УДК 316.4
JEL O31, O32, O33

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В РАМКАХ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ: ОСНОВНАЯ ХАРАКТЕРИСТИКА

Ткачева Мария Вячеславовна, канд. экон. наук
Береснев Никита Романович, специалист

Воронежский государственный университет, Университетская пл., 1, Воронеж, Россия, 394018; e-mail: tkachevamv-vsu@yandex.ru; beresnev.2002@mail.ru

Предмет: предметом данного исследования являются информация, представляющая ценность для экономического субъекта, а также средства и методы ее защиты в рамках обеспечения информационной безопасности экономического субъекта. *Цель*: обзор и классификация нормативно закрепленных и предлагаемых различными авторами ключевых характеристик средств и методов защиты информации, представляющей ценность для экономического субъекта, а также оценка основных направлений их применения в рамках обеспечения организацией информационной безопасности как составляющей экономической безопасности организации. *Дизайн исследования*: конструирование классификационной модели известных современной экономической практике средств и методов защиты информации на основе ретроспективного и перспективного анализа применяемых на практике и описанных в нормативной и научной литературе способов обеспечения информационной безопасности и оценки основных направлений их применения. *Результаты*: полученная в ходе проведенного исследования классификационная модель средств и методов защиты информации может служить информационной базой для применения экономическими субъектами тех или иных на практике в целях обеспечения их информационной безопасности как составляющей экономической безопасности организации.

Ключевые слова: информация, информационная безопасность, защита информации, средства и методы защиты информации, механизмы обеспечения информационной безопасности, инструменты и меры обеспечения информационной безопасности, информация ограниченного доступа.

DOI: 10.17308/meps/2078-9017/2024/5/165-177

Введение

Относительно недавно мы все чаще стали сталкиваться со следующими понятиями: «информационный век», «постиндустриальное общество», а также «третья промышленная революция». Данные понятия характеризуют стремительные и поистине глобальные изменения в обществе, в том числе в такой сфере общественных отношений, как «экономика». Связаны они с такими необратимыми процессами, как «компьютеризация», «информатизация» и, как следствие, с возрастанием роли информации и информационных технологий в мире.

Роль информации трудно переоценить. Таким объектом отношений могут выступать как какие-либо общедоступные сведения (например, открытые данные условий контракта, размещенные в открытой части Единой информационной системы государственных закупок), так и та или иная информация, закрытая от общего доступа (такой может выступать информация, содержащая коммерческую тайну юридического лица, или персональные данные гражданина РФ, не давшего согласия на их обработку и предоставление).

С точки зрения бизнеса и экономических отношений, информация также является одним из основных объектов экономического субъекта. Организациям необходимо владеть, пользоваться и учитывать такую общедоступную информацию, как положения из нормативно-правовых актов, с целью избежания и недопущения применения к экономическим субъектам государственных и иных негативных санкций, а также обеспечивать защищенность ограниченной организацией от общего доступа или конфиденциальной информации, к которой может относиться, к примеру, коммерческая тайна, непосредственно являющаяся одним из главных условий получения ими дохода, или налоговая тайна, распространение которой может привести к потере деловой репутации такой организации.

Именно поэтому современные экономические теоретики к традиционно выделяемым факторам производства (труд, земля, капитал, предпринимательские способности) стали относить еще один, не менее важный – «информацию», обладателем которой является тот или иной экономический субъект (то есть имеет право ею распоряжаться на основе положений нормативно-правовых актов или сделок с другими субъектами экономико-правовых отношений).

В современном мире информация играет важнейшую роль не только для сферы бизнеса и экономики в целом, но и для политической, правовой и иных областей деятельности. Именно поэтому данной сфере уделяют особое внимание на всех уровнях российской системы правоотношений.

Согласно положениям Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации», сущность обеспечения информационной безопасности заключается в

- принятии мер по защите информации от несанкционированного доступа к ней, ее модифицирования, уничтожения, предоставления, копирования, распространения и иных неправомерных действий с ней;
- контроле за выполнением функций защиты информации;
- своевременном обнаружении и выявлении вышеперечисленных правонарушений;
- борьбе с такими правонарушениями.

Субъектам, осуществляющим ту или иную экономическую деятельность, стоит обратить внимание на обеспечение информационной безопасности всех вышеперечисленных категорий информации законными средствами и методами защиты.

Основная часть

Проводя обобщенный обзор нормативно закрепленных характеристик средств и методов защиты информации, представляющей ценность для экономического субъекта, можно выделить следующую классификацию средств и методов защиты информации:

- правовые средства и методы защиты информации;
- организационные средства и методы защиты информации;
- технические средства и методы защиты информации.

Однако авторы научной литературы по данной тематике выделяют иную обобщенную классификацию средств и методов защиты информации:

- правовые (законодательные) средства и методы защиты информации;
- организационные (административные) средства и методы защиты информации;
- морально-этические средства и методы защиты информации;
- технические, включающие в себя аппаратные и физические средства и методы защиты информации;
- программные средства и методы защиты информации.

Стоит отметить, что мнения авторов в разрезе классификации инструментов обеспечения информационной безопасности экономического субъекта во многом расходятся, однако они не взаимоисключают другие, а допускают использование всех легальных средств и методов защиты информации в процессе осуществления экономической деятельности. Данная позиция, на наш взгляд, является верной, так как организациям следует использовать все возможные способы для сохранения информации, подлежащей защите, от потенциальных и реальных угроз и опасностей.

Однако организациям следует ранжировать по степени значимости риски и угрозы их информационной безопасности, а также сопоставлять между собой затраты в результате реализации той или иной потенциальной угрозы и затраты на ее предупреждение в целях экономической целесообразности и обоснованности применения мер по обеспечению защиты той

или иной обладаемой ими информации. Некоторые авторы, такие, как О.М. Васильева, Р.С. Хлебников, А.Д. Чесноков, называют данный принцип принципом благоразумности [3; 11]. Так, например, организации не следует применять подобные дорогостоящие меры в отношении информации, за распространение, модифицирование, копирование которой она не несет лишений в виде штрафных санкций от государства и иных субъектов взаимодействия. Однако стоит уделить особое внимание той информации, за модификацию, распространение и иные неправомерные действия в отношении которой организация несет определенные потери (например, данным бухгалтерского учета и отчетности, искажение которых влечет за собой штрафные санкции от органов государственной власти; коммерческой и иной конфиденциальной информации, вследствие распространения которой организация может лишиться ведущего положения на рынке и определенной доли прибыли).

В целях качественного и эффективного обеспечения информационной безопасности организации необходимо создать комплексную систему, выполняющую задачи по защите такого ценного экономического ресурса, как информация [4]. В крупных организациях в целях обеспечения информационной безопасности создаются отдельные информационно-аналитические подразделения, которые занимаются сбором той или иной релевантной или потенциально релевантной информации, имеющей отношение к осуществляемой экономическим субъектом деятельности, ее всесторонним анализом и разработкой перечня потенциальных и реальных угроз и опасностей такому виду экономической безопасности организации. В свою очередь, служба безопасности такого экономического субъекта занимается разработкой, реализацией и контролем над ней мер по ликвидации или минимизации таких угроз и опасностей. Организация информационной безопасности путем создания отдельных структурных подразделений и наделения их особыми полномочиями называется принципом системности [11].

Вернемся к классификации средств и методов защиты информации. Вследствие анализа и синтеза изученной научной и правовой информации по данной теме можно выделить следующую классификацию средств и методов защиты информации (рис. 1). Стоит отметить, что данная классификационная модель не носит исчерпывающий характер и подразумевает под собой наиболее основные и часто применимые на практике средства и методы защиты информации в рамках обеспечения информационной безопасности экономического субъекта.

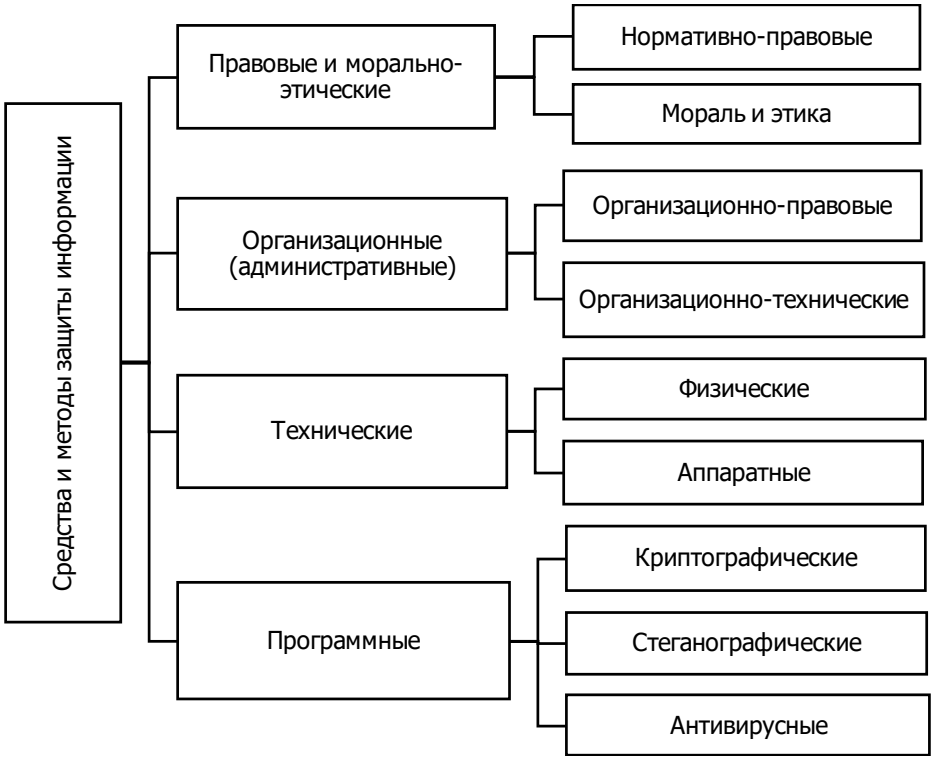

Рис. 1. Классификация средств и методов защиты информации

Представленная на рис. 1 классификационная модель отражает широкий спектр необходимых и возможных для использования экономическими субъектами средств и методов защиты располагаемой ими информации.

В первую очередь в данной модели фигурируют правовые и морально-этические средства и методы, четко разграниченные на две составляющие:

- нормативно-правовые средства и методы защиты информации;
- мораль и этика.

Первая составляющая данной группы носит характер общеобязательных (в рамках обеспечения информационной безопасности) для применения норм. Она представлена нормативно-правовыми актами, исходящими от публичных органов власти (законы, подзаконные акты и др.).

Для обеспечения упорядоченности отношений, непосредственно относящихся к сфере информационного взаимодействия, государство создает нормативно-правовую базу, регулирующую отношения, затрагивающие практически все общество и его деятельность в целом. В Российской Федерации такая нормативно-правовая база, например, широко представлена на федеральном уровне следующими федеральными законами:

- Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» и др.

В соответствии с вышеперечисленными нормативно-правовыми актами, информацию в целом, на наш взгляд, можно разделить на четыре категории (по признаку):

- общедоступная информация;
- информация ограниченного доступа, предоставляемая по соглашению (например, сведения, которыми обладают работники ввиду занимаемой должности);
- информация, подлежащая предоставлению (например, информация, содержащаяся в налоговых декларациях, предоставляемых органам ФНС) и распространению (например, бухгалтерская (финансовая) отчетность – по общему правилу);
- тайная (конфиденциальная) информация.

В процессе обеспечения информационной безопасности экономического субъекта организациям необходимо выполнять положения таких нормативно-правовых актов, а значит, и быть вовремя и в полной мере осведомленными о своих правах и обязанностях, исходящих от государства и иных публично-правовых образований, в рамках информационных правоотношений. Знание прав и обязанностей субъектами таких правоотношений позволит вовремя избежать штрафных санкций и иных видов ответственности как самим экономическим субъектом, так и его должностными лицами вследствие нарушения общеобязательных норм, а также вовремя воспользоваться своими правами в целях достижения наиболее выгодного положения на рынке.

Так, например, организациям запрещено распространять и предоставлять без специального разрешения персональные данные трудоустроенных в данных экономических субъектах работников, исходя из положений Федерального закона №152-ФЗ «О персональных данных» и иных сопутствующих данному закону нормативно-правовых источников. За нарушение данного положения организациями и их должностными лицами предусмотрена административная ответственность. Также следует привести в пример ситуацию, отражающую использование экономическими субъектами своих нормативно-закрепленных прав. Так, организации, разработавшие тот или иной промышленный образец или полезную модель, могут установить, в соответствии с нормативными актами, охраняющими интеллектуальную собственность, право на интеллектуальную собственность, тем самым заняв исключительное положение на рынке в целях достижения ими основной цели деятельности.

Вторая составляющая данной группы подразумевает наличие корпоративной культуры и сложившихся в обществе морально-этических норм, выражающихся в соблюдении сотрудниками данной организации правил

пользования и получения той или иной корпоративной информации. Кроме того, данная группа средств и методов защиты информации подразумевает общественное порицание лица, нарушившего такие правила, а также потерю им авторитета и доверия у окружающих. Такие средства и методы защиты информации предполагают наличие и утверждение в организации Кодекса морально-этических норм и профессионального поведения, разработанного, как показывает практика, какой-либо наднациональной структурой (например, «Кодекса профессионального поведения», разработанного Ассоциацией вычислительной техники [8]).

Во вторую очередь в представленной на рис. 1 классификационной модели фигурируют группа административных (организационных) средств и методов защиты информации, представленная:

- организационно-правовыми средствами и методами;
- организационно-техническими средствами и методами.

Первая составляющая данной группы характеризуется разработкой экономическим субъектом в лице тех, кто ответственные за корпоративное управление, или собственников локальных нормативно-правовых актов, регламентирующих сотрудникам правила получения, использования и обращения с информацией, подлежащей защите экономическим субъектом. Помимо того, такие акты содержат нормы, содержащие дисциплинарную ответственность за нарушение таковых. Такие средства и методы защиты информации могут быть представлены определенными должностными инструкциями, инструкциями по использованию средств и методов защиты информации, регламентацией разграничения доступа сотрудников (к информационным системам и ее частям, на определенные территории экономического субъекта и отдельные помещения). Стоит отметить, что данные локальные нормативно-правовые акты организации разрабатываются на основе данных, полученных вследствие предварительной оценки и анализа потенциальных и реальных угроз информационной безопасности организации и неразрывно связаны с организационно-техническими средствами и методами защиты информации, в основе своей зиждясь на таких ключевых понятиях информационной безопасности, как «аутентификация», «идентификация», «авторизация» и «разграничение доступа».

Что касается второй составляющей данной группы средств и методов защиты информации, то она представлена непосредственно мероприятиями по выполнению и реализации положений вышеупомянутых локальных нормативно-правовых актов. Так, в утвержденном организацией регламенте разграничения доступа к информации может быть дан перечень лиц или должностей, которые имеют и не имеют различный набор прав доступа к той или иной информации, обладателем которой является экономический субъект. А посредством реализации организационно-технических мер осуществляется предоставление или непредоставление вышеперечисленным таких прав, например, на основе тех или иных регламентированных руко-

водством действий администраторов с информационными системами. В рамках осуществления таких организационно-технических мер обеспечиваются свойства и принципы информационной безопасности, а также выполняется контроль за действиями пользователей корпоративной информации.

В целом данная группа средств и методов защиты информации нацелена на снижение риска и минимизацию угрозы утечки информации по тем или иным возможным каналам связи. Она подразумевает под собой не только закрепление правил функционирования с информацией экономического субъекта, а также ограничение и предоставление доступа к ней, но и организацию работы с носителем сведений, управление персоналом и проведение с ним работы с целью предупреждения нарушений [5].

В третью очередь в представленной на рис. 1 классификационной модели также наличествуют технические средства и методы защиты информации, подразделяющиеся на:

- физические средства и методы защиты информации;
- аппаратные средства и методы защиты информации.

Первая составляющая данной группы представлена реальными преградами и заграждениями, позволяющими ограничить доступ к информации, обладателем которой является экономический субъект. Она включает такие мероприятия, как установление турникетов, контрольно-пропускной системы в организации, которые функционируют обособленно от информационных систем. Кроме того, к такой составляющей относятся железные двери с замками, шкафы, сейфы, сигнализации, противопожарные системы и др. В основе своей данные средства и методы защиты информации можно разделить на:

- предупреждающие угрозы;
- обнаруживающие угрозы;
- ликвидирующие угрозы [1].

Вторая же составляющая такой группы включает в себя такие средства и методы защиты информации, которые являются дополнением к уже имеющимся информационным системам. К таким средствам и методам можно отнести генераторы помех, базы данных для хранения реквизитов защиты информационных систем от несанкционированного доступа (паролей, специальных ключей и прочих идентификаторов) и др. [1].

В четвертую очередь, в соответствии с представленной на рис. 1 классификационной моделью средств и методов защиты информации, необходимо рассмотреть программную составляющую, включающую в себя:

- криптографические средства и методы защиты информации;
- стеганографические средства и методы защиты информации.

Данная группа предназначена для обеспечения важнейших свойств информационной безопасности: целостности, конфиденциальности и доступности.

Криптографические средства и методы защиты информации представляют собой способы шифрования информации, которыми пользуется, а также может воспользоваться экономический субъект, в целях исключения нарушения целостности и конфиденциальности информации. К таким средствам и методам относят различные алгоритмы шифрования информации, а также функции хэширования и схемы электронно-цифровой подписи [2].

Таким образом, обладатель информации передает зашифрованную информацию получателю, обладающему ключом к ее расшифрованию. Злоумышленник, не обладающий таким ключом, не может дешифровать такую информацию, а также видоизменить ее в тайне от получателя, однако если получатель не обладает большим объемом временных и интеллектуальных ресурсов. Примером таких средств и методов защиты информации могут послужить различные исторически известные нам шифры: шифры Виженера, шифр Плейфера, шифр «Два квадрата» и др., а также специальные шифровые машины. Однако на данный момент вышеперечисленные средства и методы устарели и используются другие, соответствующие современным технологиям и достижениям информационной науки и практики – специальные программы шифрования данных.

Стеганографические средства и методы защиты информации представляют собой способы сокрытия самого факта передачи какой-либо информации от ее обладателя к получателю. Они основаны на преобразовании исходной информации так, чтобы нарушитель не понял, что была осуществлена передача какой-либо ценной информации. Такие средства и методы основаны на применении различных программ преобразования информации и ее передачи по незащищенным каналам связи [9].

Однако применение и той, и другой составляющих данной группы обеспечивает большую уверенность в том, что нарушитель не сможет получить доступ к передаваемой информации и нарушить ее целостность.

Антивирусные средства и методы защиты информации предполагают обеспечение защищенности информационных систем и хранящейся на них информации от программ-вирусов, способных своими несанкционированными действиями нарушить такие свойства информационной безопасности, как «конфиденциальность», «целостность» и «доступность», посредством деятельности вредоносных ПО. Лучший способ защитить информационные системы от подобных угроз – это регулярно использовать антивирусные программы, которые широко распространены на российском рынке.

Экономическому субъекту в целях обеспечения информационной безопасности необходимо применять средства и методы защиты информации разных видов (в соответствии с рис. 1) для получения максимально возможного эффекта. Однако при осуществлении такой деятельности стоит учитывать следующие принципы: принцип системности, принцип необходимости, а также принцип благоразумности.

Заключение

Таким образом, мы выяснили, что информация, представляющая ценность для экономического субъекта, должна обеспечиваться необходимыми средствами и методами по ее защите, исходя из стремления организации к стабильному и эффективному функционированию в целях достижения ею основных целей деятельности и состоянию экономической безопасности в целом. Кроме того, стоит отметить, что средств и методов защиты информации представляется огромное множество, и организации следует системно и согласованно организовывать соответствующие меры по такой защите, если затраты на предупреждение потенциальных и реальных угроз и опасностей ее информационной безопасности не превышают затраты по их реализации.

Обеспечение информационной безопасности – приоритетное направление деятельности экономического субъекта ввиду усилившейся в последнее время роли такого ресурса, как информация, во всех сферах общественной жизни.

В данной работе мы провели обзор и классифицировали нормативно закрепленные и предлагаемые различными авторами ключевые характеристики средств и методов защиты информации, представляющей ценность для экономического субъекта, а также оценили основные направления их применения в рамках обеспечения организацией информационной безопасности как составляющей, в целом, экономической.

Полученная в ходе проведенного исследования классификационная модель средств и методов защиты информации, представленная на рис. 1, а также ее описание в данной работе, может служить информационной базой для применения экономическими субъектами тех или иных мероприятий на практике в целях обеспечения их информационной безопасности как составляющей экономической безопасности организации.

Важно помнить, что каждая составляющая экономической безопасности организации (финансовая, кадровая, технико-технологическая, налоговая, информационная и др.) взаимосвязана и взаимообусловлена. Отдавая приоритет одной из них и не заботясь о другой, экономический субъект рискует не получить должного эффекта от своей деятельности, добиться ее целей и не достичь состояния защищенности.

Список источников

1. Аль-Аммори А., Дяченко П.В., Клочан А.Е., Бакун Е.В., Козелецкая И.К. Методы и средства защиты информации // *The Scientific Heritage,* 2020, no. 51-1 (51), с. 32-42. Доступно: https://cyberleninka.ru/article/n/metody-i-sredstva-zaschity-informatsii.

2. Баданов А.Г. Информационная безопасность ОУ // *Вестник Марийского государственного университета*, 2010, no. 5, с. 261-267. Доступно: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-ou.

3. Васильева О.М., Хлебников Р.С. Информационная безопасность в организации // *Экономика и качество систем связи,* 2018, no. 4 (10), с. 46-49. Доступно: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-organizatsii.

4. Грачева Е.А. Информационная безопасность // *The Newman in Foreign Policy,* 2020, no. 54 (98), том 3, с. 57-59. Доступно: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-5.

5. Домбровская Л.А., Васютина Т.Л. Организационные средства защиты информации как элемент общей системы защиты информации // *European science*, 2016, no. 11 (21), с. 21-25. Доступно: https://cyberleninka.ru/article/n/organizatsionnye-sredstva-zaschity-informatsii-kak – element-obschey-sistemy-zaschity-informatsii.

6. Качаев А.Ю., Хантыев Х.В., Эренженов А.М. Информационная безопасность в компании // *Вестник науки,* 2021, no. 7 (40), т. 1, с. 69-74. Доступно: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-kompanii.

7. Королев М. Информационная безопасность предприятия // Вестник Института экономики Российской академии наук, 2010, no. 4, с. 187-191. Доступно: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-predpriyatiya.

8. Полянская О.Ю. Кодексы профессиональной этики в сфере информационной безопасности // *Безопасность информационных технологий*, 2009, no. 3 (т. 16), с. 119-124. Доступно: https://studylib.ru/doc/2152084/o.-yu.-polyanskaya-kodeksy-professional._noj-etiki-v.

9. Соколова К.А., Шаров Д.А. Стеганографические средства защиты информации // *Актуальные проблемы авиации и космонавтики*, 2018, no. 14 (т. 3), с. 886-888. Доступно: https://cyberlenink.a.ru/article/n/stegano graficheskie-sredstva-zaschity-informatsii.

10. Сорокина М.Ю. Информационная безопасность vs информационные технологии // *Научные труды Вольного экономического общества России*, 2014, т. 186, с. 566-571. Доступно: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-vs-informatsionnye – tehnologii.

11. Чесноков А.Д. Информационная безопасность // *StudNet,* 2022, том 5, no. 1 (54), с. 478-489. Доступно: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-6.

12. Устинов Д. Сущность информационной безопасности // *Международный журнал гуманитарных и естественных наук*, 2017, no. 12, с. 146-151. Доступно: https://cyberleninka.ru/article/n/suschnost-informatsionnoy-bezopasnosti.

MEANS AND METHODS OF INFORMATION PROTECTION WITHIN THE FRAMEWORK OF ENSURING THE ECONOMIC SECURITY OF THE ORGANIZATION: THE MAIN CHARACTERISTIC

Tkacheva Mariya Vyacheslavovna, Cand. Sci. (Econ.)
Beresnev Nikita Romanovich, B.A. + M.A.

Voronezh State University, University Sq., 1, Voronezh, Russia, 394018; e-mail: tkachevamv-vsu@yandex.ru; beresnev.2002@mail.ru

Importance: the subject of this study is information of value to an economic entity, as well as means and methods of its protection within the framework of ensuring information security of an economic entity. *Purpose*: a review and classification of the key characteristics of the means and methods of protecting information of value to an economic entity, which are normatively fixed and proposed by various authors, as well as an assessment of the main directions of their application within the framework of ensuring information security by the organization as a component of the economic security of the organization. *Research design:* designing a classification model of information security tools and methods known to modern economic practice based on a retrospective and prospective analysis of the methods used in practice and described in the regulatory and scientific literature to ensure information security and assess the main directions of their application. *Results*: the classification model of information protection tools and methods obtained in the course of the study can serve as an information base for the use of certain economic entities in practice in order to ensure their information security as a component of the economic security of the organization.

Keywords: information, information security, information protection, means and methods of information protection, information security mechanisms, tools and measures to ensure information security, restricted access information.

References

1. Al'-Ammori A., Djachenko P.V., Klochan A.E., Bakun E.V., Kozeleckaja I.K. Metody i sredstva zashhity informacii. *The Scientific Heritage*, 2020, no. 51-1 (51), pp. 32-42. Available at: https://cyberleninka.ru /article/n/metody-i-sredstva-zaschity-informatsii. (In Russ.)

2. Badanov A.G. Informacionnaja bezopasnost' OU. *Vestnik Marijskogo gosudarstvennogo universiteta*, 2010, no. 5, pp. 261-267. Available at: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-ou. (In Russ.)

3. Vasil'eva O.M., Hlebnikov R.S. Informacionnaja bezopasnost' v organizacii. *Jekonomika i kachestvo sistem*

svjazi, 2018, no. 4 (10), s. 46-49. Available at: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-organizatsii. (In Russ.)

4. Gracheva E.A. Informacionnaja bezopasnost'. *The Newman in Foreign Policy*, 2020, no. 54 (98), tom 3, pp. 57-59. Available at: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-5. (In Russ.)

5. Dombrovskaja L.A., Vasjutina T.L. Organizacionnye sredstva zashhity informacii kak jelement obshhej sistemy zashhity informacii. *European science*, 2016, no. 11 (21), pp. 21-25. Available at: https://cyberleninka.ru/article/n/organizatsionnye-sredstva-zaschity-informatsii-kak – element-obschey-sistemy-zaschity-informatsii. (In Russ.)

6. Kachaev A.Ju., Hantyev H.V., Jerenzhenov A.M. Informacionnaja bezopasnost' v kompanii. *Vestnik nauki,* 2021, no. 7 (40), tom 1, pp. 69-74. Available at: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-kompanii. (In Russ.)

7. Korolev M. Informacionnaja bezopasnost' predprijatija. *Vestnik Instituta jekonomiki Rossijskoj akademii nauk*, 2010, no. 4, pp. 187-191. Available at: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-predpriyatiya. (In Russ.)

8. Poljanskaja O.Ju. Kodeksy professional'noj jetiki v sfere informacionnoj bezopasnosti. *Bezopasnost' informacionnyh tehnologij*, 2009, no. 3 (tom 16), pp. 119-124. Available at: https://studylib.ru/doc/2152084/o.-yu.-polyanskaya-kodeksy-professional._noj-e-tiki-v. (In Russ.)

9. Sokolova K.A., Sharov D.A. Steganograficheskie sredstva zashhity informacii. *Aktual'nye problemy aviacii i kosmonavtiki,* 2018, no. 14 (tom 3), pp. 886-888. Available at: https://cyberlenink.a.ru/article/n/stegano graficheskie-sredstva-zaschity-informatsii. (In Russ.)

10. Sorokina M.Ju. Informacionnaja bezopasnost' vs informacionnye tehnologii. *Nauchnye trudy Vol'nogo jekonomicheskogo obshhestva Rossii*, 2014, tom 186, pp. 566-571. Available at: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-vs-informatsionnye – tehnologii. (In Russ.)

11. Chesnokov A.D. Informacionnaja bezopasnost'. *StudNet*, 2022, tom 5, no. 1 (54), pp. 478-489. Available at: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-6. (In Russ.)

12. Ustinov D. Sushhnost' informacionnoj bezopasnosti. *Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk*, 2017, no. 12, pp. 146-151. Available at: https://cyberleninka.ru/article/n/suschnost-informatsionnoy-bezopasnosti. (In Russ.)