Общая теория криминалистики

КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Марина Владимировна ЖИЖИНА,
профессор кафедры криминалистики Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук
kriminalistmsal@list.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Аннотация. *Обеспечение информационной безопасности — сегодня приоритетная задача в международной и национальной политике нашего государства, обязательное условие существования и нормального развития государства, общества, личности и бизнеса. Криминалистика как прикладная наука, остро реагирующая на все потребности практики, связанные не только с борьбой с преступностью, но и с иными вызовами современности, может и должна также содействовать своими методами и средствами решению проблем, связанных с обеспечением безопасности, в том числе и информационной. В статье рассматриваются возможности применения криминалистики в исследуемом аспекте.*

Ключевые слова: *информационная безопасность, криминалистическое обеспечение, предпринимательская деятельность, бизнес-юрист, риски, защита.*

DOI: 10.17803/2311-5998.2019.55.3.029-035

M. V. ZHIZHINA,
Professor of the Criminalistics Department of the Kutafin Moscow State Law University (MSAL), doctor of juridical sciences
kriminalistmsal@list.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, 9

CRIMINALISTIC SECURITY OF INFORMATION SECURITY OF THE ENTERPRISE

Abstract. *Ensuring information security today is a priority task in the international and national policy of our state, an indispensable condition for the existence and normal development of the state, society, individual and business. Criminalistics as an applied science that is acutely responsive to all the needs of practice, connected not only with the fight against crime, but also with other challenges of our time, can and should also assist with its methods and means in solving problems related to information security. This article discusses the possibilities of using criminalistics in the aspect under study.*

Keywords: *information security, criminalistics software, business, business lawyer, risks, protection.*

Понятие «информационная безопасность» — многоаспектное и в зависимости от его применения может быть рассмотрено с нескольких сторон. В самом общем понимании информационная безопасность — это состояние защищенности информации, которое обеспечивает условия формирования и функционирования информационной среды. Под информационной средой понимается «сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации»[1].

Обеспечение информационной безопасности является обязательным условием нормального развития личности, общества и государства и в настоящее время определено стратегическим приоритетным направлением политики Российской Федерации[2]. Современная Доктрина информационной безопасности[3] выделяет в том числе угрозы интересам коммерческих организаций и меры по их предупреждению. На законодательном уровне провозглашается, что обеспечение информационной безопасности осуществляется в виде организационно-правовой защиты личности, бизнеса и государственных интересов при взаимодействии в условиях цифровой экономики[4]. При этом выделяется отдельная группа — хозяйствующие субъекты, сфера деятельности которых сопряжена с созданием массовой информации, информационных продуктов, использованием информационных ресурсов, предоставляющих информационные услуги, в том числе СМИ, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, организации, осуществляющие деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности и др.[5] Они являются участниками общенациональной системы обеспечения информационной безопасности и дополнительно обязаны осуществлять предписанные законом меры. Иные хозяйствующие субъекты, не включенные в эту систему, естественно, должны соблюдать законодательство РФ в части обеспечения защиты информации.

Однако помимо публичных интересов, регламентируемых и контролируемых на государственном уровне, каждое предприятие имеет и свой частный интерес в сфере защиты информации, так как только в случае стабильной защиты информационной сферы создаются условия для успешной деятельности и развития. Поэтому проблема создания наиболее эффективной системы для обеспечения

---

[1] Федеральный закон от 04.07.1996 № 85-ФЗ «Об участии в международном информационном обмене» (утратил силу). Ст. 2 // Российская газета. 1996. № 129.

[2] Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. № 1 (ч. II). Ст. 212 ; постановление Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации “Информационное общество (2011 — 2020 годы)”» // СЗ РФ. 2014. № 18 (ч. II). Ст. 2159.

[3] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

[4] Распоряжение Правительства РФ от 28.07.2017 № 1632-р // URL: http://static.government.ru /media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 30.05.2017).

[5] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

информационной безопасности со всей актуальностью стоит сегодня перед каждым предприятием независимо от его вида деятельности, формы собственности и размера уставного капитала.

Вопросы создания и функционирования системы информационной безопасности предприятия являются междисциплинарными, относящимися к ведению наук IT-сферы, юридических, экономических. Мы исследуем возможности применения такой юридической науки, как криминалистика, в данном аспекте. При этом в качестве субъекта обеспечения информационной безопасности мы будем рассматривать юриста, сопровождающего предпринимательскую деятельность, концентрируясь на знаниях и навыках, которыми он должен обладать в силу своей компетенции.

Для поставленных нами целей необходимо проанализировать содержательную сторону и определить базовые понятия, относящиеся к рассматриваемой проблематике.

Говоря об информационном поле предприятия, необходимо отметить, что информация пронизывает все сферы его деятельности. Под информацией понимаются «сведения (сообщения, данные) независимо от формы их представления»[6]. Любой хозяйствующий субъект осуществляет сбор, формирование, распространение, использование информации, создает информационную систему, в которой циркулирует служебная, управляющая, аналитическая, деловая информация на всех этапах его жизненного цикла (генерация, хранение, обработка, передача, уничтожение).

Информация может быть открытой и подлежащей защите в соответствии с требованиями, изложенными в правовых документах или устанавливаемыми собственником информации; последним может быть государство, юридическое или физическое лицо. Защищенность информации достигается обеспечением совокупности свойств информационной безопасности: а) конфиденциальности, т.е. требования не передавать информацию третьим лицам без согласия ее обладателя; б) доступности, т.е. беспрепятственного доступа к информации субъектов, имеющих на это право; в) целостности, т.е. ее неизменности или изменения только уполномоченными на это субъектами[7].

Приоритетность свойств информационной безопасности определяется их значимостью для интересов и целей организации. При этом носителями защищаемой информации могут быть:

— материальные объекты в любых их субстанциальных формах, например, научно-техническая, технологическая, производственная, финансово-экономическая или подобная информация, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, составляющая коммерческую тайну;

[6] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Ст. 2 // Российская газета. 2006. № 165.

[7] Защита информации. Основные термины и определения. ГОСТ Р 50922-2006. М., Стандартинформ, 2008.

— физические лица — информация «хранится» в памяти, извлекается, интерпретируется особенным способом в результате мыслительной деятельности человека и доводится устным или иным способом до потребителя;
— документы в широком смысле — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Нарушение информационной безопасности организации — это случайное или преднамеренное неправомерное действие физического лица в отношении активов организации, следствием которого является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия в виде ущерба или вреда для организации[8].

Защиту информации законодатель определяет как деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Такими воздействиями могут быть: неправомерный доступ, уничтожение, модифицирование, блокирование, копирование, предоставление, распространение и иные неправомерные действия[9], которые могут быть как случайного, так и умышленного характера. Учитывая гиперактивное развитие информационных технологий, можно сделать вывод о тенденции к росту количества киберугроз.

Система информационной защиты предполагает комплекс организационных и технических мер. Организационные меры заключаются в создании формальных процедур и правил работы с защищаемой информацией, информационными сервисами и средствами защиты; технические — включают в себя мероприятия по компьютерной безопасности, безопасному программному, аппаратному и коммуникационному обеспечению. Кроме того, на предприятиях должна функционировать система менеджмента информационной безопасности, оценивающая бизнес-риски для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

Субъектами, непосредственно обеспечивающими реализацию системы мер по защите информации, являются сотрудники службы информационной безопасности предприятия (специалисты IT-сферы, службы безопасности). Однако создание полноценной системы информационной защиты предприятия предполагает ее комплексный характер с привлечением сотрудников всех подразделений, в том числе, конечно, и юристов.

Учитывая четко очерченные рамки нашего исследования предметной деятельностью бизнес-юриста, следует определить его роль в обеспечении информационной безопасности предприятия.

Условно можно выделить три основных направления в деятельности корпоративного юриста:
— обеспечение внутренней деятельности предприятия, заключающееся в разработке документов, регулирующих гражданские, трудовые, акционерные правоотношения и т.п., консультировании сотрудников и пр.;

---

[8] ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М. : Стандартинформ, 2009.

[9] Федеральный закон «Об информации, информационных технологиях и о защите информации». Ст. 16.

— обеспечение основной (хозяйственной) деятельности предприятия, состоящее в разработке документов, регулирующих гражданско-правовые и иные отношения с контрагентами, ведении переговорных процессов и пр.;
— обеспечение представительских функций предприятия в органах государственной власти, судебных, налоговых органах и т.п. и внешних организациях.

Информация, попадающая в сферу деятельности юриста по всем трем направлениям, может быть конфиденциальной, в отношении которой следует использовать режим защиты. Юрист предприятия может быть сам носителем защищаемой информации, создателем иных носителей или их потребителем.

Соответствующим образом современный бизнес-юрист должен подходить к выполнению своих обязанностей с учетом соблюдения требований информационной безопасности:

1) как носитель конфиденциальной информации знать и неукоснительно соблюдать все правила, приемы и средства защиты при создании / преобразовании / потреблении информации, в том числе методики, технологии, средства создания автоматизированных и информационных систем автоматизации бизнес-процессов, риски и угрозы безопасности при использовании различных информационных технологий, средства обеспечения информационной безопасности;
2) юридически грамотно оформить систему информационной безопасности предприятия путем разработки соответствующих актов локального регулирования и иной документации, сопровождающей создание и деятельность предприятия, в том числе в части внутренних нормативных и распорядительных документов по вопросам защиты информации, обеспечения конфиденциальности коммерческой (банковской) тайны, защиты персональных данных, соглашений об электронном документообороте и т.д.;
3) реализовывать меры по защите создаваемых им носителей информации — документов. При этом документирование может осуществляться традиционным способом на бумажном носителе или в электронной форме в случаях и порядке, предусмотренном законодательством РФ.

Законодатель ставит знак равенства между компьютерной и информационной безопасностью, поэтому из его поля зрения совершенно выпадает важнейший носитель информации — документ на бумажном носителе, с точки зрения его защиты. Тем не менее нормальное функционирование любого предприятия неразрывно связано именно с бумажным документооборотом, содержащим в том числе конфиденциальную информацию. Кроме того, как показывает анализ судебной практики рассмотрения хозяйственных споров, фальсификация реквизитов традиционного документа сопутствует практически каждому второму делу. В связи с этим вопросы защиты традиционного документа на бумажном носителе не менее важны, чем защита информации на цифровых носителях.

Таким образом, вышеперечисленные меры и мероприятия образуют систему *юридического обеспечения информационной безопасности предприятия,* куда входят комплекс знаний из различных отраслей права (гражданского, предпринимательского, информационного, уголовного и др.) и криминалистики.

Криминалистика давно перестала быть чистой наукой о расследовании преступлений, как в свое время определил ее основатель Ганс Гросс. Многие ученые

раскрывали и рассматривали возможности применения криминалистики в различных правовых сферах: применительно к деятельности суда, рассматривающего как уголовные, так и гражданские и арбитражные дела[10], к деятельности адвокатуры[11] и нотариата[12]. Более того, развитие науки вывело ее использование за рамки непосредственно судопроизводственной сферы. Ее средства и методы оказались востребованными в областях жизни и деятельности, далеких от отправления правосудия.

Современная криминалистика представляет собой развитую область знаний, располагающую столь огромным арсеналом технических, тактических и методических средств расследования преступлений, что на ее базе могут формироваться теории и учения их применения в судебной и вообще юридической практике, а также в деятельности, находящейся вне сферы практической юриспруденции. Остро востребованными становятся основы применения методов и средств криминалистики, функция которых чисто профилактическая. Их целью является оказание помощи в соблюдении законных требований в различных судебных и несудебных областях общественных отношений, в том числе безопасности.

В настоящее время в науке криминалистики сформировалась и получила развитие теория криминалистического обеспечения безопасности предпринимательской деятельности[13], составной частью которой является криминалистическое обеспечение информационной безопасности. В нее, в частности, входят вопросы, касающиеся:

а) защиты коммуникаций, средств обработки информации, а также выявления, предупреждения и пресечения посягательств в сфере информации, составляющей служебную и коммерческую тайну, от утечки по техническим каналам;

б) защиты данных на бумажных носителях — средства и технологии защиты реквизитов документов от подделки (подписи, печати, бланка и др.) и пути их совершенствования.

---

[10] *Жижина М. В.* Теория и практика применения современной криминалистики в цивилистическом процессе : дис. … д-ра юрид. наук. М., 2017.

[11] См., например: *Игнатов Д. С.* Криминалистические основы деятельности адвоката-защитника по сбору доказательств и представлению их суду : дис. … канд. юрид. наук. Ижевск, 2004 ; *Кручинина Н. В.* Криминалистика — важный элемент в образовании будущих адвокатов // Вестник Университета имени О.Е. Кутафина (МГЮА). 2017. № 12 (40). С. 150—158.

[12] См., например: *Антюшина В. И.* Криминалистические средства и методы в нотариальной деятельности : автореф. дис. … канд. юрид. наук. Ижевск, 2004.

[13] Криминалистическое обеспечение безопасности предпринимательской деятельности : научно-практическое пособие / М. В. Жижина, Я. В. Комиссарова, О. Н. Васильева [и др.]. М. : Проспект, 2018.

БИБЛИОГРАФИЯ

1. *Антюшина В. И.* Криминалистические средства и методы в нотариальной деятельности : автореф. дис. … канд. юрид. наук. — Ижевск, 2004. — 23 с.
2. *Жижина М. В.* Теория и практика применения современной криминалистики в цивилистическом процессе : дис. … д-ра юрид. наук. — М., 2017. — 538 с.
3. *Игнатов Д. С.* Криминалистические основы деятельности адвоката-защитника по сбору доказательств и представлению их суду : дис. … канд. юрид. наук. — Ижевск, 2004. — 197 с.
4. Криминалистическое обеспечение безопасности предпринимательской деятельности : научно-практич. пособие / М. В. Жижина, Я. В. Комиссарова, О. Н. Васильева [и др.]. — М. : Проспект, 2018. — 192 с.
5. *Кручинина Н. В.* Криминалистика — важный элемент в образовании будущих адвокатов // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2017. — № 12 (40). С. 150—158.