

*Поздняков Владислав Александрович
студент 3 курса магистратуры
Университет Прокуратуры РФ
Россия, г. Москва
e-mail: vlad-pozdnyakov@inbox.ru*

*Научный руководитель: Колесов Михаил Владимирович
старший советник юстиции, кандидат юридических наук
Университет Прокуратуры РФ
Россия, г. Москва*

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ И УЧРЕЖДЕНИЯХ ПРОКУРАТУРЫ РФ

Аннотация: В статье обсуждаются некоторые вопросы правового регулирования информационной безопасности в органах и учреждениях прокуратуры РФ. Автор рассматривает понятие «информационная безопасность», а также основные ведомственные нормативно-правовые документы в сфере информационной безопасности в органах и учреждениях прокуратуры РФ.

Ключевые слова: прокуратура, информационная безопасность, информация, нормативно-правовой акт, защита информации.

*Vladislav Pozdnyakov
3rd year master student
University of the Prosecutor's Office of the Russian Federation
Russia, Moscow*

*Scientific adviser: Kolesov Mikhail Vladimirovich
senior counselor of justice, candidate of legal sciences
University of the Prosecutor's Office of the Russian Federation
Russia, Moscow*

LEGAL REGULATION OF INFORMATION SECURITY IN THE BODIES AND INSTITUTIONS OF THE PROSECUTOR'S OFFICE OF THE RUSSIAN FEDERATION

Abstract: The article discusses some issues of legal regulation of information security in the bodies and institutions of the Prosecutor's Office of the Russian Federation. The author examines the concept of "information security", as well as the main departmental regulatory documents in the field of information security in the bodies and institutions of the prosecutor's office of the Russian Federation.

Key words: prosecutor's office, information security, information, normative legal act, information protection.

Вопрос информационной безопасности её организация и обеспечения является приоритетным направлением деятельности государства и органов прокуратуры РФ в связи с развитием информационно-коммуникационных технологий и наиболее актуальным вопросом в сфере правового регулирования.

На основании доклада, подготовленного управлением правовой статистики и информационных технологий Генеральной прокуратуры РФ на тему «Состояние преступности в России» за январь-декабрь 2020 г., за последние пять лет число «киберпреступлений» увеличилось более чем в 11 раз, а удельный вес в структуре преступности возрос с 1,8 % до 25 %. На деяния, совершенные с использованием информационно телекоммуникационных технологий или в сфере компьютерной информации, по-прежнему приходится одно из четырех регистрируемых в текущем году преступлений (+73,4 %, 510,4 тыс.). Большинство «киберпреступлений» совершается с использованием сети «Интернет» (300,3 тыс.) или при помощи средств мобильной связи (218,7 тыс.) [1, с. 6].

Важной составляющей обеспечения информационной безопасности является правовое обеспечение, которое связано с необходимостью правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации.

В рамках рассмотрения феномена правового регулирования информационной безопасности в органах прокуратуры РФ необходимо раскрыть понятие «информационная безопасность». В научной литературе термин «информационная безопасность» является дискуссионным предметом и понимается как в «узком» так и в «широком» смысле. В «узком» смысле информационная безопасность понимается как набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных в компьютерных сетях.

Данный подход разделяют ряд исследователей такие как А.А. Малюк, С.В. Пазизин, Н.С. Погожин которые отмечают, что «информационная безопасность» - состояние защищённости информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности (уничтожения, искажения) или несанкционированного использования» [2]. В.Н. Ясенев определяет информационную безопасность как «защиту информации от внесения в неё изменений неуполномоченными лицами; сохранность ценных данных; надёжность работы компьютера; сохранение тайны переписки в электронной связи» [3]. В.Ю. Гайкович и Д.В. Ершов в тоже время отмечают, что безопасность информации - «это защищённость информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования» [4]. Более широкий подход к определению информационной безопасности который основывается на том, что информационная безопасность - это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства. находит свое отражение во взглядах Ю. Н. Лопатина, В.А. Мазурова и В. В. Невинского.

В частности, Ю.Н. Лопатин отмечал, что формально информационная безопасность — это состояние защищенности основных сфер жизнедеятельности по отношению к опасным информационным воздействиям [5]. У В.А. Мазурова и В. В. Невинского информационная безопасность - состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внешних и внутренних угроз, обеспечивающее ее формирование, использование и развитие [6].

Официальное закрепление понятие «информационная безопасность» получил в соответствии с Указом Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» и раскрывается как состояние защищенности личности, общества и государства

от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Анализируя данные позиции в рамках технико-технологического подхода, можно выделить приоритетный объект защиты информационной безопасности - информацию и информационно-коммуникационная инфраструктуры. При этом под информационно-коммуникационной инфраструктурой предполагается совокупность организационных структур, аппаратного и программного обеспечения для хранения информации, обработки и передачи информации [7]. Также необходимо отметить, что общий элемент большинства определений — это «состояние защищенности» и данное явление является закономерным, поскольку традиционно находит свое отражение в понимании такой категории как «безопасность». Являясь частью национальной безопасности, информационная безопасность органов прокуратуры РФ регламентируется в первую очередь Конституцией РФ, в которой отражены основные концептуальные идеи обеспечения информационной безопасности - «тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений», «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом», «свобода массовой информации». Федеральным законом «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27 июля 2006 г., в котором раскрывается такое понятие как «информация», отражены вопросы, связанные с реализацией правомочий на создание и трансляцию данных, запрещенных к доступа широкому кругу лиц, а также на реализацию охраны этих данных, в частности и в структуре прокуратуры РФ. Вместе с тем необходимо отметить, что в данном законе не отражено такое понятие как «информационная безопасность», что является существенным пробелом в законодательстве.

Указом Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации», который определяет, что при её реализации особое внимание должно уделяться обеспечению информационной безопасности с учетом стратегических национальных приоритетов. При этом должны быть приняты меры для повышения защищенности граждан и общества от деструктивного информационного воздействия со стороны экстремистских и террористических организаций, иностранных специальных служб и пропагандистских структур. А также отмечается, что Российская Федерация будет содействовать формированию системы международной информационной безопасности. Указом Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы», в соответствии с которым информационные и коммуникационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

К ведомственным нормативно-правовым актам, действующим в органах прокуратуры РФ в сфере информационной безопасности, можно отнести:

1) Федеральный Закон от 17.01.1992 № 2202–1 «О прокуратуре Российской Федерации»;

2) Приказ Генеральной прокуратуры Российской Федерации от 27.11.2019 № 830 «Об утверждении Концепции безопасности органов и организаций прокуратуры Российской Федерации» [8], который утверждает концепцию безопасности органов и организаций прокуратуры. Данный приказ определяет цели, задачи и принципы обеспечения безопасности в целом. Устанавливает потенциальные угрозы безопасности и основные способы достижения требуемого уровня безопасности.

3) Приказ Генерального прокурора Российской Федерации от 04.04.2019 № 249 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного доступа в органах и организациях прокуратуры Российской Федерации» (Далее – Приказ № 249) [9]. Приказ № 249

регламентирует базовый алгоритм любого обращения с документальными и иными физическими носителями данных, включающих в свое содержание специальные служебные данные, запрещенные в доступе, в структуре органов и должностных лиц прокуратуры Российской Федерации.

4) Приказ Генеральной прокуратуры Российской Федерации от 31 мая 2011 г. № 153 «Об организации работы по обеспечению доступа к информации о деятельности органов и учреждений прокуратуры Российской Федерации», в котором закреплен порядок обеспечения доступа к информации о деятельности органов и учреждений прокуратуры России.

5) Приказ Генеральной прокуратуры Российской Федерации от 20 ноября 2013 г. № 506 «Об утверждении и введении в действие Инструкции о порядке обработки в органах прокуратуры Российской Федерации персональных данных, полученных в связи с осуществлением прокурорского надзора» в соответствии с которым в органах прокуратуры обрабатываются персональные данные, полученные в связи с прокурорским надзором. Это анкетная и биографическая информация, сведения об образовании, о трудовой деятельности, о составе семьи, об имуществе, о доходах и расходах и др.

6) Приказ Генеральной прокуратуры Российской Федерации от 04.07.2017 № 448 «Об утверждении Правил обработки персональных данных в связи с прохождением службы (работой) в органах и организациях прокуратуры Российской Федерации» [10], в соответствии с пунктом 5.2 которого обезличивание персональных данных проводится в целях снижения ущерба от разглашения персональных данных, повышения уровня защищенности автоматизированных информационных систем органа прокуратуры и предотвращения несанкционированного использования персональных данных, если иное не предусмотрено законодательством Российской Федерации.

7) Вопросы, связанные с организацией работы со специальной служебной информацией в прокуратуре, регламентированы нормами Инструкции по делопроизводству в органах и организациях прокуратуры Российской Федерации [11].

8) «Положение об управлении физической защиты и обеспечения безопасности Генеральной прокуратуры Российской Федерации», утв. Генеральной прокуратурой России 11.09.2014. Так, в Положении об управлении физической защиты и обеспечения безопасности Генеральной прокуратуры Российской Федерации указывается, что разрабатываются и принимаются на комплексной и системной основе меры по обеспечению информационной безопасности органов и организаций прокуратуры Российской Федерации, совершенствуются формы, методы и средства выявления, оценки и прогнозирования угроз информационной безопасности, осуществляется контроль за защитой соответствующей информации на всех этапах технологических циклов ее создания, хранения, обработки и передачи. Контролируется эффективность предусмотренных технических мер защиты сведений, составляющих государственную тайну, конфиденциальной, служебной и иной информации в органах и организациях прокуратуры Российской Федерации и выполнение требований по защите информации удостоверяющего центра в Генеральной прокуратуре Российской Федерации и иных криптографических (шифровальных) средств защиты информации. Необходимо отдельно выделить Приказ Генеральной прокуратуры РФ № 627 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года», поскольку данный нормативно-правовой акт является первым документом Генеральной прокуратуры, в котором обозначена информационная безопасность как принцип, как направление деятельности. Вместе с тем при всей активной деятельности органов прокуратуры в сфере правовой регламентации организации обеспечения информационной безопасности, ни в одном правовом акте не определено место прокуратуры в системе обеспечения информационной безопасности.

В заключении хотелось бы отметить, что, информационная безопасность представляет собой, как правовой феномен, сложное системное, многоуровневое явление, на состояние и перспективы развития которого оказывают прямое воздействие внешние и внутренние факторы такие как развитие информационно-

коммуникационных технологий, появление новых видов правонарушений в информационной среде, появление цифровой экономики. В таких условиях необходимо обеспечить технологическую и производственную независимость и информационную безопасность, для защиты данных в Российской Федерации необходимо продолжить совершенствовать нормативно-правовое регулирование в сфере обеспечения безопасной обработки информации (включая ее поиск, сбор, анализ, использование, сохранение и распространение) и обеспечить применение новых технологий, уровень которых должен соответствовать развитию и интересам общества.

Список литературы:

1. Доклад управления правовой статистики и информационных технологий Генеральной прокуратуры РФ на тему «Состояние преступности в России» за январь-декабрь 2020 г. 6 с.

2. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: Горячая линия-Телеком, 2001. 148 с.

3. Ясенев В.Н. Информационная безопасность в экономических системах. Н. Новгород: ННГУ, 2006. 253 с.

4. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. М.: МИФИ, 1995. 96 с.

5. Лопатин Ю.Н. Информационная безопасность в России. Проблемы, поиски решений // Гуманитарные исследования в Восточной Сибири и на Дальнем Востоке. 2008. № 2. С. 51-57.

6. Мазуров В.А. Понятие и принципы информационной безопасности // Известия Алтайского государственного университета. 2003. № 2. С. 57-63.

7. Кривоухов А.А., Зотов В.В. Информационная безопасность как антропосоциотехнический феномен // Коммуникология. 2017. Том 5. № 4. С. 71-81.

8. Приказ Генеральной прокуратуры Российской Федерации от 27.11.2019 № 830 «Об утверждении Концепции безопасности органов и организаций прокуратуры Российской Федерации» // Законность. № 1. 2020.

9. Приказ Генерального прокурора Российской Федерации от 04.04.2019 № 249 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного доступа в органах и организациях прокуратуры Российской Федерации» // Справочно-правовая система «Консультант-Плюс».

10. Приказ Генеральной прокуратуры Российской Федерации от 04.07.2017 № 448 «Об утверждении Правил обработки персональных данных в связи с прохождением службы (работой) в органах и организациях прокуратуры Российской Федерации» // Справочно-правовая система «Консультант-Плюс».

11. Приказ Генеральной прокуратуры Российской Федерации от 29.12.2011 № 450 (ред. от 29.12.2020) «О введении в действие Инструкции по делопроизводству в органах и организациях прокуратуры Российской Федерации» // Справочно-правовая система «Консультант-Плюс».