УДК 004.056.5

DOI: 10.37468/2307-1400-2020-2-36-42

МЕТЕЛЬКОВ АЛЕКСАНДР НИКОЛАЕВИЧ

О ПРОБЛЕМЕ ТЕХНИЧЕСКИХ МЕР В СИСТЕМЕ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АННОТАЦИЯ

В теории и на практике существует проблема снятия неопределенности в реализации технических мер из-за нечеткой правой регламентации классификации мер по обеспечению безопасности данных, автоматически обрабатываемых в информационных системах. В статье на основе применения теории множеств предлагается снять эту неопределенность методом выделения групп мер по обеспечению безопасности информации. Защита информации в Федеральном законе «Об информации, информационных технологиях и о защите информации» представляет собой принятие правовых, организационных и технических мер. Однако на практике в системе мер по обеспечению информационной безопасности объектов защиты они встречаются не только в «чистом» виде, но и в тесной взаимосвязи, взаимодействии между собой (организационно-правовые, организационно-технические, технико-правовые), и весьма часто не могут быть реализованы автономно.

Ключевые слова: меры безопасности; меры по обеспечению безопасности; меры защиты информации; персональные данные; технические меры; организационные меры; правовые меры; техническая защита информации; оператор; базовый набор мер.

METELKOV A. N.

ON THE PROBLEM OF TECHNICAL MEASURES IN THE SYSTEM OF MEASURES TO ENSURE INFORMATION SECURITY

ABSTRACT

In theory and in practice, there is a problem of removing uncertainty in the implementation of technical measures due to the unclear right-hand regulation of classification of measures to ensure the security of data automatically processed in information systems. In the article, based on the application of set theory, it is proposed to remove this uncertainty by selecting groups of measures to ensure the security of information. Information protection in the Federal law «on information, information technologies and information protection» is the adoption of legal, organizational and technical measures. However, in practice, in the system of measures to ensure the information security of objects of protection, they are found not only in a «pure» form, but also in a close relationship, interaction with each other (organizational-legal, organizational-technical, technical-legal), and very often can not be implemented independently.

Keywords: security measures; security measures; information protection measures; personal data; technical measures; organizational measures; legal measures; technical protection of information; operator; basic set of measures.

Анализ действующего законодательства в сфере технической защиты информации подтверждает мнение И.Л.Бачило о плохом взаимодействии нарастающего числа законов и иных нормативных правовых актов в информационной сфере, что «приводит к формированию цепочки правовой системы и законодательства, работающей самой на себя с очень малым коэффициентом влияния на реальные отношения людей и их организаций» [1]. Указанная особенность правового регулирования характерна для всей информационной сферы. Наглядно ее можно показать на примере технической защиты персональных данных.

Актуальность рассматриваемой проблемы определяется необходимостью организации технической защиты персональных данных для реа-

лизации требований приказа МЧС России от 31 октября 2019 г. № 626 «Об обработке и обеспечении защиты персональных в Министерстве Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий» [2]. Рассматриваемая проблема характерна практически для всех государственных и иных организаций, в информационных системах которых обрабатываются сведения ограниченного доступа, в том числе конфиденциальная информация и персональные данные.

При организации защиты персональных данных следует учитывать, что наличие системы защиты информации является лишь необходимым условием и не может рассматриваться критерием защищенности системы от реальных угроз, поскольку безопасность не является абсолютной характеристикой и может рассматриваться только относительно некоторой среды, в которой действуют определенные угрозы [3].

Согласно ст.16 базового Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» защита информации «представляет собой принятие правовых, организационных и технических мер, направленных на:

– обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
– соблюдение конфиденциальности информации ограниченного доступа;
– реализацию права на доступ к информации» [4].

Легкость запоминания и поиска информации в базах данных, которые обрабатываются в электронных вычислительных машинах, привели к необходимости защиты информации о личности. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных) определяет (ст.2) своей целью обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну [5]. Заявленная цель достигается реализацией мер по обеспечению безопасности (*мер безопасности* согласно Федеральному закону от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных») [6]. В статье 18.1.(пп.1) Закона о персональных данных предписано оператору[1] принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных рассматриваемым Законом и установленными в соответствии с ним нормативными правовыми актами. Оператор наделен правом самостоятельно определять состав и перечень указанных мер, если иное не предусмотрено федеральными законами. К таким мерам может, в частности, относится применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Закона о персональных данных. Однако Закон не дает четких критериев отнесения тех или иных мер к правовым, организационным и техническим.

В отличие от организационных мер, техническая защита информации является для оператора сложным, финансово затратным и трудоемким делом, при выполнении которого требуется соблюдение определенных условий. Поэтому важно иметь четкие критерии отнесения тех или иных мер по обеспечению безопасности к техническим.

При выборе мер по обеспечению безопасности персональных данных в соответствии с требованиями приказа ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах

1 Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

персональных данных» оператору «…необходимо определить базовый набор таких мер для установленного уровня защищенности персональных данных в соответствии определенными государственным регулятором нормами. Оператор должен адаптировать этот базовый набор с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы. Оператор также обязан:

– скорректировать адаптированный базовый набор с учетом не выбранных ранее мер, по результатам которого определить меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности для конкретной информационной системы;
– дополнить уточненный адаптированный базовый набор мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации» [7].

Нормативным правовым актом ФСТЭК России оператору предоставлено право разработать иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных, и обосновать их применение, если он не имеет возможности технической реализации отдельных выбранных мер, а также учитывая экономическую целесообразность на этапах адаптации и/или уточнения адаптированного базового набора мер. Компенсирующие меры должны разрабатываться как при использовании в информационных системах новых информационных технологий, так и при выявлении дополнительных угроз безопасности персональных данных, для которых не определены меры обеспечения их безопасности. Операторам, использующим в информационных системах сертифицированные по требованиям безопасности информации средства защиты, необходимо руководствоваться положениями п.12 нормативного документа, утвержденного приказом ФСТЭК России от 18 февраля 2013 г. №21. В документе определено какие средства вычислительной техники, системы обнаружения вторжений, средства антивирусной защиты, межсетевые экраны необходимо применять для обеспечения каждого из уровней защищенности персональных данных.

Как показывает анализ подзаконных нормативных правовых актов, методической, научной и учебной литературы в целом ряде случаев разновидности и содержание рассматриваемых мер в различных источниках их авторами трактуется по-разному, что не способствует операторам информационных систем осознанно и методологически выверено подходить к выбору и реализации технических мер по обеспечению безопасности защищаемой информации.

В числе основных требований[2] Закон о персональных данных предписывает в установленный срок обеспечить соответствующую защиту обрабатываемых персональных данных. Вновь создаваемые и вводимые в эксплуатацию информационные системы персональных данных должны соответствовать требованиям рассматриваемого Закона. За неисполнение требований предусмотрена юридическая ответственность.

На первый взгляд формулировка закона о выделении правовых, организационных и технических мер не вызывает существенных возражений. Однако зафиксированный законодателем перечень видов мер по обеспечению безопасности (правовые, организационные, технические) не дает операторам ясный методологический инструмент для дифференциации и применения указанных мер. В целом ряде случае организационные и технические, правовые и технические меры не могут быть реализованы и функционировать автономно.

В настоящее время затруднительно снять неопределенность при формулировании однозначного ответа на вопрос: «По каким критериям

2 При анализе системы мер по обеспечению безопасности мы исходим из того, что термин «защита информации» является родовым по отношению к термину «защита персональных данных».

(или критерию) те или иные меры группируются в правовые, технические или организационные меры»?

В законодательстве не содержится четких норм, определяющих критерии отнесения тех или иных мер к техническим или организационным.

Рассмотрим математическую модель мер по обеспечению безопасности с позиции теории множеств. Согласно норм действующей нормативной правовой базы множество технических мер и множество организационных мер можно представить двумя пересекающимися множествами. Такая модель более точно и объективно отражает реальное положение дел. Меры, которые включены в так называемую «серую» зону пересечения этих двух множеств, входят как в состав технических, так и в состав организационных мер, то есть их однозначно отнести только к одному из их видов (организационным или техническим) по действующему законодательству невозможно. Таким образом, в виду нечеткости юридической формулировки возникает организационно-правовая неопределенность в классификации видов мер по обеспечению безопасности. Поэтому вопрос в отграничения технических мер от иных мер по обеспечению безопасности в *нормативной правовой базе по защите информации* остается открытым и требует уточнения. Безусловно, и нередко эта особенность отмечается исследователями, все разновидности мер по обеспечению безопасности информации взаимосвязаны между собой.*Прямая связь объективно существует* между организационными и техническими мерами, техническими и правовыми мерами, организационными и техническими.

Рассмотрим взаимосвязь и взаимозависимость технических и правовых мер. Иногда трудно разделить организационные и технические меры, так как без одних мер другие могут вообще не запуститься при функционировании систем защиты. Например, если часть технических мер (антивирусная защита и т.п.) включена в нормативные правовые акты, то эта мера уже вошла в состав и приобрела статус правовой меры. Вместе с тем она не утратила свою «техническую» природу, то есть она стала теперь и правовой, и технической. Возникает вопрос: к какому же виду мер (правовым или техническим) в данном случае следует оператору их относить? Из-за размытости их содержания действующее законодательство не дает определенный ответ на этот вопрос. Очевидно, нечеткость формулирования понятий негативно отражается на практической деятельности оператора при разработке и внедрении технических мер защиты. В результате операторами по-разному могут трактоваться понятия «организационные» и «технические» меры, что подтверждается методом опроса специалистов в сфере эксплуатации информационных технологий. В частности, проведенный автором опрос группы специалистов в сфере технической защиты информации (свыше 40 человек из различных регионов страны) показал, что подавляющее большинство из них антивирусную защиту, аутентификацию и идентификацию относят к техническим мерам, и лишь отдельные – к правовым.

Нередко в литературе и нормативных документах термины «организационные» и «технические» меры употребляются совместно, а собственно организационные и технические меры не выделяется. С позиции методологического подхода технические меры, которые получили правовую форму, безусловно, следует считать правовыми. В частности, «состав и содержание мер по обеспечению безопасности персональных данных включает меры по:

- идентификации и аутентификации субъектов доступа и объектов доступа;
- управлению доступом субъектов доступа к объектам доступа;
- ограничению программной среды должны обеспечивать установку и (или) запуск;
- защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных);
- регистрации событий безопасности;
- антивирусной защите должны обеспечивать обнаружение в информационной системе

компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;

- обнаружению и предотвращению вторжений;
- контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных;
- обеспечению целостности информационной системы и персональных данных;
- обеспечению доступности персональных данных;
- защите среды виртуализации;
- защите технических средств.
- защите информационной системы, ее средств, систем связи и передачи данных;
- выявлению инцидентов и реагированию на них;
- управлению конфигурацией информационной системы и системы защиты персональных данных» [7]. Так как технические меры, которые включены в вышеуказанный перечень, определены нормативным правовым актом ФСТЭК России, они приобрели статус правовых мер. При этом содержание таких мер ставится в зависимость от уровня защищенности персональных данных.

С организационно-практической и методологической точек зрения целесообразно более четко в законодательстве отграничить технические меры от правовых и организационных мер. В законодательстве они определены, если их условно рассматривать с позиций теории множеств, как три непересекающиеся множества (множество правовых мер, множество технических мер, множество организационных мер). Такая организационно-правовая модель не отражает реальное положение.

Для решения этой задачи авторами предлагается метод правового критерия определения технических мер, который позволит отделить их от «чисто» правовых и организационных мер.

Наглядно такой метод можно описать с использованием теории множеств. Условно представим правовые, организационные и технические меры соответственно в виде трех множеств *A*, *B* и *C*. Согласно действующему законодательству эти три множества - непересекающиеся, хотя в действительности A и B, B и C, A и C пересекающиеся множества (см. рис 1).

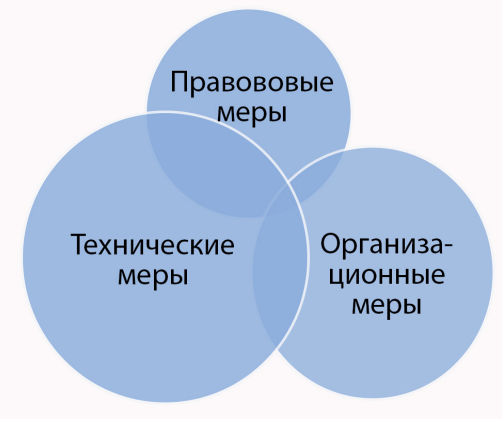

Рисунок 1 – Предложенная автором модель взаимодействия правовых, организационных и технических мер

В ряде подзаконных нормативных правовых актов регуляторов, учебной и научной литературе технические и организационные меры обоснованно указываются неразрывно. Содержание правовых мер в каждый момент времени *t* определено действующим в рассматриваемый период законодательством Российской Федерации, регулирующим правоотношения в информационной сфере, то есть является относительно стабильной (постоянной) во времени величиной. Содержание правовых мер меняется в случае принятия новых законов или внесения изменений и дополнений в действующие нормативные правовые акты. Следует заметить, что исключение упоминания правовых мер в законодательстве возможно во многом бы сняло существующую неопределенность в содержании организационных и технических мер. При этом правовые меры от этого никаким образом бы

не пострадали, так как в правовых нормах важно их содержание, которое отражается в самих нормативных правовых актах по защите информации. Зарубежный опыт правового регулирования вопроса защиты персональных данных подтверждает это предложение. Например, в руководящем документе Европейского Союза 02016R0679-EN-04.05.2016 – 000.002-22 по защите персональных данных использованы понятия «организационных и технических мер», а правовые не выделяются.

Состав конкретных организационных и технических мер более разнообразен и динамичен, чем он описан в действующих нормативных правовых актах, так как объективно нормативное регулирование отстает от реальных потребностей операторов по защите информации от постоянно возникающих новых угроз. С учетом повсеместного применения информационных технологий и недостаточной развитости защитных мер статистика показывает рост компьютерных преступлений, а специалисты прогнозируют их увеличение в России в ближайшие годы. Состав таких мер постоянно уточняется в связи с появлением или, наоборот, устранением (исчезновением) внутренних и внешних угроз, изменением состояния среды и других факторов и условий. Возможно, некоторые из организационных и технических мер, регулирующих наиболее важные правовые отношения в информационной сфере, будут в дальнейшем закреплены в законодательстве и приобретут статус правовых. В рамках предлагаемого метода следует выделить два подхода к определению содержания таких мер. Один из таких подходов заключается в том, что если технические или организационные меры, включены в нормативные правовые акты Российской Федерации, то формально их можно относить только к правовым мерам и уже не считать организационными или техническими мерами. Тогда множество «чисто» технических мер можно записать в следующем виде: $C\backslash(A \cap B)$.

Технические меры защиты персональных данных реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

Рассмотрим содержание правовых мер. Выделенные «правовые» меры, как показывает анализ нормативных правовых актов в сфере информационной безопасности, имеют широкое толкование по объему. В него включаются не только меры, названные в федеральных законах, но и указанные в нормативных правовых актах Президента Российской Федерации и Правительства Российской Федерации, а также во многочисленных подзаконных нормативных правовых актах федеральных органов исполнительной власти и даже в локальных актах организаций.

По мнению автора, «правовые меры» можно дифференцировать на законодательные и иные правовые меры. Законодательные меры прямо закреплены только в федеральных законах. Согласно статье 4 Федерального закона от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее - Закон об информации) законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из Закона об информации и других регулирующих отношения по использованию информации федеральных законов. Правовые меры, как правило, в юридической форме закрепляют организационные и технические меры по обеспечению безопасности. Вхождение в состав правовых мер технических норм не приводит к нейтрализации их технического содержания. Они по своему содержанию остаются техническими мерами. В тоже время они приобретают определенную правовую форму.

Другая часть технических мер (C^1), которая не получила нормативного закрепления, реализуется операторами по обеспечению безопасности и защиты информации самостоятельно с учетом новых условий и факторов. Технические меры ($C-C^1$), которые входят в состав как правовых, так и технических мер, являются пересечением двух множеств А и С. Их можно описать выражением: $A \cap C$.

Однако в действующем законодательстве в сфере информационной безопасности нет полной ясности к каким мерам (правовым или техническим) их относить оператору. Поэтому простое упоминание в Законе о защите информации «правовых» мер не уменьшает неопределенность в определении объема и содержания технических мер.

Другой предложенный авторами, на наш взгляд, более конструктивный метод предусматривает выделение в федеральном законе правовых, организационных, организационно-технических, программно-технических (или просто технических, включая криптографические – как особую разновидность технических мер) и иных компенсирующих мер. В этом случае множество технических мер можно представить в таком виде: $C\backslash(A \cap B)$.

Таким образом, в целях совершенствования технической защиты информации целесообразно нормативно закрепить один из предложенных методологических подходов к выделению так называемых «чисто» технических мер посредством дифференциации разновидности мер по обеспечению безопасности и защите информации.

Список литературы

1. *Бачило И.Л.* О подходах к совершенствованию информационного законодательства // Информационная безопасность регионов России (ИБРР-2013): материалы VIII Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 23-25 октября 2013. – СПб.: СПОИСУ, 2013. – С. 27-28. [Электронный ресурс]. – Режим доступа: http://www.spoisu.ru/files/ibrr/ibrr2013/ibrr2013_materials.pdf

2. Приказ МЧС России от 31 октября 2019 г. № 626 «Об обработке и обеспечении защиты персональных в Министерстве Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий».

3. *Аникин И.В., Глова В.И., Нейман Л.И., Нигматуллина А.Н.* Теория информационной безопасности и методология защиты информации: учебное пособие. – Казань: Изд-во Казан. гос. техн. ун-та, 2008. – С.12-13.

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

5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

6. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

7. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691 (дата обращения 07.05.2020).

Статья поступила в редакцию 14 мая 2020 г.
Принята к публикации 21 июня 2020 г.

Ссылка для цитирования: Метельков А.Н. О проблеме технических мер в системе мер по обеспечению информационной безопасности // Национальная безопасность и стратегическое планирование. 2020. № 2(30). С. 36-42. DOI: https://doi.org/10.37468/2307-1400-2020-2-36-42