МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра конституционного и муниципального права

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ПРОКУРАТУРЫ РФ

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 2 курса 261 группы направления подготовки 40.04.01«Юриспруденция»

магистерской программы «Правовое обеспечение деятельности органов публичной власти»

юридического факультета
Павленко Алёны Дмитриевны

Научный руководитель
профессор, д.ю.н С.Е. Чаннов

Зав. кафедрой
профессор, д.ю.н., Заслуженный юрист РФ Г.Н.Комкова

Саратов 2025

Введение

Актуальность темы исследования. Информационная безопасность является в современных условиях особенно актуальным явлением, в том числе, и в контексте обеспечения национальной безопасности российского государства. Вопросы обеспечения информационной безопасности не обошли стороной и органы прокуратуры Российской Федерации. Деятельность прокурорского работника при осуществлении надзорных мероприятий непосредственным образом сопряжена с обработкой существенных объемов информации, поступающей из различных источников, циклы получения и отправки такой информации многократно повторяются, что обуславливает возникновение потенциальных угроз несанкционированного распространения информации.

Нормативное закрепление обеспечения информационной безопасности в качестве одной из приоритетных задач государства обусловлено систематическим и стремительным ростом информационных угроз самого разнообразного характера, в том числе и угроз применения информационного оружия. Современные закономерности и тенденции широкомасштабного ускоряющегося процесса развития и при этом совершенствования информационных систем и технологий наглядно демонстрируют возрастание актуальности проблемы поиска высокого уровня технических, юридических, организационных и иных мероприятий обеспечения информационной безопасности.

Кроме того, современные условия развития общественных отношений характеризуются повсеместным распространением процессов цифровизации, в которые прочно утвердились и в органах прокуратуры РФ. Использование современных информационных технологий повышает вероятность утечки служебной информации. Обилие нового программного обеспечения, переход на электронный документооборот и электронное взаимодействие являются современными трендами развития производства и сферы услуг. Игнорирование этого фактора может снизить эффективность прокурорского

надзора в перспективе. Вместе с тем создание условий безопасного информационного взаимодействия в цифровой среде не менее важно, чем создание самой цифровой среды.

Сегодня риски кибератак, а также иных способов незаконного завладения информацией очень высоки. Несанкционированное изъятие (копирование), распространение служебной информации может не только нанести имиджевый ущерб органам прокуратуры, но и затронуть права и законные интересы тех лиц, сведения о которых были разглашены. В современное время против российского государства осуществляется беспрецедентная медиакоммуникационная агрессия, призванная осуществлять целенаправленное сопровождение военных действий, диверсий и разнообразных санкционных мер. В осуществлении такой агрессии активно задействованы различные сетевые и социальные средства массовой информации, сайты и порталы, сфера блогинга. Против Российской Федерации, таким образом, была начата информационная кампания, сопровождавшаяся огромным количеством фейков в сети Интернет.

Кроме того, стоит сказать и о том, что значительная доля прокурорских работников, не в полной мере осознают серьезность и масштабы угроз информационной безопасности. Существенную угрозу информационной безопасности представляют и современные вредоносные программы.

Усилились угрозы информационной безопасности и в связи с противоправными действиями со стороны недружественных государств, что обуславливает повышенную необходимость обеспечения информационной безопасности органов государственной власти. В связи с этим, выбранная тема исследования является актуальной в настоящее время.

Степень теоретической разработанности темы. Вопросам обеспечения информационной безопасности в органах прокуратуры в настоящее время необходимого внимания в рамках научной литературы не уделено, комплексных исследований по данному вопросу не проводилось. Однако, отдельно вопросы осуществления прокурорской деятельности и

вопросы обеспечения информационной безопасности на доктринальном уровне исследованы в достаточной степени. Так, в рамках настоящей работы использовались научные разработки, содержащиеся в следующих диссертационных исследованиях: М.А. Ефремова «Уголовно-правовая охрана информационной безопасности»; А.В. Кубышкин «Международно-правовые проблемы обеспечения информационной безопасности государства»; П.У. Кузнецов «Теоретические основания информационного права»; В.Н. Лопатин «Информационная безопасность России» и др.

Также были задействованы научные исследования таких авторов, как: С.С. Алексеев, В.А. Баранова, О.А. Бельков, Ю.Е. Винокуров, Д.Е. Волков, О.В. Воронин, И.И. Головко, И.А. Данилюк, Р.О. Долотов, З.А. Зумакулова, Е.А. Иванченко, Д.В. Крылова, М.А. Кистанова, Н.Д. Казаков, О.Ю. Казаков, Ю.О. Карпышева, А.Г. Климашин, М.В. Колесов, Г.Н. Королев, А.А. Косоруков, Д.Н. Лапаев, М.Н. Марченко, Н.И. Матузов, С.Э. Мерзляков, Е.А. Миллерова, Г.А. Морозова, В.Н. Пасичник, В.А. Поздняков, Е.О. Прилепских, Е.И. Рудакова, Э.В. Талапина, Е.О. Таппасханова, Р.А. Токмакова, А.А. Турко, А.Ю. Чурикова, Л.И. Шершенев, В.Н. Южаков, А.В. Яшина и др.

Объектом исследования являются общественные отношения, складывающиеся в ходе обеспечения информационной безопасности в органах прокуратуры Российской Федерации.

Предметом исследования выступает совокупность правовых норм, регламентирующих отдельные вопросы обеспечения информационной безопасности в Российской Федерации и органах прокуратуры Российской Федерации, а также научные разработки в рассматриваемой области.

Цель исследования заключается в комплексном анализе вопросов обеспечения информационной безопасности в органах прокуратуры Российской Федерации.

Научная новизна диссертации, определяемая положениями, выносимыми на защиту:

1. Информационную безопасность предложено понимать как состояние защищенности информации и соответствующей инфраструктуры от случайного или преднамеренного воздействия естественного или искусственного характера, - воздействия, способного причинить неприемлемый ущерб охраняемым законом отношениям, а также субъектам, эту информацию использующим. Также предложено выделение следующих структурных элементов информационной безопасности: общественные отношения, обеспечивающие реализацию права на информацию и на охрану информации от неправомерного доступа; общественные отношения, обеспечивающие безопасность информационных ресурсов; общественные отношения, обеспечивающие безопасность использования информационно-телекоммуникационных технологий.

2. Важнейшим механизмом обеспечения информационной безопасности является уголовно-правовой механизм ее обеспечения, который в настоящее время, как справедливо отмечается в научной литературе, не является совершенным. Во-первых, информационная безопасность до настоящего времени не рассматривается как самостоятельный объект уголовно-правовой охраны, а во-вторых, существующие составы преступлений, как правило, направлены на борьбу с «внешними» информационными угрозами. В связи с этим представляется обоснованным и необходимым:

- определение информационной безопасности в качестве самостоятельного объекта уголовно-правовой охраны и включение в Особенную часть УК РФ раздела «Преступления против информационной безопасности»;
- включение в текст Особенной части УК РФ специальной нормы, предусматривающей уголовную ответственность за незаконные разглашение или использование сведений, составляющих служебную тайну, субъектами которых будут выступать лица, деятельность которых непосредственно сопряжена с обращением с информацией служебного пользования. Данная

норма, наряду с положениями иных статей УК РФ, направленных на охрану информационной безопасности (137, 138, 138.1, 183, 272, 273, 274, 283, 283.1, 284, 310, 311, 320 УК РФ и др.) может быть включена в раздел «Преступления против информационной безопасности».

3. В соответствии с Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года органы прокуратуры начинают активно внедрять в свою деятельность технологии искусственного интеллекта. В том числе, применение искусственного интеллекта видится необходимым для исследования информации, размещаемой в информационно-телекоммуникационных сетях, в том числе в сети Интернет; использование искусственного интеллекта способствовало бы организации более эффективного надзорного сопровождения реализации национальных проектов, а также в целом осуществлению надзора за исполнением законов о контрактной системе и об оборонно-промышленном комплексе; возможна автоматизация процедуры антикоррупционной экспертизы сиспользованием методов искусственного интеллекта. Однако, в таком случае закономерно встает вопрос обеспечения информационной безопасности в органах прокуратуры. В данном аспекте, считается, что возможно внедрение лишь «слабых» технологий искусственного интеллекта, более того, представляется необходимым закрепление такой ответственности, а также проработка вопросов, связанных с распределением ответственности между разработчиком технологии ИИ и организацией, которая такие технологии применяет, в случае причинения вреда.

Теоретическая значимость результатов исследования определяется тем, что выработанные выводы и предложения расширяют сферу научных знаний в области правового регулирования обеспечения информационной безопасности в органах прокуратуры.

Практическая значимость результатов исследования определяется направленностью исследования на решение актуальных проблем правового регулирования информационной безопасности в органах прокуратуры.

Сделанные выводы могут быть использованы при совершенствовании норм действующего российского законодательства. Кроме того, результаты проведенного исследования могут быть использованы в процессе преподавания учебных дисциплин в юридических вузах, на юридических факультетах.

Структура диссертации представлена введением, двумя главами, включающими в себя четыре параграфа, заключением и библиографическим списком.

Основное содержание работы

В первой главе магистерской работы рассматривается понятие и значение обеспечения информационной безопасности в органах прокуратуры. В первом параграфе определен правовой статус прокурора и особенности организации его деятельности; во втором параграфе проанализировано понятие информационной безопасности и особенности ее обеспечения в органах прокуратуры.

Во второй главе диссертационного исследования проанализированы особенности правового регулирования и способов обеспечения информационной безопасности в органах прокуратуры. В первом параграфе рассмотрено правовое регулирование информационной безопасности в органах прокуратуры Российской Федерации; во втором параграфе проанализированы основные механизмы обеспечения информационной безопасности в органах прокуратуры; в третьем параграфе проанализированы перспективы использования технологий искусственного интеллекта в деятельности органов прокуратуры в контексте обеспечения информационной безопасности.

Заключение

На основании проведенного исследования был получен ряд следующих выводов.

1. Под прокурорским надзором можно понимать один из видов деятельности органов прокуратуры, осуществляемый от имени Российской Федерации, состоящий в осуществлении надзора за поднадзорными субъектами в части исполнения и соблюдения ими Конституции РФ и иных федеральных нормативно-правовых актов, допускающим возможность применения средств прокурорского реагирования в случаях, предусмотренных нормами действующего законодательства.

2. Прокурор в Российской Федерации наделен общим и специальным правовым статусом, поскольку, участвуя в различных видах судопроизводства, рассматриваемый субъект наделяется совокупностью различных прав и обязанностей. Для эффективной реализации прокурором предоставленных ему полномочий, российское законодательство устанавливает ряд соответствующих правовых гарантий осуществления прокурорской деятельности. Правовые гарантии обеспечивают прокурорам возможность выполнять свои обязанности и использовать свои права для решения задач, возложенных на них государством, а именно: обеспечение верховенства закона, единства и укрепления законности, защита прав и свобод человека и гражданина, а также охраняемых законом интересов общества и государства.

3. Безопасность представляет собой такое состояние общественных отношений, при котором обеспечивают от негативного воздействия внутренних и внешних угроз интересы человека, общества и государства, вместе с тем – это специфическая деятельность уполномоченных органов, направленная на обеспечение состояния защищенность указанных субъектов. Информационную безопасность можно определить как состояние защищенности информации и соответствующей инфраструктуры от случайного или преднамеренного воздействия естественного или искусственного характера, - воздействия, способного причинить неприемлемый ущерб охраняемым законом отношениям, а также субъектам, эту информацию использующим.

4. Структура информационной безопасности включает в себя: общественные отношения, обеспечивающие реализацию права на информацию и на охрану информации от неправомерного доступа; общественные отношения, обеспечивающие безопасность информационных ресурсов; общественные отношения, обеспечивающие безопасность использования информационно-телекоммуникационных технологий.

5. Деятельность прокурорского работника при осуществлении надзорных мероприятий непосредственным образом сопряжена с обработкой существенных объемов информации, поступающей из различных источников, циклы получения и отправки такой информации многократно повторяются, что обуславливает возникновение потенциальных угроз несанкционированного распространения информации. Кроме того, современные условия развития общественных отношений характеризуются повсеместным распространением процессов цифровизации, в которые прочно утвердились и в органах прокуратуры РФ.

6. Реализация органами прокуратуры возложенных на нее функций и задач, а также сама специфика осуществления прокурорского надзора обуславливает аккумуляцию в ведомстве существенных объемов информации, основная часть из которой в силу норм действующего законодательства ограничена в доступе. Такая информация может быть сопряжена с уголовно-процессуальной деятельностью, за законностью которой органами прокуратуры осуществляется надзор, с персональными данными граждан, сведениями, составляющими банковскую, коммерческую, иную охраняемую законом тайну и проч. Обеспечение безопасности такой информации обусловлено необходимостью защиты интересов государства, общества и каждой конкретной личности, которым может быть нанесен существенный ущерб при несанкционированном доступе / изменении / блокировании / удалении / хищении такой информации. Однако в настоящее время внутренние угрозы информационной безопасности органов прокуратуры достаточно высоки, что обуславливается множественными

факторами, основными из которых выступают: в отношении государства и его органов осуществляется беспрецедентная медиа-коммуникационная агрессия, в том числе учащены в современных условиях риски кибератак; значительная часть прокурорских работников не обладает должной квалификацией, знаниями, навыками и умениями, необходимыми для безопасной работы с информацией; органы прокуратуры в современных условиях подвержены существенной цифровой трансформации.

7. Ведомственными актами прокуратуры регламентируются: алгоритм осуществления любых действий и любого обращения с документальными и иными физическими носителями данных, которые содержат в себе специальные служебные данные;порядок обеспечения доступа к информации о деятельности органов и учреждений прокуратуры России; правила обработки в органах прокуратуры персональных данных, которые сотрудники прокуратуры получают в ходе осуществления прокурорского надзора; правила организации работы со специальной служебной информацией в органах прокуратуры; контроль защиты информации на всех этапах ее создания, хранения, обработки и передачи; комплексные и системные меры по обеспечению информационной безопасности органов и организаций прокуратуры, совершенствование форм, методов и средств выявления, прогнозирования и оценки угроз информационной безопасности.

8. К числу объектов информационной безопасности органов прокуратуры могут быть отнесены:

– информационные ресурсы с ограниченным доступом, составляющие государственную, коммерческую, банковскую, служебную тайну и персональные данные, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также открытая (общедоступная) информация, представленная в виде документов и массивов информации независимо от формы и вида их представления;

– процессы обработки информации в информационно-телекоммуникационной системе и на объектах информатизации органов прокуратуры;

– научно-технический персонал разработчиков, пользователи системы и ее обслуживающий персонал, информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты информационно-телекоммуникационной системы и объекты информации органов прокуратуры.

9. В структуру прокуратур вводятся должностные единицы, основной обязанностью которых выступает пресечение случаев умышленного или неосторожного несанкционированного доступа к информационным системам и каналам связи. Защита распространяется на внутренние инфраструктурные системы, предназначенные для обобщения и анализа информации, работа которых обеспечивается специальным программным сопровождением, разработанным для органов прокуратуры.

10. Важнейшим механизмом обеспечения информационной безопасности является уголовно-правовой механизм ее обеспечения, который в настоящее время, как справедливо отмечается в научной литературе, не является совершенным. Во-первых, информационная безопасность до настоящего времени не рассматривается как самостоятельный объект уголовно-правовой охраны, а во-вторых, существующие составы преступлений, как правило, направлены на борьбу с «внешними» информационными угрозами. В связи с этим представляется обоснованным и необходимым:

– определение информационной безопасности в качестве самостоятельного объекта уголовно-правовой охраны и включение в

Особенную часть УК РФ раздела «Преступления против информационной безопасности»;

– включение в текст Особенной части УК РФ специальной нормы, предусматривающей уголовную ответственность за незаконные разглашение или использование сведений, составляющих служебную тайну, субъектами которых будут выступать лица, деятельность которых непосредственно сопряжена с обращением с информацией служебного пользования.

11. XXI век характеризуется достаточно высокой степенью развития информационных технологий и цифровизацией практически всех сфер общественной жизни. Одной из наиболее совершенных и перспективных технологий в настоящее время является технология искусственного интеллекта, которая позволяет выполнять отдельные операции, свойственные мыслительному процессу индивида. Технологии искусственного интеллекта внедряются в общественную жизнь повсеместно, не стала исключением и деятельность органов государственной власти, в том числе органов прокуратуры. Технологии искусственного интеллекта в деятельности органов прокуратуры могут обуславливать многие преимущества, однако, риски использования таких технологий достаточно высоки, наиболее серьезным из них считается угроза информационной безопасности органов прокуратуры.

12. В соответствии с Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года органы прокуратуры начинают активно внедрять в свою деятельность технологии искусственного интеллекта. В том числе, применение искусственного интеллекта видится необходимым для исследования информации, размещаемой в информационно-телекоммуникационных сетях, в том числе в сети Интернет; использование искусственного интеллекта способствовало бы организации более эффективного надзорного сопровождения реализации национальных проектов, а также в целом осуществлению надзора за исполнением законов о контрактной системе и об оборонно-промышленном комплексе; возможна автоматизация процедуры антикоррупционной экспертизы сиспользованием

методов искусственного интеллекта. Однако, в таком случае закономерно встает вопрос обеспечения информационной безопасности в органах прокуратуры. В данном аспекте, считается, что возможно внедрение лишь «слабых» технологий искусственного интеллекта, более того, представляется необходимым закрепление такой ответственности, а также проработка вопросов, связанных с распределением ответственности между разработчиком технологии ИИ и организацией, которая такие технологии применяет, в случае причинения вреда.

13. В апреле 2024 г. Генеральным прокурором Российской Федерации был подписан план по внедрению в деятельность органов прокуратуры искусственного интеллекта и нейросетей. Концептуально, рассматриваемый план предполагает: изучение возможности доработки автоматизированного информационного комплекса «Надзор-WEB» в части создания модуля, позволяющего анализировать обращения граждан, в том числе до их рассмотрения по существу, на основе текста прикрепленных к регистрационной карточке файлов, а также отображать аналитическую информацию, касающуюся обращений, по рубрикам и регионам на картографической основе; расширение функционала автоматизированного информационного комплекса «Надзор- WEB» в целях достижения максимальной автоматизации подготовки проектов однотипных документов: постановления об отмене процессуальных решений, исковые заявления, уведомления заявителям, сопроводительные письма о переадресации обращений и т. п. изучение возможности искусственного интеллекта в области поддержания государственного обвинения.

14. Вполне обоснованной и рациональной можно признать точку зрения относительно возможности использования рассматриваемой технологии сотрудниками органов прокуратуры при осуществлении мониторинга информации в цифровом пространстве. Обязанности по осуществлению такого мониторинга закреплены в целом ряде отраслевых актов, которые возлагают на сотрудников прокуратуры мониторинг

огромного количества информации в сети Интернет, социальных сетях, мессенджерах и иных объектах виртуального пространства для достижения целей деятельности данного ведомства.

15. Применительно к составлению соответствующих процессуальных документов в рамках деятельности органов прокуратуры РФ представляется обоснованным говорить лишь о вероятности внедрения «слабых» технологий искусственного интеллекта, которые позволят не полностью заменить умственный индивидуальный труд сотрудников по составлению соответствующих документов (в силу высокой степени важности данной деятельности в рассматриваемом ведомстве), а лишь упростить и автоматизировать отдельные технические аспекты составления процессуальных документов.