кандидат технических наук, преподаватель
Ростовского института (филиала)
ВГУЮ (РПА Минюста России)
Назарьянц Елена Геворговна

преподаватель
Ростовского института (филиала)
ВГУЮ (РПА Минюста России)
Солонченко Юлия Анатольевна

студент
Ростовского института (филиала)
ВГУЮ (РПА Минюста России)
Белашев Алексей Павлович

ЗАКОНОДАТЕЛЬСТВО В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

В данной научно-исследовательской работе будет рассматриваться законодательство в сфере обеспечения информационной безопасности РФ. Статья посвящена разбору нормативно-правовых актов регулирующие защиту информации, ее обработку и пользования. Также в процессе работы мы рассмотрели некоторые вопросы обеспечения безопасности в сфере персональных данных. Рассмотрели также проблемы кибертерроризма, который оказывает влияние на критическую инфраструктуру путем хакерских атак на информационную составляющую.

КЛЮЧЕВЫЕ СЛОВА: Информационные технологии, защита, обработка, правовое регулирование.

XXI век ознаменовался веком развития цифровых технологий. Уже ни у кого не вызывает сомнения, что процесс глобализации информационных технологий представляет собой неограниченные возможности. Данные возможности являются как доброжелательными, так и ужасающими. Так, если мы будем рассматривать позитивную часть развития информационных технологий, то можно привести несколько примеров: человеку стало легче получать различную информацию, получать данные с организаций, искать различную для себя работу и т.д. Особое место занимает «...значительная часть торговли и платежей сегодня осуществляется через Интернет и платежные системы» [1].

К сожалению, развитие информационных технологий является двухсторонней медалью, с одной стороны облегчает жизнь, с другой, наносит вред общественным отношениям, которые подлежат правовой охране.

Прежде чем приступить к рассмотрению вопроса законодательства в сфере обеспечения информационной безопасности, необходимо рассмотреть, что из себя представляет «информация» и «информационная безопасность» [2]. Рассматривая нормативно-правовую базу, мы не обнаружили легализованного понятия «информационной безопасности». Но обнаружили, что исследователи пробуют давать свое понятие, что также вызывает дискуссию между ними.

Следует обозначить, что на сегодняшний день существует огромное количество нормативно-правовых актов, подзаконных актов, регулирующих вопросы информационной безопасности на территории РФ. За последние 15-20 лет развитие информационно-коммуникативной сети «Интернет» предоставило новые возможности пользователям, например, свободно обмениваться информацией, скачивать с торрентов программные обеспечения, кинофильмы и т.п [3]. Особой популярностью начали пользоваться социальные сети.

Считаем, что следует рассмотреть нормативно-правовые акты и выделить их ключевые моменты.

Первым рассматриваемым законом будет Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Данный закон является основополагающим в сфере обеспечения информационной безопасности на территории РФ.

Наше сказанное подтверждается тем, что данный закон определяет и закрепляет ключевые термины, которые используются в нормативных документах, например, таким термином является «информация» (см. ст. 2 ФЗ № 149) [4].

Рассмотрим ключевые особенности данного закона.

Во-первых, закон закрепляет конституционное право регламентированное (ст. 23 Конституции РФ) [5].

Во-вторых, данный закон закрепляет диспозитивные нормы относительно применению информационных систем.

В-третьих, закрепляется особые требования к контенту, информации, например, сцены насилия (как морального, так и сексуального).

В-четвертых, закреплено право на защиту информации уполномоченными лицами.

В-пятых, закон предусмотрел специализированных государственный реестр запрещенных сайтов на территории РФ. Орган, который является начальствующим в этой сфере можно по праву сказать: «Роскомнадзор». Все действия с блокировкой, разблокировкой и т.п. выполняет Роскомнадзор.

Следующим законом имеющий особое влияние является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Данный закон является основополагающим в работе с персональными данными. Организации, которые запрашивают согласия на использование и обработку персональных данный обязаны ее сохранять, а также защищать от возможной утраты (ст. 7) [6].

Выделим ключевые моменты.

Во-первых, главным условием работы данного закона является «разрешение» владельца на обработку его данных. Примечательно, что для поступления на государственную (гражданскую) службы, если лицо

отказывается от проведения в отношении него проверки, то ему автоматически отказывается.

Во-вторых, собранные данные хранятся и организация, компания, которая запрашивала ваши данные обязана их хранить.

В-третьих, в случае прекращения использования какой-либо программы, лицо имеет право сделать запрос, для удаления его персональных данных.

Следующий закон является одним из важнейших, наравне с ФЗ № 149 и ФЗ № 152, а именно ФЗ от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [7].

Данный закон касается организаций оказывающие медицинские услуги, безопасность граждан, организацию работы АЭС, ТЭС и т.д.

Данная сфера подвержена постоянным хакерским атакам. Это подтверждается огромным количеством научных работ. Например, по сей день не было дано основного легализованного понятия, что из себя представляет «кибертерроризм». Хотя, хакерские атаки на АЭС, банковские системы, являются подтверждением, что понятие «кибертерроризма» является более подходящим, т.к. действия хакеров направлены на выведение из строя АЭС, парализованные медицинской работы. Анализируя проблему данного подвида терроризма, мы нашли достаточно большую теоретическую основу. Так было выделено, что «кибертерроризм» в первую очередь посягает на важнейшие инфраструктуры. К таким у нас относятся АЭС, ТЭС, военно-промышленные комплексы [8].

Считаем, что рассмотрения вопроса информационной безопасности необходимо проводить комплексно, для этого считаем, что стоит указать на некоторые проблемы, которые существуют на наш взгляд. В особенности хотим подчеркнуть сферу защиты персональных данных.

Проблема применения последних достижений науку и техники в преступных целях связана с созданием глобальной информационно-телекоммуникационной сети «Интернет», которая объединила весь мир в свою трансграничную сеть. Данная сеть обеспечивает преступникам большую

латентность, анонимность, что делает их неуязвимыми. К примеру, пару лет назад, раскрывать преступления наркотической направленности было легче, но на сегодняшний день, наркоторговцы используют «Интернет», что делает раскрываемость по данным преступлениям низкую.

Особым местом в данных преступлениях является вопрос обеспечении информации, а именно защита персональных данных, которая имеет особую опасность в руках преступников. Так, если в руки преступников попадет информация о персональных данных, это может быть опасным оружием, направленным против данного гражданина [9].

Вопросам обеспечения безопасности персональных данных в РФ уделяется достаточно большое внимание. Так, анализируя национальное законодательство, мы обнаружили, что в РФ существует:

1. Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи»;
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Данный закон регулирует: обеспечение права на поиск, получения, передачи, производства и распространения информации, а также обеспечение защиты информации;
3. Федеральный закон от 19.12.2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
4. Указ президента РФ от 22.05.2015 г. № 260 «О некоторых вопросах информационной безопасности РФ»;
5. Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности РФ».

Мы видим, что на законодательном уровне вопрос защиты «информации» развит достаточно. Но для противодействия и сохранения информационной безопасности необходимо развивать не только законодательство, но и правоприменительную практику, путем повышения уровня сотрудников, занимающихся защитой информации.

Так, вопросом обеспечения безопасности, а также расследования преступлений совершаемых с использованием информационных технологий занимается Управления «К», которая была создана и закреплена в структуре Министерства Внутренних Дел РФ. Данный отдел занимается расследованием преступлений в сфере информационных технологий.

Основными направления работы МВД России является:

1) Выявление и пресечение фактов неправомерного доступа к компьютерной информации.

2) Борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ.

3) Противодействие мошенническим действиям с использованием возможностей электронных платежных систем.

4) Пресечение противоправных действий в информационно телекоммуникационных сетях, включая сеть Интернет.

5) Выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи.

6) Противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет.

7) Противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.

8) Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

9) Выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий. Борьба с международными преступлениями в сфере информационных технологий.

Проблема обеспечения защиты информационного пространства зависит не только от количества принятых законодательных актов, но еще и от способа отражения посягательства на охраняемую информацию.

Также, стоит не забывать, что особую роль играет правосознание граждан, которые своими преступными действиями нарушают права граждан в данной сфере.

Наиболее действующим для отражения информационной безопасности будет: во-первых, повышения уровня правовй культуры молодежи, т.к. именно молодежь проводит огромное количество времени в данной сети; во-вторых, повышение оброзовательной программы для сотрудников правоохранительных органов, органов служб безопасности, которые уполномочены на выявление, расследование и пресечения деятельности преступников, а также отражения их атак. Особе место стоит уделить налаживанию международного сотрудничество, но по данному вопросу пока существуют некоторые проблемы, из-за последних ситуаций в мире.

Некоторые авторы, например, Смоленский М.Б. считает, что «...наиболее перспективным направлением для вмешательства государства представляется ограничение возможности анонимного распространения информации» [10]. Считаем, что Смоленский М.Б. предлагает положительный вариант для решения некоторых проблем.

Библиографический список:

1. Фомин, Д. В. Информационная безопасность: учебное пособие для СПО / Д. В. Фомин. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2022. — 218 с.

2. Ефремова, Марина Александровна. Уголовно-правовая охрана информационной безопасности: автореферат дис. ... доктора юридических наук : 12.00.08 / Ефремова Марина Александровна; [Место защиты: Акад. Генер. прокуратуры РФ]. - Москва, 2018. - 59 с.

3. Петрищева Елена Николаевна, Лемайкина Светлана Владимировна Правовые аспекты государственного регулирования Рунета // ЮП. 2017. №3 (82).

4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 14.07.2022) // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448

5. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993г. с изменениями, одобренными на общероссийском голосовании 1 июля 2020) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ) // Собрание законодательства РФ. – 01.07.2020. – № 15. – ст. 1691.

6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 01.09.2022) // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3451

7. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ, 31.07.2017, № 31 (Часть I), ст. 4736

8. Аракелян А.А. Агаян А.А. «Понятие и место кибертерроризма в уголовном праве России» // Сборник тезисов работ участников XVI Всероссийского молодежного форума «МОЯ ЗАКОНОТВОРЧЕСКАЯ ИНИЦИАТИВА» 2021 ГОД ТОМ I, ст.261 [Электронный ресурс] URL: https://integraciya.org/sborniki/

9. Бондарь, Е. О. Киберпреступность как новая криминальная угроза / Е. О. Бондарь // Вестник Московского университета МВД России. – 2020. – № 1. – С. 155-158.

10. Смоленский, М. Б. Законодательство о персональных данных как инструмент государственного регулирования в сфере информационных коммуникаций / М. Б. Смоленский, Н. С. Левшин // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2019. – № 5(108). – С. 75-80.