ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.5

DOI: 10.37468/2307-1400-2020-4-68-78

МЕТЕЛЬКОВ АЛЕКСАНДР НИКОЛАЕВИЧ

О КРИПТОГРАФИЧЕСКИХ МЕРАХ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВНЕДРЕНИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РЕШЕНИЕ ЗАДАЧ УПРАВЛЕНИЯ В СОЦИАЛЬНЫХ И ЭКОНОМИЧЕСКИХ СИСТЕМАХ

АННОТАЦИЯ

В теории и на практике существует неопределенность в существовании мер криптографической защиты информации из-за нечеткой правой регламентации классификации мер защиты информации, связанных с применением криптографических методов и шифровальных (криптографических) средств защиты информации по обеспечению безопасности данных, автоматически обрабатываемых в информационных системах. Криптографические методы широко используются не только для защиты информации от несанкционированного доступа, но и в качестве основы ряда современных информационных технологий. Автором предложено ввести в научный оборот понятие «криптографические меры защиты информации», и включить это понятие в базовый закон о защите информации. Защита информации в Федеральном законе «Об информации, информационных технологиях и о защите информации» представляет собой принятие правовых, организационных и технических мер. В статье на основе применения теории множеств предложена модель групп мер по обеспечению безопасности информации, включая криптографические.

Ключевые слова: криптографические меры, информация, криптография, математические методы, криптографическая защита, криптографические методы, криптографические средства, криптографические преобразование, защита конфиденциальной информации, информационные технологии.

METELKOV A. N.

ABOUT CRYPTOGRAPHIC INFORMATION PROTECTION MEASURES IN THE IMPLEMENTATION OF INFORMATION TECHNOLOGY IN THE SOLUTION OF MANAGMENT PROBLEMS IN THE SOCIAL AND ECONOMIC SYSTEMS

ABSTRACT

In theory and in practice, there is uncertainty in the existence of measures for cryptographic protection of information due to the fuzzy legal regulation of the classification of information protection measures associated with the use of cryptographic methods and encryption (cryptographic) information protection tools to ensure the security of data automatically processed in information systems. Cryptographic methods are widely used not only to protect information from unauthorized access, but also as the basis for a number of modern information technologies. The author proposed to introduce the concept of "cryptographic measures of information protection" into scientific circulation, and to include this concept in the basic law on information protection. Information protection in the Federal Law "About Information, Information Technologies and Information Protection" is the adoption of legal, organizational and technical measures. In the article, based on the application of set theory, a model of groups of measures to ensure information security, including cryptographic ones, is proposed.

Keywords: cryptographic measures, information, cryptography, mathematical methods, cryptographic protection, cryptographic methods, cryptographic instrument, cryptographic transformation, protection of confidential information, information technology.

Расширение областей применения информационных технологий в решении задач управления как важный фактор развития экономики и совершенствования функционирования общественных и государственных институтов порождает новые информационные угрозы. Возможности трансграничного оборота информации используются для достижения геополитических, противоречащих

международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей. При этом практика внедрения информационных технологий, как отмечено в Доктрине информационной безопасности в Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. N 646, без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

Согласно Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. N 683, стратегия реализуется также за счет комплексного использования политических, организационных, социально-экономических, правовых, информационных, военных, специальных и иных мер. Таким образом, в основе реализации Стратегии национальной безопасности Российской Федерации лежит именно комплексное использование различных мер. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам.

Система обеспечения информационной безопасности – совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности. Осуществление такой деятельности связано с принятием соответствующих мер. Силами обеспечения информационной безопасности при принятии необходимых мер используются правовые, организационные, технические и другие средства обеспечения информационной безопасности. В соответствии с Положением «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утвержденной Постановлением Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. № 912-51, работы по защите информации в органах государственной власти и на предприятиях проводятся на основе актов законодательства Российской Федерации, а конкретные методы, приемы и меры защиты информации разрабатываются в зависимости от степени возможного ущерба в случае ее утечки, разрушения (уничтожения).

В целях обеспечения государственной и общественной безопасности совершенствуется система выявления и анализа угроз в информационной сфере, противодействия им. Принимаются меры для повышения защищенности граждан и общества от деструктивного информационного воздействия со стороны экстремистских и террористических организаций, иностранных специальных служб и пропагандистских структур.

Бурное развитие информационных технологий и внедрение автоматизированных методов и средств обработки информации в различные сферы деятельности людей привели к широкому использованию криптографических средств защиты информации. К. Шенноном были выделены три направления или три метода защиты информации: психологический, технический и криптографический [6]. Выдающимся исследователем технический и криптографический методы рассматриваются как самостоятельные методы, раздельно.

Предотвращение перехвата техническими средствами сведений, передаваемых по каналам связи, достигается применением криптографических и иных методов и средств защиты, а также проведением организационно-технических и режимных мероприятий. Авторами книги «Основы криптографии» справедливо подчеркивается, что «без использования криптографии сегодня немыслимо решение задач по обеспечению безопасности информации, связанных с конфиденциальностью и целостностью, аутентификацией и невозможностью отказа сторон от авторства» [1]. Если до 1990 г. криптография обеспечивала только закрытие государственных линий связи, то благодаря развитию компьютерных сетей и электронного обмена данными криптографические методы стали широко применяться в финансовом и банковском деле, торговле, медицине и других сферах человеческой деятельности.

Криптографическая защита – это защита данных с помощью криптографического преоб-

разования, под которым понимается преобразование данных шифрованием и (или) выработкой имитовставки [8]. Известны методы криптографического закрытия информации, которые классифируются по типу ключей, по размеру блока информации, по характеру производимых над данными воздействий, а также аналитические, аддитивные (гаммирование) и комбинированные методы.

Криптографические методы нашли широкое применение не только для защиты информации от несанкционированного доступа, но и в качестве основы многих новых информационных технологий: электронного документооборота, электронных денег, тайного электронного голосования [3, с.5]. Представляется, что значение криптографических методов в указанных областях будет возрастать и далее [1, с.3], а также будет усиливаться роль и значение математического метода в развитии криптографических алгоритмов.

В современной криптографии, образующей отдельное научное направление на стыке математики и информатики, математические методы играют главную роль. Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Криптография – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации. В ГОСТ Р ИСО 7498-2-99 термин криптография определяется в качестве дисциплины, охватывающей принципы, средства и методы преобразования данных для сокрытия их информационного содержимого, предотвращения их необнаруживаемой модификации и/или их несанкционированного использования. В ГОСТ Р ИСО/ТО 13569-2007 криптография определяется как математический аппарат, используемый для шифрования или аутентификации информации.

Криптография дает средства для защиты информации, и поэтому она является частью деятельности по обеспечению безопасности информации. Криптография предоставляет средства для обеспечения конфиденциальности информации при передаче сообщений по контролируемому злоумышленником (нарушителем, противником) каналу связи. Только криптография способна обеспечить конфиденциальность информации при хищении носителя информации [1]. Криптография утвердилась как важнейшее средство защиты информации и обеспечения государственной безопасности [6]. В отличие от существующих методов криптография преобразует сообщения в форму, недоступную для понимания даже при полном контроле противником канала связи.

Рассуждая о криптографических средствах защиты информации, можно утверждать об их ключевой роли в системе мер защиты конфиденциальной информации. Значимость роли криптографических средств определяется высокой надежностью защиты от актуальных угроз непосредственно самой конфиденциальной информации. Однако, несмотря на важность криптографических мер в защите конфиденциальной информации, они в настоящее время не нашли должного отражения в нормативных правовых актах Российской Федерации и руководящих документах государственных регуляторов, технической и учебной литературе, что не соответствует их роли в защите данных в условиях информатизации различных сфер государственного управления и жизнедеятельности общества.

Согласно ГОСТ Р 53110-2008 техническое направление обеспечения информационной безопасности включает в себя «мероприятия и действия» по:

а) выполнению функциональных требований безопасности, путем: – определения функциональных мер безопасности; – внедрения, осуществления эксплуатации и контроля за техническим обслуживанием механизмов обеспечения безопасности и средств защиты, реализующих меры обеспечения безопасности; б) реализации разрешительной системы допуска обслуживающего персонала к работам, документам и информации управления средствами связи; в) разграничению доступа обслуживающего персонала к информационным ресурсам, программным средствам обработки

(передачи) и защиты информации в подсистемах различного уровня и назначения; г) учету активов, регистрации действий пользователей и обслуживающего персонала, контроля за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц; д) предотвращению атак и внедрения в средства связи и автоматизированные системы программ-вирусов и программных закладок; е) применению СКЗИ при необходимости для защиты обрабатываемой информации; ж) надежному хранению носителей информации, ключей (ключевой документации) и их обращения, исключающего хищение, подмену и уничтожение; и) резервированию технических средств, баз данных и носителей информации; к) оборудованию информационных систем, средств связи и СВТ устройствами защиты от сбоев электропитания и помех в линиях связи; л) постоянному обновлению технических и программных средств защиты от несанкционированного доступа к средствам связи и антивирусных средств в соответствии с меняющейся окружающей обстановкой. Приказом ФСБ России от 10 июля 2014 г. N 378 г. определены состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации (СКЗИ), необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности. Применение таких организационных и технических мер обеспечивает оператор с учетом требований эксплуатационных документов на СКЗИ, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах.

Анализ приведенных выше положений позволяет отнести в некоторой мере криптографические средства защиты информации к техническому направлению обеспечения информационной безопасности. Однако такая позиция в документах не всегда поддерживается. В частности, ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» рассматривает техническую защиту информации как защиту информации, заключающуюся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств. При этом понятия «правовая защита информации», «техническая защита информации», «криптографическая защита информации» разделены и рассматриваются как самостоятельные одноранговые термины. Выделение в организационно-правовых документах мер защиты (правовых, организационных, технических) непосредственно связано с применением правовых, организационных и технических средств. Однако криптографические средства с какой-либо самостоятельной группой мер в теории и документах регуляторов не связываются. Криптографическая защита информации определена как «защита информации с помощью ее криптографического преобразования». ГОСТ Р ИСО/МЭК ТО 19791-2008 «Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» определяет меры безопасности как совокупность мер защиты и контрмер. Меры обеспечения безопасности (security controls) объединяют управленческие, организационные и технические меры обеспечения безопасности, применяемые в информационной системе для защиты и доступности системы и ее информации. Под управленческими мерами безопасности (management controls) понимаются меры безопасности информационной системы, направленные на менеджмент рисков и менеджмент информационной безопасности информационных систем. Организационные меры безопасности (operational controls) представляют собой меры безопасности информационной системы, которые, главным образом, реализуются и выполняются операторами, а не системами. Термин «технические меры безопасности» (technical controls) определяется как меры безопасности информационной системы, которые реализуются и выполняются самой информационной системой через механизмы, содержащиеся в аппаратных,

программных или программно-аппаратных компонентах системы. В Положении о порядке разработки, производства (изготовления), реализации, приобретения и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, в программно-технические средства обеспечения безопасности информации включены криптографические средства. В указанном руководящем документе определено, что на стадии проектирования и создания объекта информатизации оформляются технический проект и эксплуатационная документация СЗИ, состоящие из пояснительной записки с изложением решений по комплексу организационных мер и программно-техническим (в том числе криптографическим) средствам обеспечения безопасности информации, составу средств защиты информации. В Типовых требованиях по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 г. N 149/6/6-622 (в настоящее время утратили актуальность) содержалось положение о том, что оператор или уполномоченное им лицо осуществляет «описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности персональных данных с использованием криптосредств при их обработке в информационных системах,…». Таким образом, с точки зрения регулятора применение криптосредств согласно ранее действовавшему руководящему документу охватывалось принятием организационных и технических мер. В Положении о лицензировании деятельности по технической защите конфиденциальной информации, утвержденном постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79, понятие «техническая защита информации» определено достаточно широко, и может, по нашему мнению, включать шифровальные (криптографические) средства, предназначенные для защиты конфиденциальной информации от несанкционированного доступа. Под технической защитой конфиденциальной информации в рассматриваемом Положении понимается выполнение работ и (или) оказание услуг по ее защите от несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней. В действовавшем до его принятия Положении о лицензировании деятельности по технической защите конфиденциальной информации, утвержденной постановлением Правительства Российской Федерации от 15 августа 2006 г. N 504, под технической защитой конфиденциальной информации понимался «комплекс мероприятий и (или) услуг…». Важно подчеркнуть, что техническая защита – это не только защита от утечки информации по техническим каналам, но и защита от НСД, от математического воздействия, от вредоносных программ и т.п. Объектами технической защиты информации могут быть:- объект информатизации; – информационная система; – ресурсы информационной системы; информационные технологии; программные средства; – сети связи. Следовательно, рассуждая логически, в содержание термина «технические средства защиты информации» формально возможно включение СКЗИ.

Как известно, в основу классификации требований к безопасности с учетом сложности информационных систем (ИС) положена существующая классификация АС и ИС по безопасности и защищенности в соответствии с РД ФСТЭК России (до 2002 г. Гостехкомиссии России). В общем случае, комплекс требований и мер решений по защите информации от несанкционированного доступа (НСД) реализуется в рамках системы защиты информации от НСД, состоящей из следующих четырех групп требований: – управления доступом; – регистрации и учета; – криптографической защиты; – обеспечения целостности.

Согласно статье 71 Конституции Российской Федерации обеспечение безопасности личности,

общества и государства при применении информационных технологий, обороте цифровых данных находится в исключительном ведении государства. Следует подчеркнуть, что принятие и развитие мер защиты информации и мер безопасности (мер по обеспечению безопасности) исторически осуществлялось разными государственными регуляторами, что привело к появлению особенностей и усложнению терминологического аппарата, а также отразилось во взглядах исследователей на применение в построении теоретических подходов к определению таких терминов как «меры», «мероприятия», «методы», «требования», «средства» и др. Можно предположить, что в основу выделения правовых, организационных и технических мер защиты информации взят критерий выбора средств и/или методов защиты. И.Н.Васильева выделяет организационные, технологические, правовые обобщенные категории методов защиты информации. Технологические методы включают в себя криптографические, технические, аппаратные и аппаратно-программные, программные [4, с.41]. Е.В. Вострецова выделяет технические, программные, организационные, законодательные и морально – этические средства защиты информации [5, с.28-30]. Ю.И. Коваленко полагает, что информационная безопасность процессов изготовления ключевой информации документов СКЗИ должны обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты [11, с.158]. В научной литературе и документах существуют и другие подходы к классификации мер и средств защиты информации.

В рамках существовавших ранее «представлений о защите информации практически независимо развивались следующие виды защиты: организационная защита (режим секретности), техническая (противодействие техническим средствам разведки), криптографическая и обеспечение компьютерной безопасности. При этом имело место дублирование решаемых задач» [7, с.35]. В ГОСТ Р 53114-2008 понятие «техническое средство обеспечения информационной безопасности» определено как «оборудование, используемое для обеспечения информационной безопасности организации некриптографическими методами. Такое оборудование может быть представлено техническими и программно-техническими средствами, встроенными в объект защиты и/или функционирующими автономно (независимо от объекта защиты)». Вместе с тем понятие криптографические (шифровальные) средства широко используется в научно-технической литературе и нормативных правовых актах, однако соответствующих таким средствам мер в законодательстве Российской Федерации не установлено.

Такими мерами, на наш взгляд, могли бы быть криптографические меры.

В подтверждение существования термина «криптографические меры» служит ГОСТ Р ИСО/МЭК ТО 19791-2008, в котором используется понятие «криптографические меры обеспечения безопасности для защиты информации». Неудачность термина «криптографические меры обеспечения безопасности для защиты информации» заключается в его несоответствии нормам базового Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. N 149-ФЗ о том, что «защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: 1) обеспечение защиты информации…». В нормативном правовом акте «защита информации» не совсем корректно определяется через родственное понятие «обеспечение защиты информации». При этом указаны только три самостоятельных группы мер, что не отражает реальное положение дел.

Попытаемся выяснить место криптографических мер в системе защиты информации ограниченного доступа, определить их соотношение с техническими мерами. В документах государственного регулятора (в частности, в приказе ФСТЭК России от 15 февраля 2017 г. N 27) в сфере технической защиты информации определено, что «технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они

реализованы, имеющих необходимые функции безопасности». Аналогично, по нашему мнению, криптографические меры защиты информации реализуются путем применения СКЗИ. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами. Например, при обработке персональных данных оператор обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

В связи с тем, что законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. N 149-ФЗ и других регулирующих отношения по использованию информации федеральных законов, обратимся к их содержанию. Согласно статье 16 Федерального закона N 149-ФЗ «защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; 2) соблюдение конфиденциальности информации ограниченного доступа; 3) реализацию права на доступ к информации». Исходя из данного определения достаточно сложно ответить на вопрос: «К какому виду мер (правовым, организационным или техническим) возможно отнести криптографические меры»? К сожалению, следует констатировать, что меры защиты информации, связанные с применением криптографических методов, «выпали» из законодательной классификации. Криптографические меры тесно взаимосвязаны как с техническими, так организационными и правовыми мерами. Данный вывод автора подтверждает содержание методического документа «Меры защиты информации в государственных информационных системах», утвержденного ФСТЭК России 11 февраля 2014 г. В нем прямо сказано о том, что правила выбора и реализации «мер защиты информации, связанных с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации», в указанном документе не рассматриваются. Однако существование криптографических мер не отрицается, а, наоборот, подразумевается. Принятие таких мер защиты информации обеспечивается в соответствии с законодательством Российской Федерации. Таким образом, в документе ФСТЭК России допускается отдельное от технических мер существование «мер защиты информации, связанных с применением криптографических методов … и средств …» (то есть криптографических мер), которые выводятся за рамки деятельности по технической защите информации. Однако в федеральных законах и нормативных правовых актах Российской Федерации, многочисленной технической литературе по информационной безопасности автору не удалось обнаружить какого-либо упоминания о криптографических мерах защиты информации. На практике криптографическое закрытие информации осуществляется аппаратно, программно- и аппаратно-программно (программно-аппаратно).

Назовем меры защиты информации, связанные с применением криптографических методов и средств, криптографическими мерами. Для раскрытия их сущности рассмотрим особенности криптографических средств, так как основным содержанием и особенностью криптографических мер является применение криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

Криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности [1, с.8]. Специфика криптографических

средств защиты проявляется в методе криптографического преобразования, основанном на математике. В настоящее время, как правило, каждая из «криптографических задач … формализуется и решается средствами математики» [2]. В приложении 2 к Приказу Министерства образования и науки Российской Федерации от 12 сентября 2013 г. N 1060 «Об утверждении перечней специальностей и направлений подготовки высшего образования, применяемых при реализации образовательных программ высшего образования, содержащих сведения, составляющие государственную тайну или служебную информацию ограниченного распространения» (с учетом изм. в соответствии с приказом Минобрнауки России от 23 марта 2018 г. N 210) криптография включена в блок дисциплин «Инженерное дело, технологии и технические науки» наряду с информатикой и вычислительной техникой, информационной безопасностью, противодействием техническим разведкам, инфокоммуникационные технологии и системы. Специальность «Криптография» (10.05.06) является инженерно-технической дисциплиной, которая занимается математическими методами защиты информации. Криптография – область научных, технических исследований и практической деятельности, которая связана с разработкой средств криптографических защиты информации от угроз со стороны противника и/или нарушителя, а также анализом и обоснованием их стойкости криптографической. Основной задачей криптографии является обеспечение конфиденциальности, целостности, аутентификации, невозможности отказа, неотслеживаемости. В отличие от организационных и других способов защиты информации, под криптографическими понимаются такие, которые используют математические методы преобразования защищаемой информации.

В криптографии нашло отражение сложное противоречивое взаимодействие техники и математики. Между техникой как средством человеческой деятельности и математикой, как наукой о рациональной форме человеческих знаний, возникли взаимоотношения, исторически имеющие диалектически противоречивый характер. Концептуальный аппарат математических теорий, результаты прикладных математических исследований оказывают существенное влияние на решение практических задач в обеспечении безопасности информации и характер теоретического описания исследуемых информационных процессов. Метод криптоанализа сводится к решению разнообразных математических задач (например, к решению систем нелинейных уравнений в разнообразных алгебраических структурах, определению начального состояния автомата по его выходной и входной последовательностям, определению входной последовательности автомата по его начальному состоянию и выходной последовательности и др.). Нахождение эффективных алгоритмов решения какой-либо из этих математических задач может значительно понизить криптографическую стойкость многих шифров [2, с.230].

Национальным стандартом определены алгоритмы базовых блочных шифров, которые применяются в криптографических методах обработки и защиты информации, в том числе для обеспечения конфиденциальности, аутентичности и целостности информации при ее передаче, обработке и хранении в автоматизированных системах. Определенный в стандарте ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая» алгоритм криптографического преобразования предназначен для аппаратной или программной реализации. Стандарт рекомендуется использовать при создании, эксплуатации и модернизации систем обработки информации различного назначения.

Криптографические средства и методы широко применяются для защиты персональных данных. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы. Такая система включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах. Криптографические меры в систему защиты персональных данных включены опосредовано через выбор средств и мето-

дов защиты информации для этой системы. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми ФСБ России и ФСТЭК России.

При выработке теоретических взглядов на выделение криптографических мер защиты важно проанализировать соответствующие положения доктринальных документов. Согласно определению, предложенному в Доктрине информационной безопасности Российской Федерации (далее -Доктрина), обеспечение информационной безопасности представляет собой «осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления». Как известно защита информации является одним из элементов информационной безопасности. Средства обеспечения информационной безопасности в Доктрине определены как правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности. Если криптографические средства, реализующие криптографические меры, в силу их технико-математической специфики, можно выделить в самостоятельную группу мер, то они могут быть, на наш взгляд, охвачены с точки зрения Доктрины понятием «другие» меры.

В ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» мера безопасности, мера обеспечения безопасности определяются как сложившаяся практика, процедура или механизм обработки риска, а меры обеспечения информационной безопасности как совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности. Следует подчеркнуть, что техническое средство обеспечения информационной безопасности определено как «оборудование, используемое для обеспечения информационной безопасности организации некриптографическими методами». Такое оборудование может быть представлено техническими и программно-техническими средствами, встроенными в объект защиты и/или функционирующими автономно. В подтверждение необходимости введения в научный оборот термина «криптографические меры» служит ГОСТ Р ИСО/МЭК ТО 19791-2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем», в котором используется сложное и внутренне противоречивое понятие «криптографических мер обеспечения безопасности для защиты информации». В частности, раскрывая составляющие политики в области криптографии в документе указывается, что функции безопасности, реализуемые организационными мерами (ОФБ), должны определять криптографическую политику использования криптографических мер обеспечения безопасности в FOS_POL.4.1 «…для защиты информации в соответствии с релевантными соглашениями, законами и положениями», а в FOS_POL.4.2 «…для защиты информации».

Одно из значений слова «мера», которое используется в русском языке в словосочетаниях «принять меры», «осуществить меры» и им подобных означает «действие или совокупность действий, средств для осуществления чего-либо» [10,с.252], «мероприятие, способ действия» [11, с.184] «средство для осуществления чего-нибудь, мероприятие» [9, с.289]. Исходя из определения рассматриваемого значения понятия «меры» криптографические меры как совокупность действий, направленных на разработку и/или практическое применение методов и средств криптографии целесообразно включить в состав научно-технических, либо иных мер, либо прямо указать в законодательстве «криптографические меры». В руководящем документе ПКЗ-66 существование таких мер уже просматривается. В частности, с целью оценки обоснованности и достаточности мер, принятых для защиты информации конфиденциального характера, обладатель, пользователь (потребитель) данной информации, установивший режим ее защиты

с применением СКЗИ, а также собственник (владелец) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ, вправе обратиться в ФСБ России с просьбой о проведении контроля за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования СКЗИ. При этом СКЗИ должны удовлетворять требованиям технических регламентов, оценка выполнения которых осуществляется в порядке, определяемом Федеральным законом от 27 декабря 2002 года N 184-ФЗ «О техническом регулировании».

Дискуссия о целесообразности выделения и определения места криптографических мер в системе защиты информации и обеспечения безопасности информации носит объективный характер и связана с особым статусом криптографических методов, реализуемым в СКЗИ. Из всех существующих методов только криптография защищает саму информацию путем ее математического преобразования с использованием криптографических алгоритмов. В таких методах находит отражение не только противоречивое взаимодействие двух понятий «техники» и «математики», но многовековой опыт закрытости, замкнутости методов и средств криптографии на решение специфических государственных задач (оборона, безопасность, дипломатия и т.п.). На основе непосредственных запросов техники к проблемам развития средств вычислительной техники с применением уже изданных математических теорий с опубликованием теории информации К.Шеннона сформировалась прямая связь математики с техникой в информационной сфере.

Попытаемся смоделировать систему мер защиты конфиденциальной информации. Условно представим правовые, организационные и технические меры соответственно в виде трех множеств A, B и C. Множество криптографических мер Cr выделим отдельно. Все множества мер – пересекающиеся (см. рис 1).

Защита данных с помощью шифрования является одним из эффективных решений проблемы безопасности. В целях преодоления противоречия, сложившегося в понимании роли и места криптографии в защите информации, в соответствии с положениями Стратегии национальной безопасности Российской Федерации предлагается ввести в научный технический оборот и нормативные правовые документы Российской Федерации научное и правовое понятие «криптографические меры защиты информации».

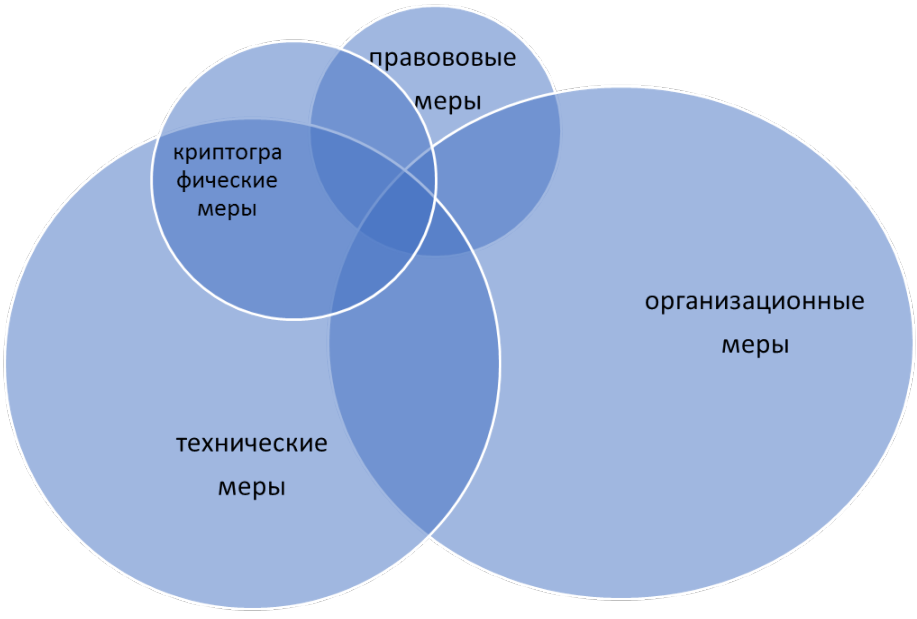

Рисунок 1 – Модель взаимодействия множеств технических, организационных, правовых и криптографических мер защиты информации.

Автором предложена следующая дефиниция термина «криптографические меры защиты информации». Криптографические меры представляют собой совокупность действий, направленных на разработку и/или практическое применение методов и криптографических (шифровальных) средств защиты информации. Криптографические меры защиты информации – это обязательные для исполнения требования и процедуры применения защиты данных с помощью их криптографического преобразования, устанавливаемые в целях защиты информации от актуальных угроз безопасности информации и предотвращения иного ущерба, связанного с уничтожением, изменением (модификацией), блокированием, копированием, предоставлением, распространением персональных данных, а также с иными неправомерными действиями.

Список литературы

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. – М.. Гелиос АРВ, 2002. – 480 с.
2. *Бабаш А.В., Шанкин Г.П.* Криптография / Под редакцией В.П. Шерстюка, ЭЛ. Применко. – М.: СОЛОН-ПРЕСС, 2007. – 512 с.
3. *Бескид П.П., Тагарникова Т.М.* Криптографические методы защиты информации. Ч.1. Основы криптографии. Учебное пособие. – СПб.: изд. РГГМУ, 2010. – 95 с.
4. *Васильева И.Н.* Защита информации: учеб. пособие – СПб.: СПбГИЭУ, 2011. – 162 с.
5. *Вострецова Е.В.* Основы информационной безопасности: учебное поосбие для студентов вузов. – Екатеринбург: Изд-во Урал. ун-та, 2019. –204с.
6. *Голубев Е.А.* Стеганографические технологии новое направление защиты информации // T-Comm. – 2012. – № 6.
7. *Коваленко Ю.И.* Организационно-правовое обеспечение криптографической защиты конфиденциальной информации. – М.: Горячая линия – Телеком, 2019. – 324 с.
8. Криптографическая защита информации: учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с.
9. *Ожегов С.И.* Толковый словарь русского языка [Текст]: 100000 слов, терминов и выражений / под общ. ред. Л. И. Скворцова. – 26-е изд., перераб. – М.: Мир и образование, 2010. – 736 с.
10. Словарь русского языка: в 4-х т. / РАН, Ин-т лингвистич. исследований; под ред. А. П. Евгеньевой. – 4-е изд., стер. – М.: Рус. яз.; Полиграфресурсы, 1999, Т.2: К- О. – 1999. –736 с.
11. Толковый словарь русского языка в 4 томах / Под ред. Д.Н. Ушакова. – М.: Гос. изд-во иностр. и нац. слов, 1938. – Том II. – С.184.

Статья поступила в редакцию 8 сентября 2020 г.
Принята к публикации 21 ноября 2020 г.

Ссылка для цитирования: Метельков А.Н. О криптографических мерах защиты информации при внедрении информационных технологий в решение задач управления в социальных и экономических системах // Национальная безопасность и стратегическое планирование. 2020. № 4(32). С. 68-78. DOI: https://doi.org/10.37468/2307-1400-2020-4-68-78