. Это означает, что преступление происходит «здесь и сейчас» после появления какого-либо благоприятного условия, способствующего развитию преступной идеи. Для такого поведения характерна импульсивность, стремление показать свои способности перед третьими лицами, состояние алкогольного опьянения и отсутствие мыслей о последствиях, в связи с чем, этапы мотивации, принятия и исполнения решения практически совпадают, и выделить временной промежуток конкретного этапа невозможно.

На последнем этапе преступного поведения анализируется произошедшее, осознаются последствия, возможно принимаются попытки избежать уголовной ответственности и т. д. В некоторых случаях, преступления, связанные с оборотом персональных данных, даже не осознаются виновным, например, если доступ к данным был не затруднен, и преступное поведение возникло из-за любопытства и чрезмерного доверия со стороны потерпевшего. Если же деяние было осознанным, то преступник на данном этапе сравнивает достигнутое с желаемым, возможно раскаивается, пытается удалить следы, вырабатывает психологическую защиту от обвинения.

Например, Одинцовский городской суд Московской области приговорил Д. к уголовному наказанию по ч. 2 ст. 272 УК РФ за неправомерный доступ к охраняемой законом компьютерной информации, изменение пароля доступа к аккаунту, модификацию компьютерной информации. После совершения противоправных действий Д. осознал нарушение закона, но, так как изменения в аккаунте уже нельзя было предотвратить, он удалил историю браузера в надежде избежать ответственности[79].

Немаловажным элементом преступного поведения являются причины и условия, способствующие совершению преступления. Поиск этих факторов сопровождает людей уже достаточно длительное время. Во второй половине XIX и в начале XX в. основным направлением было биолого-антропологическое, развивавшее ломброзианские идеи. Одним из типичных представителей его был Э. Кречмер, ставящий в зависимость от психофизической конституции характер и склонности человека, в т. ч. и преступные. Второе направление – психоаналитическое. Его представитель З. Фрейд преступность объяснил давлением подсознательных, главным образом, сексуальных влечений[80]. Позднее стали считать, что причиной преступности может быть низкий уровень образования населения как в научном плане, так и в культурном, и, возможно, именно благодаря увеличению числа людей с высшим профессиональным образованием и развитию культуры в стране, с 2015 года замечено сокращение общего числа преступлений на территории России[81].

Причины необходимо отделять от условий преступности, потому что оба явления являются социальными, но причины порождают преступность как свое закономерное следствие, а условия лишь способствуют, облегчают

[79] Приговор № 1-394/2014 от 23 мая 2014 г. по делу № 1-394/20142018 [Электронный доступ]: судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/jj74tyQZBMWW/.

[80] Дворецкий, М. Ю., Авдеев, Р. В. Причины и условия преступности / М. Ю. Дворецкий, Р. В. Авдеев // Вестник ТГУ. Серия: Гуманитарные науки. – Томбов, 2014. – С. 3-5.

[81] Портал правовой статистики [Электронный доступ]: Генеральная прокуратура РФ. Портал правовой статистики. – Режим доступа: http://crimestat.ru/offenses_map.

формирование причин[82]. В качестве причин преступности выступают те социальные явления с которым связана закономерность возникновения преступности. Установление причин конкретного преступления означает выявление факторов, играющих наиболее активную роль в его генезисе[83].

По мнению В. С. Карпова, существует две основные причины возникновения компьютерной преступности в целом – полная автоматизация систем данных в учреждениях, предприятиях, организациях и возможность в современном мире получения материальной выгоды от полученной информации[84]. К.Н. Евдокимов выделяет еще одну причину компьютерных преступлений, относимых в том числе к нарушению оборота персональных данных - недостаточное правовое регулирование отношений по защите персональных данных в сети Интернет, недостаточный понятийный аппарат, дозволение со стороны закона использовать оценочные понятия при решении вопроса об уголовной ответственности[85]. Еще Ч. Беккариа отмечал, что «одно из самых действенных средств, сдерживающих преступления, заключается не в жестокости наказаний, а в их неизбежности и, следовательно, в бдительности властей»[86].

Учитывая вышесказанное можно выделить еще несколько причин преступлений в отношении персональных данных в сети «Интернет»:

1. Рост информационного обмена через социальные сети, мессенджеры, в связи с чем увеличивается объем персональных данных, обрабатываемой и хранимой в ЭВМ;
2. Недостаточность мер по защите ЭВМ, программного обеспечения;

---

[82] Кузнецова, Н. Ф., Лунеева, В. В. Криминология: учебник / Н. Ф. Кузнецовой, В. В. Лунеева // Волтерс Клувер. – Москва, 2005. – С. 167 – 168.

[83] Дворецкий, М. Ю., Авдеев, Р. В. Причины и условия преступности / М. Ю. Дворецкий, Р. В. Авдеев // Вестник ТГУ. Серия: Гуманитарные науки. – Томбов, 2014. – С. 6-7.

[84] Карпов, В. С. Уголовная ответственность за преступления в сфере компьютерной информации: дис. … канд. юр. наук: 12.00.08 / Карпов Виктор Сергеевич. – Красноярск, 2002.

[85] Евдокимов, К. Н. Проблемы противодействия неправомерному доступу к компьютерной информации: Уголовно-правовые и криминологические аспекты / К. Н. Евдокимов // Монография. – Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2013

[86] Беккариа, Ч. О преступлениях и наказаниях. / Ч. Беккариа // ИНФРА-М. – Москва, 2004. – С. 123–124.

3. Искажение нравственных ценностей и правосознания населения;

4. Неразвитость системы виктимологической профилактики преступлений.

Вторым важным фактором появления преступности являются ее условия. Факторы, выступающие в качестве причин, без условий не могут в полной мере способствовать преступности. Именно связь причин и условий порождает следствие – преступление и называется криминогенным детерминантом[87]. Среди условий совершения преступлений в отношении персональных данных, совершаемых в сети Интернет, можно отнести следующие:

1. Несовершенство парольной системы защиты от несанкционированного доступа с социальной страницы, электронной почты и т. д.;

2. Низкий уровень программного обеспечения, позволяющий «взламывать» аккаунты в социальных сетях, электронную почту и т.д.;

3. Возможность быстро и без особых усилий найти необходимую информацию конфиденциального характера об определенном человеке;

4. Нежелание и незаинтересованность должностного лица в выполнении своих должностных обязанностей, а именно в предоставлении доступа гражданину к своим персональным данным, содержащиеся в картотеках государственных органов;

5. Стремление узнать персональные данные для личного интереса либо для последующего использования в корыстных целях;

6. Неудовлетворенность заработной платой лиц, имеющих в доступе персональные данные широкого круга лиц, в совокупности с желанием получить денежные средства за передачу данных.

Особо следует отметить, что иногда преступнику не требуется особых усилий и программ для получения доступа к персональным данным в сети

[87] Кудрявцев, В. Н., Эминова, В. Е. Криминология. Учебник / В.Н. Кудрявцева, В.Е. Эминова // ИНФРА-М. – Москва, 2004. – С. 186.

Интернет, ему достаточно воспользоваться неосмотрительностью потерпевших, которые оставляют свои информационные системы без должной защиты. Значительная часть уголовных дел, касающихся посягательств на персональные данные в сети Интернет, как раз связана с беспрепятственным доступом к личному компьютеру или социальной сети, электронной почты потерпевшего. Например, Советским районным судом г. Казани был признан виновным Х. по ч.2 ст. 272 УК РФ за неправомерный доступ к охраняемой законом компьютерной информации, повлекшей ее модификацию и блокирование, а именно, он получил доступ к учетной записи в социальной сети «Вконтакте» своей знакомой в результате того, что она поделилась с ним логином и паролем. После чего, он изменил данные для входа в учетную запись и стал знакомиться с личной информацией своей знакомой[88]. Вероятно, что более внимательное отношение потерпевшей к своим персональным данным предупредило бы подобное преступление и потерю учетной записи. Данный пример наглядно показывает, что именно доверие потерпевшей личной информации о своей учетной записи стало условием для совершения преступления. Согласно проведенному нами анкетированию, половина от всех респондентов делится в переписке по сети Интернет сведениями, разглашения которых не желают, при этом 42 % ведут общение с незнакомыми им в жизни людьми. Интересным фактом является то, что многие осознают факт возможного нарушения оборота персональных данных, но продолжают делиться ими в сети Интернет и в телефонных разговорах (Рис. 2).

[88] Постановление № 1-535/2018 от 12 июля 2018 г. по делу № 1-535/2018 [Электронный доступ]: Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/dzcV2m8pqmb1/.

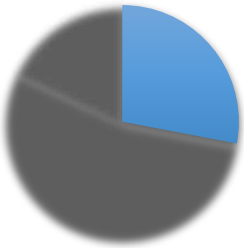


Рисунок 2 – осознание факта возможного нарушения оборота персональных данных

Тем не менее, существуют уголовные дела, где потерпевший не способствовал совершению преступлений, не разглашал информацию о том, где и как можно беспрепятственно получить доступ к его персональным данным. Например, Кировским районным судом г. Астрахани был осужден Ш. за неправомерный доступ к охраняемой законом компьютерной информации, что повлекло ее копирование, а также нарушил тайну телефонных переговоров с использованием служебного положения. А именно, к нему обратилось неустановленное лицо, осведомленное о том, что он имеет индивидуальный и конфиденциальный логин и пароль для работы в компьютерной программе, содержащей персональные данные клиентов организации. Названное лицо попросило Ш. предоставить детализацию абонентского номера, принадлежащего и находящегося в пользовании интересующего его человека, на что Ш. согласился[89]. Подобных дел, когда сотрудники, имеющие доступ к персональным данным абонентов, нарушают тайну переговоров достаточно много в судебной практике, что говорит об искажении нравственных ценностей и стремлении получить денежные средства вопреки закону.

[89] Приговор № 1-250/2018 от 13 июня 2018 г. по делу № 1-250/2018 [Электронный доступ]: Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/1hvQtG3bkTJp/.

Подводя итог, следует отметить, что комплекс причин и условий преступлений связан в первую очередь с отсутствием должного правосознания людей и законодательного регулирования оборота персональных данных в сети Интернет. Также немаловажным является отсутствие контроля за автоматизированными базами персональных данных со стороны организаций. Преступления в отношении оборота персональных данных в сети Интернет по большей части совершаются из-за интереса и проверки своих способностей, а зачастую деяния даже не осознаются нарушителем как противозаконные. Для борьбы с такими преступлениями необходимо воздействовать на одну из их причин - неразвитость системы виктимологической профилактики, ведь осведомленность о подобных преступлениях заставит субъектов самих качественней защищать свои данные, а, следовательно, и искоренит преступников «делитантов», выбравшие преступный путь ради малозначительного повода.

2.3 Личность преступника, совершающего преступления в отношении персональных данных в сети Интернет

При изучении преступности криминологи активно исследуют личность преступника, и помогают им в этом различные науки, в особенности социальные. Понятие «человек», «индивид», «личность» нередко употребляются в художественной литературе, публицистической и даже научной как равнозначные. Между тем, содержание этих понятий различное. Понятием «человек» обозначается особый вид живого существа в единстве его биологической природы и социальной сущности. Под «индивидом» понимают отдельного представителя рода «человек». Понятие «личность» фиксирует социальное качество индивида[90]. Под личностью преступника можно понимать совокупность значимых в социальном плане свойств, которые в сочетании с

[90] Прозументов, Л. М., Шеслер, А.В. Криминология. Общая часть: Учебник / Л. М. Прозументов, А. В., Шеслер // – Томск: ООО «ДиВо», 2007. – С. 143.

внешними условиями влияют на преступное поведение[91]. Интересующая нас личность преступника будет несколько отличаться от типичных компьютерных преступников.

Типовая классификация лиц, совершающих преступления в сфере компьютерной информации, рассматривалась многими известными учеными, к примеру, В. В. Крылов выделяет четыре основных типа преступников:

1) нарушители правил пользования компьютерной техникой;

2) «белые воротнички» – респектабельные преступники;

3) компьютерные шпионы;

4) хакеры, или «одержимые программисты»[92].

Применительно к теме нашего исследования данные типы личности можно отнести лишь к преступникам, нарушающих норму права из ст. 272 УК РФ. Как правило, нарушение оборота персональных данных в сети Интернет происходит не профессиональными «хакерами», а людьми, имеющими доступ к персональным данным в ЭВМ в связи с своими рабочими обязанностями, либо людьми, которые получили этот доступ по неосмотрительности субъекта данных. Специалисты в области компьютерной безопасности считают, что наиболее многочисленны из подобных преступников, но наименее опасны именно хакеры-дилетанты. На их долю приходится до 80 % всех нарушений оборота персональных данных в сети Интернет. Но этих людей интересует не некая цель, а сам процесс нахождения данных и дальнейшего их использования. Они испытывают удовольствие от преодоления систем защиты[93].

---

[91] Малкова, В. Д. Криминология. Учебник для вузов / В. Д. Малкова // ЮСТИЦИНФОРМ. – Москва, 2015. – С. 63.

[92] Крылов, И. Ф. Избранные труды по криминалистике / И.Ф. Крылов // Изд. Дом С.-Петерб. гос. ун-та. – Спб, 2006. – С. 344.

[93] Клещева, А. С. Криминалистическая характеристика личности преступника, совершающего преступления в области компьютерной информации / А. С. Клещева // Молодой ученый. – Казань, 2018. – №37. – С. 57- 60.

Криминологические исследования личности преступника показали, что среди ценностных ориентаций у данной категории лиц преобладают индивидуально- и кланово-эгоистические. В данных случаях доминируют желания материального благополучия, наиболее комфортных условий, проявления своего эго либо кланово-эгоистический интерес[94]. В частности, общедоступность компьютерных технологий, позволяющих получить любую информацию, приводят к объединению хакеров в преступные группировки.

У лиц, совершающих преступления в сфере оборота персональных данных в сети Интернет, нет особого преступного типажа, отличавшего бы их от других, ведь зачастую это люди, переступившие закон в связи с определенной ситуацией и моментальным появлением умысла. Такие преступления редко готовятся заранее и нуждаются в плане. Исключением является неправомерный доступ к охраняемой законом компьютерной информации с уничтожением, блокированием, модификацией либо копированием этой информации, потому что здесь мы можем наблюдать типичного компьютерного преступника, имеющего познания в программировании. Молодые люди, составляющие основную массу компьютерных преступников, зачастую совершают преступления из личной заинтересованности либо из корыстных побуждений. Ничем не ограниченная возможность использования сети Интернет, возможность узнать любую информацию о человеке приводит к невероятно сложной борьбе с такими преступлениями, а значит и к стремлению бросить вызов обществу у молодых людей.

Важно заметить, что с повсеместным распространением сети Интернет возраст нарушителей оборота персональных данных значительно понизился. Это обусловлено, в том числе недостатком воспитания в сфере информационной культуры в связи с непониманием старшим поколением возможности совершать преступления в информационно-

[94] Долгова, А. И. Криминология. Учебник для вузов /Под общ. ред. д. ю. н.,проф. А. И. Долговой // — 3-е изд., перераб. и доп. – М.: Норма. – Москва, 2005. – С. 292.

телекоммуникационной сети. Молодые люди, в том числе школьники, рассылают фотографии других людей, читают переписки без согласия субъекта, даже не задумываясь о нарушении закона. Считаем, что именно со школьного возраста необходимо заниматься правосознанием детей, в том числе для развития информационной культуры в целях недопущения увеличения числа преступлений в сфере компьютерной информации.

Большинство ученых сходятся во мнении, что совершение преступлений рассматриваемой категории характерно для мужчин. Однако в последнее время наблюдается тенденция к увеличению количества женщин, совершающих данные преступления[95]. Можно предположить, что это связано со стиранием границ «мужских» и «женских» профессий, ведь в наше время все больше девушек стремятся получить образование программиста и разбираться в компьютерных технологиях, а кто-то из них применяет свои знания в преступных целях.

Распространено мнение, что компьютерные преступники — высококвалифицированные специалисты с высшим техническим или юридическим образованием. Но если брать во внимание судебную практику, то виновным в преступлении по ст. ст. 137, 138 были признаны люди, не имеющие ни среднего технического, ни высшего образования, а ведь именно эти преступления составляют основную массу вреди всех преступлений в отношении оборота персональных данных в сети Интернет. В связи с этим, можно сделать вывод, что подобные преступления не нуждаются в специальном высшем образовании, а достаточно простых знаний в пользовании сети Интернет.

Определить типаж преступника, совершающего исследуемые деяния также крайне сложно. Представление о них как об инфантильных, замкнутых, склонных к депрессиям, а также всевозможным злоупотреблениям, небрежно

[95] Дьяков, В. В. О личности преступника как компоненте системы криминалистической характеристики преступлений в сфере компьютерной информации / В. В. Дьяков // Бизнес в законе. Изд. Юр-ВАК. – Москва, 2014. – № 2. – С. 33-34.

выглядящих молодых людях устарело. Нарушить неприкосновенность частной жизни в сети Интернет может любой, не обладающий вышеперечисленными качествами человек. Обращаясь к типологии преступников можно определить, что изучаемый тип относится к ситуативным, а также к ситуативно-криминогенным, потому что совершает преступления под сильным (резко неожиданным или чрезвычайно затяжным) влиянием конкретной криминогенной жизненной ситуации либо даже неосознанием преступного характера своих действий[96]. Изучая судебную практику, невозможно сделать вывод, что эти люди имеют предрасположенность к преступлениям, очевидно только то, что в момент совершения преступления были подвластны интересу и отсутствием должной защиты персональных данных. Поскольку преступники, относящиеся к этому типу, характеризуются общей положительной направленностью личности, а совершенное ими преступление не является закономерным следствием предшествовавшей жизни, то они наиболее легко и быстро поддается индивидуально-профилактическому воздействию.

Ю.В. Гаврилин предлагает лиц, совершающих компьютерные преступления, разбить на две категории. Первая категория - это лица, состоящие в трудовых отношениях с предприятием (организацией, учреждением, фирмой или компанией), где совершено преступление (по данным автора, они составляют более 55%). Вторая категория - граждане, не состоящие в правоотношениях с предприятием, где совершено преступление (около 45%). Ими могут быть пользователи и обслуживающий персонал ЭВМ других организаций, связанных компьютерными сетями с предприятием, а также лица, имеющие в своем распоряжении компьютерную технику и доступ к телекоммуникационным компьютерным сетям[97].

---

[96] Долгова, А. И. Криминология. Учебник для вузов /Под общ. ред. д. ю. н.,проф. А. И. Долговой // — 3-е изд., перераб. и доп. – М.: Норма. – Москва, 2005. – С. 365 - 366.

[97] Гаврилин, Ю. В. Расследование преступлений в сфере компьютерной информации: Глава в учебнике / Ю. В. Гаврилин // Криминалистика: Учеб. для вузов– 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА: Закон и право, 2008.

Главной проблемой, связанной с преступлениями в сети Интернет, является мода на них. Принадлежать к это преступной среде считается модным как среди профессионалов в сфере информационных технологий, так и среди подростков и лиц, не имеющих специального образования в области информатики. Эта мода влечет новых лиц к компьютерным журналам, атрибутике, сленгу, к использованию хакерских программ (зачастую легко доступным и простым в применении), а, в конечном счете, — к целенаправленному развитию в качестве компьютерного правонарушителя.

Подводя итог, следует отметить, что личность преступника является ситуативной, ситуативно-криминогенной и поддается индивидуально-профилактическому воздействию. Зачастую это «хакеры – дилетанты», которые не знакомы с программированием и переступили закон из-за интереса и проверки собственных способностей. Значительную роль в совершении преступлений играет неосмотрительность и излишнее доверие со стороны потерпевших, ведь зачастую преступники получают доступ к персональным данным без каких- либо усилий.

Сегодня, ни законодательство, ни правосознание людей не успевает сориентироваться в стремительном развитии компьютерных технологий, о многих нарушениях оборота персональных данных их субъекты даже не догадываются либо не предают должного внимания. Опасность встать на путь преступлений в сети Интернет грозит в первую очередь подросткам и молодежи, которых привлекает своеобразная интеллектуальная романтика, а также уверенность в относительной безнаказанности и «незначительности» своих общественно опасных деяний. Поэтому решительные действия правоохранительных органов в борьбе с компьютерными преступлениями особенно важны с точки зрения профилактики. С связи с этим необходимо освещать данную тему в СМИ и проводить профилактические мероприятия в первую очередь среди подрастающего поколения как основных пользователей сети Интернет.

2.4 Предупреждение преступлений в отношении персональных данных в сети Интернет

Предупреждение преступлений в сфере компьютерной информации является актуальной задачей борьбы с преступностью в России вообще и в частности противоправными деяниями в контексте поддержания общественной безопасности. В настоящее время, борьба с преступностью в сети Интернет в России ведется под воздействием факторов, которые снижают эффективность профилактических мер. По мнению исследователя Н. А. Щеголаева, такими факторами являются:

1. Актуальность. Область компьютерной информации одна из самых быстроразвивающихся на данный момент, в связи с чем общественные отношения, связанные с ней, быстро видоизменяются и дополняются новыми видами отношений.

2. Технологическая сложность. Да, не все преступления в отношении персональных данных требуют глубоких познаний в сфере программирования, но все же, существуют и сложные «хакерские» приемы взлома информационных систем, требующие специальных знаний от лиц, их расследующих.

Анализ научной литературы позволяет выделить следующие подходы к освещению данной проблематики. Так, В. Б. Вехов и В. Е. Козлов в своих работах указывают три основные группы мер предупреждения компьютерных преступлений, а именно правовые, организационно-технические и криминалистические[98]. С позиции Т. М. Лопатиной, система мер предупреждения компьютерных преступлений должна быть комплексной и включать в себя, с одной стороны, организационно-управленческие, технические (физические) меры, с другой - кадровые (в сочетании с морально-

[98] Козлов, В. Е., Вехов, В. Б Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов, В. Б. Вехов // М. : Горячая линия – Телеком, 2002. – С. 238. 336 с.

этическими) и правовые[99]. С точки зрения теории, разнообразие взглядов несомненно носит позитивный характер, поскольку в конкурентной борьбе способны родиться новые подходы. Однако ни одна из теорий на данный момент не может изменить ход преступности в сети Интернет. Несмотря на это, на наш взгляд, самой целостной можно считать позицию разделения данной деятельности государства на три направления: техническое, организационное и правовое.

К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных информационных систем, пересмотр минимальных требований к парольной системе аккаунтов в социальных сетях и электронной почте, разработка защиты сотовых устройств от прослушек и т. д.. Согласно результатам нашего анкетирования, только 26% опрошенных не сталкивались со «взломом» своих аккаунтов в социальных сетях (Рис. 3), что проявляет абсолютную незащищенность всех данных, находящихся там. Показательным примером защиты персональных данных в мессенджерах можно считать использование криптографического протокола MTProto в Telegram. В основе протокола лежит оригинальная комбинация симметричного алгоритма шифрования AES, протокол Диффи-Хеллмана для обмена 2048-битными RSA-ключами между двумя устройствами и ряд хеш-функций. Протокол допускает использование шифрования end-to-end с опциональной сверкой ключей[100]. Важно при этом понимать, что данный вид шифрования относится только к секретным чатам, а для облачных существуют ключи, позволяющие перехватывать информацию и знакомиться с перепиской. Учитывая это, самим пользователям с целью защиты своих персональных данных следует пользоваться именно секретными чатами, а разработчикам других мессенджеров активно развивать данный принцип шифрования.

---

[99] Лопатина, Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : дис. ... д-ра юрид. наук / Т. М. Лопатина // М. : РГБ, 2007. – С. 316 418 с.

[100] Jakob Bjerre Jakobsen. On the CCA (in) Security of MTProto. – 2016. [Электронный доступ]: On the CCA (in) security of MTProto. – Режим доступа: https://eprint.iacr.org/2015/1177.pdf.

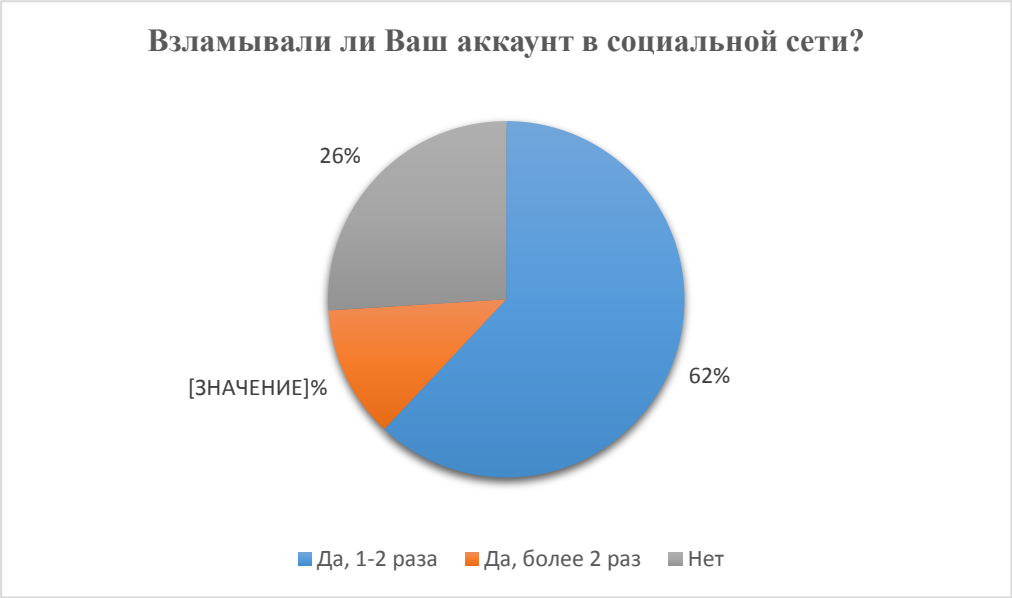


Рисунок 3 – количество «взлома» аккаунтов в социальных сетях

Следующее направление по предотвращению преступлений в сети Интернет - организационное. В данное направление входят меры, регламентирующие процессы функционирования автоматизированной системы, использование ее ресурсов, деятельности персонала, а также порядок взаимодействия пользователей системой таким образом, чтобы максимально затруднить или исключить возможность реализации угроз безопасности информации. С. С. Шахрай относит к таким мерам:

1. Создание категорий допуска для лиц, работающих с автоматизированными базами персональных данных, то есть, необходимо определить область служебных интересов каждого лица, вид информации с правом доступа и полноту их полномочий исходя из функциональных обязанностей;
2. Разработка периодического системного контроля за качеством защиты информации посредством проведения проверок в том числе с привлечением компетентных специалистов (экспертов) из других организаций;
3. Обучение и ознакомление работающего персонала с применяемыми в конкретной организации организационно-техническими мерами защиты;

4. Введение в штатное расписание организации должности специалиста по компьютерной безопасности (администратора по защите информации)[101].

Так же, необходимо ввести осуществление профилактических мероприятий среди людей разных возрастных категорий. В связи с тем, что не всегда нарушение оборота персональных данных признается обществом как преступное деяние, необходимо как можно больше людей ознакомить со спецификой данного посягательства, а также с тем, как его предотвратить. Согласно результатам нашего анкетирования, 50% опрошенных считают себя неосведомленными о возможном незаконном доступе к информации в сети Интернет, а также преступном его использовании, при этом 82% респондентов считают необходимым проведение мероприятий виктимологической профилактики, что подтверждает их необходимость. Следует со школьной скамьи прививать детям правила поведения в сети Интернет, например, не делиться своим местоположением, паролем и логином от аккаунта, не вводить все данные, которые могут потребовать при регистрации на каком – либо сайте, не скачивать файлы неизвестного расширения, не пользоваться чужими компьютерами в местах массового скопления людей и не открывать подозрительные сайты, которые созданы для сбора информации о пользователе. Все эти простые правила помогут сократить реальное количество посягательств на персональные данные в сети Интернет и повысят уровень компьютерной безопасности в целом.

Последнее рассмотренное направление – правовое, под ним следует понимать совершенствование уголовно-правовых норм законодательства, устанавливающих ответственность за их совершение. На основе уже изложенного ранее можно выделить следующее:

[101] Шахрай, С. С. Основные направления предупреждения преступлений в сфере компьютерной информации / С. С. Шахрай //Журнал Вестник экономической безопасности. – 2009. – С. 154-158.

1. Отсутствуют значимые понятия, либо дается слишком широкое определение, позволяющее принимать решение при расследовании преступления по усмотрению субъекта (например, «персональные данные»). Необходимо разработать качественный понятийный аппарат, выделяющий основные признаки того или иного явления.

2. Отсутствие толкования норм ст. 137 УК РФ и ст. 272 УК РФ приводит к неправильной квалификации деяний при наличии нарушении неприкосновенности частной жизни, которая была выражена в незаконном доступе к компьютерной информации, а именно к персональным данным в сети Интернет.

3. Необходимо ввести перечень пресональных данных, при этом оставить его открытым. Это поможет привести судебную практику в состояние единства позиции по поводу отнесения к персональным данным той или иной конфиденциальной информации.

Важно понимать, что предупреждение новых преступлений можно разделить условно на две части, где отдельно будет проходить виктимологическая профилактика, а отдельно развитие технологий и законодательства для предотвращения новых нарушений. Остановимся поподробнее на первой части.

При определении целей и задач виктимологической профилактики необходимо выделить три ее уровня: общесоциальный, специальный, индивидуальный. Раскрывая объект виктимологической профилактики на общесоциальном уровне, следует иметь в виду, что любой человек (вне зависимости от индивидуальной степени его виктимности) может стать жертвой преступления. В этом смысле в качестве объекта выступают все жители страны как потенциальные жертвы преступлений. Основной задачей виктимологической профилактики на данном уровне является создание системы эффективной социальной защиты всех граждан от возможной

виктимизации, изменение сложившейся практики обращения с потерпевшими и другими жертвами преступлений.

Виктимологическая профилактика на специальном уровне имеет своим объектом не все население, а его отдельные группы повышенной виктимности, например, безработных, алкоголиков и т. д., потому что у этих групп населения повышенная склонность к совершению преступлений из-за корыстных мотивов.

В борьбе с преступлениями в отношении персональных данных в сети Интернет чрезвычайно важно вести профилактические мероприятия с населением о возможности перехвата информации третьими лицами из переписок, телефонных разговоров, потому что применение некоторых мер безопасности возлагается именно на субъектов данных, а также необходимо доступно объяснять, как защищать свои права на частную жизнь, куда обращаться при возникновении посягательств на персональные данные. Только такая деятельность государства способна уменьшить число лиц, совершающих преступление ради своего личного интереса, а также на профессиональных «хакеров», извлекающих выгоду из полученных персональных данных.

Индивидуальная виктимологическая профилактика состоит в выявлении лиц с повышенной виктимностью и проведении с ними защитно-воспитательных мероприятий, направленных на снижение риска стать жертвой преступных посягательств. Приемы и методы индивидуальной виктимологической профилактики достаточно известны, они, как правило, сводятся к защитно-воспитательной работе с гражданами, уже ставшими потерпевшими, например, беседы школьного психолога после случая распространения персональных данных ученика с целью недопущения подобных случаев в дальнейшем.

В заключение необходимо отметить, что за последнее время в России накоплен определенный опыт виктимологической профилактики, взяты на вооружение многие рекомендации зарубежной практики по вопросам

предупредительной работы с потенциальными и реальными жертвами преступлений. Издан ряд брошюр, серии памяток для населения, использование которых в практической работе поможет обеспечить более надежную защиту граждан от противоправных посягательств.

ЗАКЛЮЧЕНИЕ

Подводя итог работе можно сказать следующее. Повсеместное внедрение сети Интернет определенно сыграло важную роль в жизни каждого человека, имея при этом как плюсы, так и минусы. К плюсам можно отнести появление новых возможностей в получении новых знаний, знакомстве и общении, покупки онлайн, развитие новых технологий и появлении новых рабочих мест. Среди минусов – угроза информационной безопасности как отдельных лиц, так и государств, «интернет зависимость», дезинформация населения, угроза для детей и подростков в виде непредназначенной для них информации в открытом доступе. Для настоящей работы мы выделили одну важнейшую проблему распространения сети Интернет – преступления в отношении персональных данных и изучили ее с точки зрения науки криминологии.

Итак, для начала мы определили, что персональные данные – это информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу, которая если носит режим конфиденциальности, то требует согласия субъекта для передачи ее третьим лицам за исключением случаев, установленных в законе. Важно учесть, что персональные данные не всегда могут идентифицировать человека по отдельности, часто это можно сделать по совокупности двух – трех данных. Также следует отметить, что отсутствие конкретного перечня персональных данных является существенным пробелом в российском законодательстве. Все же, необходимо установить открытый перечень, что повлечет за собой более разумную судебную практику и более качественный уровень защиты персональных данных.

Анализируя развитие законодательства об охране персональных данных, можно с уверенностью сказать, что Россия совершила огромный шаг к созданию демократического государства, где приоритетом является

частноправовой интерес личности. Принятие Конституции РФ 1993 года и объявление прав и свобод человека и гражданина высшей ценностью потребовало создание нормативно-правовой базы охраны личной жизни каждого. На смену декларативным нормам пришел Закон о персональных данных, хоть и содержащий оценочные понятия, но ставший мощным фундаментом для появления других нормативных актов. Вместе они создают единую правовую базу, позволяющую каждому человеку чувствовать защищенность и неприкосновенность частной жизни.

Сравнивая же развитие международного законодательства с российским можно заметить, что наша страна достаточно поздно стала учитывать частноправовые интересы личности по сравнению с другими странами. В то время, когда СССР создавал декларативные нормы, на международной арене право человека на охрану персональных данных стало уже фундаментальным и это крайне важно, учитывая развитие технологий и все новые способы несанкционированного использования данных. Принимая во внимание глобальный характер проблемы, России необходимо учитывать опыт других стран и совершенствовать свое законодательство в сфере охраны персональных данных.

Можно с уверенностью сказать, что законодательство и судебная практика по преступлениям, связанным с оборотом персональных данных в сети Интернет не совершенно. Существует проблема квалификации деяний по ст. 137 УК РФ и ст. 272 УК РФ, предлагается за нарушение неприкосновенности частной жизни, которая была выражена в незаконном доступе к компьютерной информации применять совокупность вышеназванных статей.

Комплекс причин и условий преступлений связан в первую очередь с отсутствием должного правосознания людей и законодательного регулирования оборота персональных данных в сети Интернет. Также немаловажным является отсутствие контроля за автоматизированными базами персональных данных со

стороны организаций. Преступления в отношении оборота персональных данных в сети Интернет по большей части совершаются из-за интереса и проверки своих способностей, а зачастую деяния даже не осознаются нарушителем как противозаконные. Для борьбы с такими преступлениями необходимо воздействовать на одну из их причин - неразвитость системы виктимологической профилактики, ведь осведомленность о подобных преступлениях заставит субъектов самих качественней защищать свои данные, а, следовательно, и искоренит преступников «дилетантов», выбравшие преступный путь ради малозначительного повода.

Изучая личность преступника в данной сфере достаточно сложно определить его типаж. Он отличается от типичного компьютерного преступника и совершает преступления по большей части без специальных знаний в программировании. Представление о них как об инфантильных, замкнутых, склонных к депрессиям, а также всевозможным злоупотреблениям, небрежно выглядящих молодых людях устарело. Нарушить неприкосновенность частной жизни в сети Интернет может любой, не обладающий вышеперечисленными качествами человек. Обращаясь к типологии преступников можно определить, что изучаемый тип относится к ситуативным, потому что совершают преступления под сильным (резко неожиданным или чрезвычайно затяжным) влиянием конкретной криминогенной жизненной ситуации либо даже неосознаванием преступного характера своих действий. Изучая судебную практику невозможно сделать вывод, что эти люди имеют предрасположенность к преступлениям, очевидно только то, что в момент совершения преступления были подвластны интересу и отсутствием должной защиты персональных данных. Поскольку преступники, относящиеся к этому типу, характеризуются общей положительной направленностью личности, а совершенное ими преступление не является закономерным следствием предшествовавшей жизни, то они наиболее легко и быстро поддается индивидуально-профилактическому воздействию.

Что же касается профилактики подобных преступлений, то очень важно принимать во внимание мероприятия, нацеленные на работу с виктимологическим поведением населения разных возрастных категорий. Значительная часть преступлений в отношении персональных данных в сети Интернет совершается из-за отсутствия их защиты со стороны субъектов этих данных (слабая парольная защита, доверие персональных данных незнакомым лицам по переписке, пользование одним ПК или сотовым телефоном несколькими лицами). В первую очередь профилактические мероприятия необходимо проводить в школах, так как именно дети и подростки являются самими активными пользователями сети Интернет и зачастую не осознают своих действий.

Для защиты персональных данных необходимо улучшить нормативное регулирование посягательств на них, активно проводить профилактические мероприятия, а также лучше контролировать работу операторов персональных данных. Необходимо добиться осознания проблем передачи персональных данных в сети Интернет с целью уменьшения латентности данных преступлений и развития правосознания со школьной скамьи.

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

Нормативно правовые акты

1. Европейская конвенция о защите прав человека и основных свобод ETS №005 [Электронный ресурс] : конвенция о защите прав человека и основных свобод (Заключена в г. Риме 04.11.1950) (с изм. от 13.05.2004) // Информационно-правовой портал «Гарант.ру». — Режим доступа: https://www.garant.ru.

2. Всеобщая декларация прав человека [Электронный доступ]: всеобщая декларация прав человека принятая Генеральной Ассамблеей ООН 10.12.1948 // Информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

3. Европейская конвенция о защите прав человека и основных свобод ETS №005 [Электронный ресурс] : Конвенция о защите прав человека и основных свобод (Заключена в г. Риме 04.11.1950) (с изм. от 13.05.2004) // информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

4. Директива Европейского Парламента и Совета Европейского Союза [Электронный доступ]: директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24.10.1995 // информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

5. Хартия Европейского Союза об основных правах [Электронный доступ]: хартия Европейского Союза об основных правах от 12.12.2007 // информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

6. Конституция Российской Федерации [Электронный ресурс] : федер. закон от 25.12.1993 ред. от 21.07.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

7. Уголовный кодекс РФ [Электронный ресурс] : федер. закон от 13.06.1996 г. № 63-ФЗ ред. от 23.04.2018 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

8. Уголовный кодекс РСФСР [Электронный ресурс] : федер. закон от 01.06.1922 // Федеральный правовой портал Юридическая Россия. – Режим доступа: http://www.law.edu.ru/norm/norm.asp?normID=1241523&subID.

9. Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ ред. от 18.03.2019 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

10. О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 №152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

11. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс] : федер. закон от 19.12.2005 № 160 // Информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

12. Об обороте земель сельскохозяйственного назначения [Электронный ресурс] : федер. закон от 24.07.2002 ред. 01.05.2019 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

13. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы (утв. Указом Президента РФ 09.05.2017 № 203) [Электронный ресурс] : информационно-правовой портал «Гарант.ру». – Режим доступа: https://www.garant.ru.

14. О международном информационном обмене [Электронный ресурс] : модельный закон от 26.03.2002 № 19-7 // Информационно-правовой портал «Гарант.ру». — Режим доступа: https://www.garant.ru.

15. Собрание законодательства Российской Федерации [Электронный ресурс] : собрание законодательства 1995 №8 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

16. Устав о наказаниях, налагаемых мировыми судьями [Электронный доступ] : Русская энциклопедия Традиция. – Режим доступа : https://traditio.wiki/Устав_о_наказаниях,_налагаемых_мировыми_судьями.

17. Уголовное Уложение 22 марта 1903 года / Издание Н.С. Таганцева. – Санкт Петербург, 1904. – 845 с.

Судебная практика

18. Апелляционное определение Московского городского суда от 22.05.2014. № 33-14709 [Электронный ресурс] : справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=RAMSMARB&n=719253#02431987170781642.

19. Приговор № 1-53/2018 от 24 сентября 2018 г. по делу № 1-53/2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/JHBHzJUXOmWW/.

20. Приговор № 1-389/2017 1-6/2018 от 2 октября 2017 г. по делу № 1-389/2017 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/kN7MkWMrBlUK/.

21. Приговор № 1-22/2017 1-378/2016 от 13 февраля 2017 г. по делу № 1-22/2017 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/uFVINSkG4CHZ/.

22. Приговор № 1-218/2018 от 15 октября 2018 г. по делу № 1-218/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/BTGs3iNkWxUw/.

23. Приговор № 1-211/2018 от 27 июля 2018 г. по делу № 1-211/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/zUJ8vvZC2Udq/.

24. Решение № 2-2438/2018 от 23 октября 2018 г. по делу № 2-2438/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/fRg7fDCcbjWK/.

25. Решение № 2-2193/2018 от 19 октября 2018 г. по делу № 2-2193/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/3BLhkoppApQX/.

26. Решение № 2-5812/2018 от 5 октября 2018 г. по делу № 2-5812/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/lwgoHBIpJK51/.

27. Решение № 2-1-547/2018 от 3 октября 2018 г. по делу № 2-1-547/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/n8suO3Gne2Qc/.

28. Решение № 2-3620/2018 от 27 сентября 2018 г. по делу № 2-3620/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/cFgxlKrkoBV5/.

29. Case of Benedik v. Slovenia. The European Court of Human Rights. Application no. 62357/14. 24.04.2018 2018 [Электронный доступ] : The European Court of Human Rights. – Режим доступа: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}.

30. Постановление КС РФ от 26.10. 2017 № 25-П [Электронный доступ] : Российская газета - Федеральный выпуск № 259(7425) . – Режим доступа : https://rg.ru/2017/11/16/ks-dok.html.

31. Решение № 2-3188/2016 от 6 июля 2016 г. по делу № 2-3188/2016 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа : https://sudact.ru/regular/doc/PbeMmON8wmZP/.

32. Решение № 2-209/2018 от 23 мая 2018 г. по делу № 2-209/2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа : https://sudact.ru/regular/doc/TtSMpYKDwfor/.

33. Определение Конституционного Суда РФ от 09.06.2005 г. № 248-О [Электронный доступ] : информационно-правовой портал «Гарант.ру». – Режим доступа: https://base.garant.ru/1354478/.

34. Приговор № 1-878/1/2017 1-878/2017 от 15 декабря 2017 г. по делу № 1-878/1/2017 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/1KmWTdMX4qHo/.

35. Приговор № 1-389/2017 1-6/2018 от 2 октября 2017 г. по делу № 1-389/2017 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/kN7MkWMrBlUK/.

36. Апелляционное постановление № 22-6353/2018 от 15 ноября 2018 г. по делу № 22-6353/2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/60mfkd1UoDQr/.

37. Приговор № 1-133/2018 от 25 июля 2018 г. по делу № 1-133/2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/tHIOr1LSy3Ya/.

38. Постановление № 1-678/2018 от 13 сентября 2018 г. по делу № 1-678/2018 2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/JGUHXNS8aBd8/.

39. Постановление № 1-535/2018 от 12 июля 2018 г. по делу № 1-535/2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/dzcV2m8pqmb1/.

40. Приговор № 1-250/2018 от 13 июня 2018 г. по делу № 1-250/2018 [Электронный доступ] : судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/1hvQtG3bkTJp/.

Учебная и научная литература

41. Агентство правовой информации. Статистика [Электронный доступ]: Агентство правовой информации. – Режим доступа: http://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17.

42. Абдулгалимов, Г. Л., Кугель, Л. А. Обучение проектированию информационных систем и анализу данных / Г. Л. Абдулгалимов, Л. А. Кугель // Профессиональное образование. Столица. – Москва, 2013. – № 4. – С. 31-33.

43. Алямкин С. Н. Персональные данные как объект правового регулирования: понятие и способы защиты / С. Н. Алямкин // Мир науки и образования. – Саранск, 2016. – № 4(8).

44. Баглай, М. В. Конституционное право Российской Федерации / М. В. Баглай // Норма. – Москва, 2009. – 782 с.

45. Беккариа, Ч. О преступлениях и наказаниях. / Ч. Беккариа // ИНФРА-М. – Москва, 2004. – С. 123–124.

46. Большой толковый словарь русского языка [Электронный ресурс] : коллекция словарей и энциклопедий сост. и гл. ред. С.А. Кузнецов. СПб. — Режим доступа: https://gufo.me.

47. Важорова, М. А. История возникновения и становления института персональных данных / М. А. Важорова // Государство и право: теория и практика: материалы Междунар. науч. конф. – Челябинск, 2011. – С. 33.

48. Винер Н. Кибернетика и общество / Н. Виннер // Издательство иностранной литературы. – Москва, 1958. – С. 31.

49. Волчинская, Е. К. Место персональных данных в системе информации ограниченного доступа / Е. К. Волчинкская // Право. Журнал Высшей школы экономики. – Москва, 2014. – 325 с.

50. Гаврилин, Ю. В. Расследование преступлений в сфере компьютерной информации: Глава в учебнике / Ю. В. Гаврилин // Криминалистика: Учеб. для вузов– 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА: Закон и право, 2008. – 784 с.

51. Гайфутдинов, Р. Р. Уголовно-правовая характеристика посягательства на персональные данные, обрабатываемые в автоматизированных системах / Р. Р. Гайфутдинов // Учёные записки Казанского университета. Серия: Гуманитарные науки №4. – Казань, 2014. – С. 159-169.

52. Дворецкий, М. Ю., Авдеев, Р. В. Причины и условия преступности / М. Ю. Дворецкий, Р. В. Авдеев // Вестник ТГУ. Серия: Гуманитарные науки. – Томбов, 2014. – С. 3-5.

53. Долгова, А. И. Криминология. Учебник для вузов /Под общ. ред. д. ю. н., проф. А. И. Долговой // — 3-е изд., перераб. и доп. – М.: Норма. – Москва, 2005. – 912 с.

54. Дьяков, В. В. О личности преступника как компоненте системы криминалистической характеристики преступлений в сфере компьютерной информации / В. В. Дьяков // Бизнес в законе. Изд. Юр-ВАК. – Москва, 2014. – № 2. – С. 33-34.

55. Евдокимов, К. Н. Проблемы противодействия неправомерному доступу к компьютерной информации: Уголовно-правовые и криминологические аспекты / К. Н. Евдокимов // Монография. – Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2013

56. Иванников, А. Д., Тихонов, А. Н., Цветков, В. Я. Основы теории информации / А. Д. Иванников, А. Н. Тиханов, В. Я. Цветков // МАКС Пресс. – Москва, 2007. – 356 с.

57. Карпов, В. С. Уголовная ответственность за преступления в сфере компьютерной информации: дис. … канд. юр. наук: 12.00.08 / Карпов Виктор Сергеевич. – Красноярск, 2002.

58. Клещева, А. С. Криминалистическая характеристика личности преступника, совершающего преступления в области компьютерной информации / А. С. Клещева // Молодой ученый. – Казань, 2018. – №37. – С. 57-60.

59. Козлов, В. Е., Вехов, В. Б Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов, В. Б. Вехов // М. : Горячая линия – Телеком, 2002. – 336 с.

60. Крылов, И. Ф. Избранные труды по криминалистике / И.Ф. Крылов // Изд. Дом С.-Петерб. гос. ун-та. – Спб, 2006. – С. 343-354.

61. Кудрявцев, В. Н., Эминова, В. Е. Криминология. Учебник / В.Н. Кудрявцева, В.Е. Эминова // ИНФРА-М. – Москва, 2004. – 512 с.

62. Кузнецова, Н. Ф., Лунеева, В. В. Криминология: учебник / Н. Ф. Кузнецовой, В. В. Лунеева // Волтерс Клувер. – Москва, 2005. – С. 167 – 168.

63. Лазарев, В. В. Теория государства и права : учебник для академического бакалавриата / В. В. Лазарев, С. В. Липень // 5-е изд., испр. и доп. Издательство Юрайт. – Москва, 2017. – 521 с.

64. Лопатина, Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : дис. ... д-ра юрид. наук / Т. М. Лопатина // М. : РГБ, 2007. – 418 с.

65. Лысак, И. В. Информация как общенаучное и философское понятие: основные подходы к определению / И. В. Лысак // Философские проблемы информационных технологий и киберпространства. – Пятигорск, 2015. – С. 9 - 26.

66. Малкова, В. Д. Криминология. Учебник для вузов / В. Д. Малкова // ЮСТИЦИНФОРМ. – Москва, 2015. – С. 63.

67. Мелик-Гайказян, И. В., Мелик-Гайказян, М. В., Тарасенко, В. Ф. Методология моделирования нелинейной динамики сложных систем / И. В. Мелик-Гайказян, М. В. Мелик-Гайказян, В. Ф. Тарасенко // Физматлит. – Москва, 2001. – 272 с.

68. Научно-практический комментарий к ст. 272 УК РФ [Электронный доступ]: Образовательный портал Geum.ru. – Режим доступа: http://geum.ru/lav/index-42778.php.

69. Ответы на вопросы в сфере защиты прав субъектов персональных данных. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный доступ] : Официальный сайт РОСКОМНАДЗОР. – Режим доступа : https://rkn.gov.ru/treatments/p459/p468/.

70. Портал правовой статистики [Электронный доступ]: Генеральная прокуратура РФ. Портал правовой статистики. – Режим доступа: http://crimestat.ru/offenses_map.

71. Прозументов, Л. М., Шеслер, А.В. Криминология. Общая часть: Учебник / Л. М. Прозументов, А. В., Шеслер // – Томск: ООО «ДиВо», 2007. – 230 с.

72. Романовский, Г. Б. Право на неприкосновенность частной жизни / Г. Б. Романовский // МЗ – Пресс. – Москва, 2001. – С. 63-65.Симонова, Е. В. Определение понятия персональных данных в Российской Федерации / Е. В. Симонова // Молодой ученый. – Казань, 2017. – №10. – С. 323-326.

73. Словарь синонимов русского языка [Электронный ресурс] : З. Е. Александрова. Практический справочник. М.: Русский язык, 2001. — Режим доступа: https://alleng.org.

74. Социальные сети в 2018 году: глобальное исследование. [Электронный ресурс] : WebCanape. Социальные сети в 2018 году: глобальное исследование. – Режим доступа: https://www.web-canape.ru.

75. Шахрай, С. С. Основные направления предупреждения преступлений в сфере компьютерной информации / С. С. Шахрай //Журнал Вестник экономической безопасности. – 2009. – С. 154-158.

76. Шеннон, К. Работы по теории информации и кибернетике. / К. Шеннон // Издательство иностранной литературы. – Москва, 1963. – 829 с.

77. General Data Protection Regulation. Wikipedia. [Электронный доступ] : Wikipedia. The Free Encyclopedia. – Режим доступа : https://en.wikipedia.org/wiki/General_Data_Protection_Regulation.

78. Jakob Bjerre Jakobsen. On the CCA (in)Security of MTProto. – 2016. [Электронный доступ]: On the CCA (in) security of MTProto. – Режим доступа: https://eprint.iacr.org/2015/1177.pdf.

79. Jones, C. R. Nobody knows you’re a dog / C. R. Jones // Education in Cyberspace. — New York, 2004.

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Юридический институт
институт
Деликтологии и криминологии
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ И.А. Дамм
подпись инициалы, фамилия
« 10 » 06. 2019 г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01 – Юриспруденция

Криминологический анализ и предупреждение преступлений в отношении персональных данных, совершаемых в сети Интернет

Руководитель _____ 19.06.19. доцент, к.ю.н. С.И. Гутник
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ 19.06.2019 А.С. Синякова
подпись, дата инициалы, фамилия

Красноярск 2019