Законодательный щит

А. А. Салкуцан

магистрант 2 курса финансового факультета РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова»,
117997, Москва, Стремянный пер., д. 36.
E-mail: ol-1@mail.ru

Legislative Shield

A. A. Salkutsan

Master of the Second Year of the Faculty of Finance of the PRUE.
Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane,
Moscow, 117997, Russian Federation.
E-mail: ol-1@mail.ru

Аннотация

Сегодняшний мир трансформируется и становится полностью цифровым, меняя структуру экономик многих стран. Цифровая индустрия – одна из бурно развивающихся мировых отраслей, которая наращивает огромные обороты в глобальном пространстве. Данная ситуация породила множество проблем, среди них можно выделить рост числа компьютерных преступлений, совершенных с использованием различных аппаратно-программных средств, что способствовало краже информации. Для того чтобы контролировать ситуацию и отвечать на сегодняшние вызовы, государство и бизнес-структуры разрабатывают в правовой сфере множество законодательных актов и инструкций. В данной правовой сфере определяются понятия и критерии для определенных секторов экономики и классы для каждой потенциальной угрозы. Также основной акцент в законопроектах делается на внедрении на предприятиях внутренних правил, призванных обеспечить соблюдение антимонопольных требований.

Ключевые слова: законы, безопасность, киберпреступление, программа, секрет, бизнес, государство.

Abstract

Today's world is transforming and becoming completely digital, changing the structure of the economies of many countries. The digital industry is one of the world's booming industries, which is increasing huge turnover in the global space. This situation has caused a lot of problems, among them can be distinguished by the increase in the number of computer crimes committed with the use of various hardware and software, which contributed to the theft of information and became part of our lives. In order to control and respond to today's challenges, the state and business structures are developing a variety of legal acts and regulations in the legal sphere. In this sphere of law concepts and criteria are defined, which are contained in the main points for certain sectors of the economy and classes for each potential threat. Also, the main focus of the draft laws is on the introduction of enterprises internal rules designed to ensure compliance with antitrust requirements.

Keywords: law, security, cybercrime, software, secret, business, government.

На сегодняшний день информация, какой бы она ни была, должна охраняться четко разработанной и понятной нормативно-правовой базой, так как в глобальном информационном пространстве главную роль играет информационная безопасность.

Важно отметить, что не столько современные программно-технические изделия, сколько механизмы генерации новых решений и предложений в правовой сфере позво-

ляют отвечать на вызовы в бурном информационном прогрессе.

Сегодня информация, которая используется государственными структурами и бизнесом, регулируется не очень сильной законодательной базой в сфере информационной безопасности. Необходимо подчеркнуть, что для защиты субъектов информационных взаимоотношений затрагиваются четыре компонента:

- административный;
- законодательный;
- программно-технический;
- процедурный.

Важно отметить, что все субъекты информационных отношений создают механизмы, которые позволяют согласовать процессы разработки законов с реалиями цифровой эпохи, благодаря чему происходит максимальная автоматизация и наращивание информационного контроля.

Приведем перечень основных нормативно-правовых актов в России, которые затрагивают сферу информационной безопасности. К ним относятся [2]:

- Конституция Российской Федерации от 12 декабря 1993 г.;
- Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ;
- Гражданский кодекс Российской Федерации (часть вторая) от 26 января 1996 г. № 14-ФЗ;
- Гражданский кодекс Российской Федерации (часть четвертая) от 18 декабря 2006 г. № 230-ФЗ;
- Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ;
- Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ;
- Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ;
- Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (действует с 03.11.2011);
- Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» (действовал до 02.11.2011);
- Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»;
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
- Федеральный закон от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»;

– Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895;

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Постановление Правительства Российской Федерации от 26 января 2006 г. № 45 «Об организации лицензирования отдельных видов деятельности».

К нормативно-правовым актам, которые тесно взаимосвязаны с информационной безопасностью, а именно затрагивают сферу криптографии, относится следующая законодательная база:

- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 г. № 1-ФЗ (действовал до 01.07.2012);
- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (утверждено Приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. № 66);
- Постановление Правительства Российской Федерации от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;
- Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 976 «О Федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи»;
- Требования к форме квалифицированного сертификата ключа проверки электронной подписи (утверждены Приказом Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. № 795);
- Приказ Министерства связи и массовых коммуникаций Российской Федерации от 28 декабря 2011 г. № 360 «Об утверждении административного регламента предоставления Министерством связи и массовых коммуникаций Российской Федерации государственной услуги по подтверждению подлин-

ности ЭЦП уполномоченных лиц УЦ в выданных ими сертификатах ключей подписи»;

- Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (утверждена Приказом ФАПСИ РФ от 13 июня 2001 г. № 152).

Многие крупные компании в России используют различные аппаратные средства для защиты информации. Для того чтобы приобрести эти средства, они проходят два главных этапа: лицензирование и сертификацию [4]:

Данные этапы тоже в свою очередь регулируются законодательными актами:

- Федеральный закон от 10 января 2003 г. № 15-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона "О лицензировании отдельных видов деятельности"» (последняя редакция);

- Закон Российской Федерации от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

Обратим внимание, что данные законы контролируются и неукоснительно исполняются ФАПСИ России, которое регулирует сферу оборота криптографических средств, и ГОСТЭККОМИССЕЙ, которая специализируется на лицензировании.

В качестве примера можно привести средства защиты информации, которые сертифицированы ФАПСИ России:

- Комплекс виброакустической защиты «ЭШЕЛОН»;

- Защищенный абонентский пункт сети Интернет СТБ 502;

- Персональная электронная вычислительная машина «Базальт ВР-01» в защищенном исполнении;

- Защищенный абонентский пункт «Обруч АП-2»;

- Программно-аппаратный комплекс ViPNet IDS 2.0 (вариант исполнения 1: IDS 1000 Q1):

- Аппаратно-программный модуль доверенной загрузки «Центурион-Е» ИТБВ.468266.002-01 и т. д.

Сущность вышеизложенного сводится к тому, что все эти программно-аппаратные средства при реализации на рынках России должны в строгом порядке соответствовать требованиям ФАПСИ и ФСБ России, которые данные ведомства предъявляют к компаниям, предоставляющим услуги по безопасности информации. Стоит отметить, что данные аппаратные комплексы размещаются в особых помещениях и применяются для обработки общедоступной информации при условии выполнения требований руководства по эксплуатации.

Нельзя не согласиться, что вся законодательная база в сфере защиты информации постоянно совершенствуется и дополняется новыми актами, которые учитывают новые проблемы с безопасностью во Всемирной паутине.

Обратим внимание, что к концу 2020 г. Россия планирует разработать и внести в международные организации проекты нормативно-правовых актов, которые бы устанавливали мораторий на разработку, распространение и применение кибероружия.

Одновременно с этим российское правительство намерено инициировать подписание законов, определяющих условия и порядок определения источников киберугроз, т. е. методов обнаружения источника компьютерной атаки – ответственной за нее страны, организации или группы лиц.

Во многих зарубежных правовых актах понятие «кибероружие» трактуется по-разному. Так, не всегда к нему добавляются технические и программные средства, например, для совершения DDoS-атак или ведения слежки, но большинство экспертов в сфере информационной безопасности считают это ошибочным и определяют кибероружие как техническое средство, предназначенное непосредственно для нанесения ущерба в киберпространстве [2].

В качестве примера можно привести один из наиболее известных видов кибероружия – вирус Stuxnet, который обнаружили в 2010 г. на промышленных объектах Ирана. Суть данного вируса состоит в том, попав в блоки управления газовых центрифуг, предназна-

ченных для получения обогащенного урана, он выводил их из строя. Таким образом, можно сказать, что впервые в истории информационной эпохи компьютерный вирус разрушал физическую и информацию инфраструктуру на компьютерах в засекреченных объектах в Иране.

В одной из авторитетнейших газет США The New York Times вышла статья, которая пролила свет на данную компьютерную программу. Разведывательными службами США и Израиля велись разработки, целью которых была приостановка иранской ядерной программы.

Меры, ограничивающие разработку и распространение аппаратных средств, которые могут уничтожить, украсть, исказить информацию, на международной арене предпринимаются давно.

Так, например, инициативной группой правительственных экспертов в сфере информатизации и телекоммуникаций в контексте международной безопасности ООН в 2015 г. был оглашен доклад, который предлагал государствам на добровольной основе пресекать и предупреждать распространение преступных программных и технических средств в сфере информационно-коммуникационных технологий, которые содержали скрытые функции.

Стоит отметить, что в 2009 г. похожие определения и меры были упомянуты в текстах межправительственных соглашений Шанхайской организации сотрудничества. Так, соглашение считается единственным существующим многосторонним юридически обязывающим механизмом, ограничивающим деятельность государств по использованию информационно-коммуникационных технологий, которые бы прямо или косвенно касались информационной безопасности.

В то же время большинство норм и положений по информационной безопасности не получили практического развития. В 2011 г. Россия также выступала с концепцией конвенции об обеспечении международной информационной безопасности. Данный документ опирался на введение понятия «информационного оружия» и описывал меры по ограничению его распространения в рамках контроля военных конфликтов в информаци-

онном пространстве. Однако данный документ не был принят в серьез [3].

На практике ограничить разработку кибероружия практически невозможно, поскольку это не физическое оружие, для создания которого требуются железо и инфраструктура. Сегодня кибероружие может создать даже одиночка, и запретить ему это делать невозможно, даже несмотря на наличие соответствующих статей в уголовном кодексе многих стран.

Внедрение запрета на международном уровне и вовсе представляется нереальным в среднесрочной перспективе.

Ясно, что запретить кибероружие на международном уровне можно, но для этого в первую очередь надо дать этому термину корректное и полное определение, которого до сих пор не существует. Для начала нужно, чтобы к запрету на кибероружие присоединились все государства и крупные участники бизнеса.

В ходе обсуждений кибератак российские правоохранительные органы и компании, занимающиеся компьютерной криминалистикой, анализируют множество различных факторов, с помощью которых пытаются найти злоумышленников: место регистрации IP-адресов и доменов, участвующих в атаке, программный код, время проведения атаки и др. Но каких-либо единых принципов выявления источника кибератаки на международном уровне сейчас нет [3].

Отсутствие правил в сфере информационной безопасности позволило сначала США, а затем и ряду европейских стран обвинить Россию в атаке на выборы, WADA, государственные органы и частные компании.

Особо следует выделить, что при этом никаких доказательств не представлено, а санкции против нашей страны были введены. Это все равно что обвинить и затем осудить человека за преступление без каких-либо доказательств и проведения суда.

Поэтому, прежде чем обвинять какое-либо государство в киберагрессии, необходимо получить доказательства, которые бы принимались международным сообществом.

В заключение следует сказать следующее. Согласно опубликованным отчетам американских спецслужб, для определения хакерских атак на сервера Демократической

партии США в 2016 году. использовались четыре основных параметра – принадлежность IP-адресов российскому адресному пространству, время, в которое осуществлялись атаки, применение веб-сайтов с русскоязычным интерфейсом и использование вредоносных программ, продаваемых на русскоязычных форумах [5].

Однако даже беглый взгляд на эти атрибуты позволяет сделать вывод, что атака могла осуществляться не только из России, но и из сопредельных государств – Белоруссии, Украины, иных стран СНГ. Это если не рассматривать вариант, что Россию хотели

просто подставить и хакеры маскировались под российских.

Таким образом, можно сделать вывод, что в обозримом будущем вряд ли возможно создать некий единый универсальный алгоритм определения на уровне международного права, так как нет единого решения, это слишком сложно технически, а сценарии атак и сами инциденты слишком разнятся. Пока государства и компании могут лишь собирать лучшие практики и укреплять обмен ими в рамках расследования компьютерных инцидентов в сфере информационной безопасности.

Список литературы

1. Защита информации с человеческим лицом // itsec2012. – URL: <http://itsec2012.ru/normativno-pravovye-akty-po-informacionnoy-bezopasnosti> (дата обращения: 22.03.2018).
2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993; с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ. – 2014. – 4 августа. – № 31. – Ст. 4398.
3. Обзор законодательства Российской Федерации в сфере информационной безопасности. Часть 1: Общий обзор // Digital.Report. – URL: <https://digital.report/zakonodatelstvo-rossii-informatsionnaya-bezopasnost/> (дата обращения: 22.03.2018).
4. Правовое регулирование защиты информации в России // Enigma. – URL: http://www.enigma.ru/stat/dip_1 (дата обращения: 22.03.2018).
5. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция) // Справочно-правовая система «Консультант-Плюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 22.03.2018).