DOI: http://dx.doi.org/10.21686/2411-118X-2025-4-187-193

К вопросу об основных принципах построения административной архитектуры обеспечения информационной безопасности

Е. А. Иванченко
кандидат юридических наук, доцент,
доцент кафедры правовой культуры и защиты прав человека Юридического института
ФГАОУ ВО «Северо-Кавказский федеральный университет».
Адрес: ФГАОУ ВО «Северо-Кавказский федеральный университет»,
355017, Ставрополь, ул. Пушкина, д. 1А.
E-mail: kvi-elena@yandex.ru

Т. В. Воротилина,
кандидат юридических наук, доцент,
доцент кафедры гражданско-правовых дисциплин
РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова»,
109992, Москва, Стремянный пер., д. 36.
E-mail: vorotilina@mail.ru

On the Issue of the Basic Principles of Building an Administrative Architecture for Ensuring Information Security

E. A. Ivanchenko
PhD in Law, Associate Professor, Associate Professor of the Department
of Legal Culture and Protection of Human Rights
of Juridical institute of FSAEI «North-Caucasian Federal University».
Address: North-Caucasus Federal University,
1A Pushkin Str., Stavropol, 355017, Russian Federation.
E-mail: kvi-elena@yandex.ru

T. V. Vorotilina
PhD in Law, Associate Professor,
Associate Professor of the Department of Civil Law Disciplines of the PRUE.
Address: Plekhanov Russian University of Economics,
36 Stremyanny Lane, Moscow, 109992, Russian Federation.
E-mail: vorotilina@mail.ru

Поступила 08.09.2025 Принята к печати 25.09.2025

Аннотация

Авторами проведена оценка актуальных научных исследований в рамках рассматриваемого проблемного поля обеспечения информационной безопасности. Рассмотрены элементы, составляющие предмет информационной безопасности; данным элементам дана необходимая характеристика. Методологическая основа исследования представлена такими всеобщими и общенаучными методами познания, как анализ, диалектический и логический методы, структурно-функциональный метод; также применялись специально-юридические методы исследования, а именно формально–юридический и системно-структурный. Авторы приходят к выводу о том, что архитектура построения системы информационной безопасности представляет собой прежде всего скоординированное административное взаимодействие основных публичных субъектов, применяющих правовые, административные, криптографические и иные меры защиты информационной безопасности.

Ключевые слова: информационная безопасность, принципы обеспечения информационной безопасности, угрозы информационной безопасности, административное управление.

Abstract

The authors conducted an assessment of current scientific research in the framework of the considered problematic field of information security. The elements that make up the subject of information security are considered, these elements are given the necessary characteristics. The methodological basis of the research is represented by such universal and general scientific methods of cognition as analysis, dialectical and logical methods, structural and functional method, as well as special legal research methods, namely, formal legal and systemic structural methods. The authors conclude that the architecture of the information security system is primarily a coordinated administrative interaction of the main public entities applying legal, administrative, cryptographic and other measures to protect information security.

Keywords: information security, principles of information security, threats to information security, administrative management.

В свете последних геополитических трансформаций мирового сообщества информация становится значительным экономическим, стратегическим и политическим ресурсом, обладание которым обусловливает надлежащее состояние национальной безопасности государства в глобальном смысле. Именно поэтому обеспечение информационной безопасности входит в число обозначенных национальных приоритетов[1].

Динамичное развитие информационных технологий свидетельствует, что нормативно-правовые акты, регламентирующие правоотношения, возникающие в информационном поле или относительно информационного пространства, должны характеризоваться комплексным подходом в оценке информационных угроз и организации надлежащего государственного управления данными общественными отношениями.

Актуальность темы объясняется значимостью качественного стратегического планирования и надлежащего административного управления вопросами, относящимися к сфере информационной безопасности.

Значительные бюджетные средства, направляемые на реализацию многочисленных целевых программ, логически связанных общей доктриной обеспечения информационной безопасности, обязывают организовать соответствующий государственный надзор (контроль) этой сферы, особенно в условиях взаимодействия в бюджетных процессах многих субъектов публичной власти и в связи с многоступенчатостью этих процессов.

Выбранная тема представляется авторам безусловно актуальной и в свете беспрецедентного расширения международного сотрудничества Российской Федерации с зарубежными странами в пределах отдельных регионов по вопросам информационной безопасности, заключения в рамках указанного сотрудничества числа важных государственных соглашений. Высказываясь по этому вопросу в 2021 г., Президент Российской Федерации В. В. Путин отметил: «Начата совместная работа по проблемам стратегической стабильности и информационной безопасности …Мы открыты к контактам и к обмену мнениями, конструктивному диалогу»[2].

Анализ специальных источников показал, что накоплен значительный опыт научных исследований в рамках рассматриваемого проблемного поля, однако горизонт потенциальных угроз информационной безопасности настолько широк, а угрожающие процессы-вызовы информационному суверенитету настолько динамичны, что потребность в научных исследованиях сохраняется в достаточно высокой степени.

Отдельные аспекты государственного управления в сфере информационной безопасности были освещены в исследованиях таких ученых, как С. М. Бойко, А. К. Дубень, М. В. Киян, О. С. Макаров, Я. Е. Коровина, А. В. Крутских, А. Г. Оносов, О. В. Петровская, Т. А. Полякова, О. М Пьянков, и других исследователей, труды которых положены в теоретическую основу данной работы.

[1] Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Собрание законодательства Российской Федерации. – 19.04.2021. – № 16. – Часть I. – Ст. 2746; Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. – 05.07.2021. – № 27. – Часть II. – Ст. 5351.

[2] Международная информационная безопасность: подходы России / А. В. Крутских, Е. А. Зиновьева, В. И. Булва, М. Б. Алборова, Ю. А. Юдина; под ред. А. В. Крутских, Е. С. Зиновьева. – М., 2021.

Нельзя отказать в справедливости единодушно поддерживаемому российскими правоведами мнению о том, что вопросы обеспечения информационной безопасности с точки зрения стратегической безопасности стоят в одном ряду с проблемами военной, ядерной безопасности, некоторых других ее видов [8. – С. 284]. Бесконтрольная же информационная среда неизбежно приведет к дестабилизации общества и манипулированию сознанием (прибавим к этому угрозы, относящиеся к сфере кибербезопасности как части информационной безопасности) [4. – С. 95].

Угрозы национальной информационной безопасности традиционно подразделяются на две группы – внутренние и внешние. Мы также будем придерживаться данной традиции.

Внутренние угрозы мы представим следующим списком:

– продолжающаяся несогласованность действий субъектов публичной власти по поддержанию общей информационной безопасности;

– несоблюдение режима оборота информации, имеющей статус ограниченного доступа;

– несоблюдение требований к кадровому обеспечению работ, связанных с обеспечением информационной безопасности;

– несоблюдение требований законодательства о защите изобретений, имеющих статус «секретно» (несоблюдение процедуры регистрации и прочие нарушения), в том числе изобретенных в рамках государственного заказа;

– ненадлежащая урегулированность вопросов, относящихся к сфере информационной безопасности, в российском законодательстве;

– продолжающееся использование зарубежных технологий в сфере информационных процессов.

Перечень внешних угроз информационной безопасности можно представить следующим образом:

– установление неправомерной цензуры и фильтрации информационного контента о проводимой Россией политике, предлагаемых ею инициативах для международного сообщества, умышленное умаление на этой арене роли России;

– активная разведывательная деятельность спецслужб недружественных России стран;

– активные акты агрессии на информационные системы органов государственной власти, иных субъектов, а также на объекты критической инфраструктуры;

– распространяющаяся практика применения когнитивного оружия.

Таким образом, состояние опасности и неопределенности можно назвать характеризующим информационную среду. Значит, государством должен быть предусмотрен административный механизм, на постоянной основе нивелирующий информационные угрозы и предусматривающий через систему эффективного прогнозирования противодействие таким угрозам в условиях постоянной геополитической трансформации.

Что представляет собой в самых общих чертах административная архитектура обеспечения информационной безопасности, которая позволит поддерживать эту безопасность на надлежащем уровне? Попытаемся ее охарактеризовать, называя и давая параллельно характеристику основным современным информационным угрозам.

1. Административная архитектура обеспечения информационной безопасности должна учитывать и быть выстроена с учетом следующих характеристик современных цифровых технологий – «их конвергентности, сквозного и прорывного характера» [2. – С. 75].

Указанные характеристики предоставляют безграничные возможности для научно-технического прогресса, вместе с тем обладая высочайшим потенциалом опасности для состояния защищенности российского общества. Об этом свидетельствует значительный рост преступлений, совершенных в сфере компьютерных технологий.

Так, по информации МВД России, число преступлений, связанных с неправомерным доступом к компьютерной информации, выросло втрое за 2024 год и составило 104 653 случая (в 2023 г. — 36 274). 90% из них связаны со взломом аккаунтов на «Госуслугах»[1].

2. Административная архитектура обеспечения информационной безопасности должна предусматривать усиление негативных тенденций в связи с распространяющейся практикой организации трудовой деятельности в дистанционном формате и использованием цифровых сервисов.

[1] МВД: взломы «Госуслуг» составляют 90% преступлений с незаконным доступом к данным / Ответ пресс-центра МВД России на запрос ТАСС 01.06.2025. – URL: https://tass.ru/obschestvo/24104331

Дистанционная форма осуществления трудовой деятельности на порядок увеличивает возможности злоумышленников осуществлять информационные атаки. Помимо прочих факторов, как обоснованно отмечают М. О. Пьянков и Е. Ю. Никитина, основным остается то, что на личном компьютере крайне сложно контролировать устанавливаемое программное обеспечение и обеспечивать должный уровень защиты [7]. Данная тенденция детерминировала усиление противоправных действий, совершаемых на информационные системы органов государственной власти и объектов критической инфраструктуры.

Особенно актуализировался данный вопрос в связи с расширением практики применения технологий ИИ в отдельных сферах трудовой деятельности, которую граждане осуществляют дистанционно, т. е., как справедливо отмечает Д. В. Лемешко, государственный аппарат должен экстренно озадачиться «…повышением культуры информационной безопасности профессиональных и бытовых пользователей» [5. – С. 125].

3. Отдельного внимания при выстраивании административной архитектуры обеспечения информационной безопасности требуют организационно-правовые меры, направленные на поддержание безопасности в кредитно-финансовой сфере Российской Федерации, так как успешные (не предотвращенные) информационные атаки в данном сегменте:

– наносят вред экономической устойчивости государства через его финансовые институты;

– снижают уровень доверия населения к государственным институтам в сфере финансов;

– негативным образом влияют на непрерывность работы субъектов публичной власти, на всю систему управления в целом.

Между тем административная архитектура обеспечения информационной безопасности адаптируется в противостоянии информационным угрозам, и именно необходимостью адекватного противостояния было обусловлено принятие в мае 2022 г. управленческих мер, о которых мы упоминали во введении к работе.

Комментируя вводимые управленческие меры, министр иностранных дел России С. В. Лавров подчеркнул необходимость отказа от старой парадигмы в связи с переходом органов государственной власти на новую – цифровую основу организации деятельности. Согласно мнению министра, страны Евросоюза и прочие отдельные государства стремятся сохранять доминирующее положение в высоких технологиях, а потому объекты критической инфраструктуры и государственные учреждения в России продолжают оставаться в положении риска, что формирует новые вызовы и новые задачи, стоящие перед органами исполнительной власти, а также необходимость усиления контроля за исполнением соответствующих поручений правительства[1].

4. Административной архитектуре обеспечения информационной безопасности надлежит организовать постоянно функционирующие системы:

– подготовки и переподготовки кадров, способных осуществлять свои обязанности в среде постоянно предпринимаемых информационных атак (так, А. Г. Оносов, рассуждая о ключевых организационных мерах защиты на предприятиях, особое внимание уделяет вопросам подготовки персонала, обороту и управлению паролями, проведению аудитов безопасности и т. д. [6. – С. 20], поддерживают его и иные авторы, во главу мер информационной безопасности ставящие именно надлежащее внимание к человеческому фактору);

– осуществления бета-тестирования программного оборудования для выявления уязвимости информационных рисков и угроз [9. – С. 1110] (так, специалисты по данному вопросу отмечают следующее: «Изучение уязвимостей программного обеспечения является важным элементом моделирования угроз, так как позволяет обнаружить потенциальные точки проникновения для злоумышленников. Для этого применялись специализированные сканеры уязвимостей, такие как Nessus и OpenVAS, которые помогают выявить слабые места как в операционных системах, так и в приложениях. Эти инструменты нацелены на нахождение известных уязвимостей, включая ошибки в конфигурации безопасности, устаревшие версии программного обеспечения или ошибки кода, которые могут быть использованы хакерами» [1. – С. 7]).

В связи с необходимостью организации такой системы на правительственном уровне было

[1] Выступление министра иностранных дел Российской Федерации С. В. Лаврова на пленарной сессии «Международные отношения в условиях цифровизации общественной жизни» международной научно-практической конференции «Цифровые международные отношения 2022», Москва, 14 апреля 2022 г. – URL: https://www.mid.ru/ru/press_service/video/view/1809294

принято решение о создании к 2022 г. специальных полигонов, на которых специалистов будут обучать основам информационной безопасности[1], при этом к 2024 г. число таких центров планировалось довести до 15[2].

Однако данному решению не суждено было реализоваться[3], что мы считаем серьезной управленческой недоработкой. Функционируют лишь 8 опорных центров обучения кибербезопасности на базе отдельных вузов, что, конечно, не совсем соответствует первоначальной идее.

5. Предотвращение распространения недостоверной информации должно осуществляться административной архитектурой обеспечения информационной безопасности. Информационное противоборство – это реалии нашего времени, в условиях которых должен продолжать свою деятельность государственный аппарат обеспечения информационной безопасности.

Цели распространения недостоверной информации могут быть самыми разными, но их можно объединить одной генеральной – умышленная дестабилизация государственного аппарата для недружественного вмешательства во внутренние дела государства. При этом, как отмечают ученые, «фейковые новости представляют собой не просто ложные сведения, но целенаправленные действия, когда ложная информация распространяется под видом правдивой с целью вызвать определенные реакции или повлиять на поведение граждан» [3. – С. 29], что, несомненно, еще больше угрожает национальной безопасности.

6. Предотвращение противоправной деятельности транснациональных IT-корпораций, направленной на ограничение свободы распространения и получения информации, должно осуществляться административной архитектурой обеспечения информационной безопасности. Деятельность данных субъектов прежде всего выражается в противоправной интернет-цензуре и применении санкционных средств в отношении пользователей, относящихся к российскому сегменту информационного пространства.

Необходимо отметить, что выстраивание эффективной архитектуры обеспечения информационной безопасности возможно только на основе соответствующего международно-правового режима, на установление которого направлены все силы международного сотрудничества по поддержанию международной информационной безопасности.

В частности, должны быть приняты соответствующие глобальные соглашения по двум генеральным вопросам международной информационной безопасности:

– правилам поведения государств – сторон соглашения в информационном пространстве;

– правилам поведения государств – сторон соглашения, находящихся в состоянии вооруженного конфликта или в правовом режиме специальной военной операции.

Таким образом, мы уверенно разделяем мнение, высказываемое большинством российских ученых о том, что разработка таких правил – основное направление международного сотрудничества в сфере информационной безопасности.

Выводы

Архитектура обеспечения информационной безопасности должна быть выстроена с учетом характеристик современных цифровых технологий, а именно – их конвергентности, сквозного и прорывного характера. Указанные характеристики предоставляют безграничные возможности для научно-технического прогресса и вместе с тем обладают высочайшим потенциалом опасности для состояния защищенности российского общества, о чем свидетельствует значительный рост количества преступлений, совершенных в сфере компьютерных технологий.

Обозначенная архитектура должна учитывать усиление негативных тенденций в связи с распространяющейся практикой организации трудовой деятельности в дистанционном формате и использованием цифровых сервисов.

Кроме того, архитектура должна содержать организационно-правовые меры, направленные на поддержание безопасности в кредитно-финансовой сфере Российской Федерации.

---

[1] Чернышенко: в РФ в 2022 году создадут два новых центра Национального киберполигона // Интерфакс, 24.11.2022. – URL: https://academia.interfax.ru/ru/news/articles/8136/

[2] К 2024 году в РФ создадут 15 центров для киберучений // Интерфакс, 02.05.2022. – URL: https://www.interfax-russia.ru/modernizaciya-obrazovaniya/k-2024-godu-v-rf-sozdadut-15-centrov-dlya-kiberucheniy

[3] Из нацпрограммы «Цифровая экономика» исключен проект создания «Национального киберполигона», предназначенного для обучения специалистов основам информационной безопасности и проведению киберучений для различных отраслей экономики // ИТ В ГОССЕКТОРЕ. 02.04.2024. – URL: https://gov.cnews.ru/news/top/2024-04-02_vlasti_sekonomili_milliard

В состав административной архитектуры обеспечения информационной безопасности должна быть включены две постоянно функционирующие подсистемы:

– подготовки и переподготовки кадров, способных осуществлять свои обязанности в среде постоянно предпринимаемых информационных атак;

– осуществления бета-тестирования программного оборудования для выявления уязвимости информационных рисков и угроз.

Угрозы информационной безопасности позволяют очертить круг административно-правовых и организационных мер первоочередного характера, которые направлены на сохранение информационной среды в безопасном для национальных интересов, общественной безопасности и благополучия каждого отдельного гражданина состоянии и позволяют, в частности:

– завершить полный переход на отечественные информационные технологии во всех сферах, а не только представляющих для национальной безопасности стратегический интерес – на объектах критической инфраструктуры, как это стало практиковаться с 1 января 2025 г.;

– создать благоприятные условия для постоянного повышения квалификации специалистов по информационной безопасности;

– сформировать надлежащий уровень информационной культуры населения для повышения устойчивости граждан к умышленному деструктивному информационно-психологическому влиянию со стороны иностранных спецслужб;

– поступательно привести правовые нормы относительно информационной среды и объектов интеллектуальной собственности в согласование с положениями других отраслей национального права;

– продолжить техническое регулирование обращения и использования информации посредством лицензирования, стандартизации, аттестации и сертификации.

Проведенный анализ административно-правового регулирования позволил определить следующие направления, по которым развивается национальное законодательство в анализируемой сфере:

– детализация и дифференциация юридической ответственности за противоправные деяния, совершенные в информационном пространстве или в отношении информационных прав граждан;

– создание надлежащих нормативных условий для скорейшего импортозамещения технологий в промышленности и других сферах.

Развитие административно-правового сопровождения процессов информатизации и цифровизации общества – важнейший элемент реализации государственной информационной политики. Общие принципы такого административно-правового сопровождения можно изложить следующим образом:

1) административно-правовое регулирование не должно противоречить иным нормам национального права, а также положениям международных актов;

2) неотвратимые правовые негативные последствия для участника информационных отношений – нарушителя административного запрета или требования;

3) обеспечение административно-правовыми мерами генеральной цели реализации российской информационной политики, каковым является цифровой и технологический суверенитет.

Список литературы

1. *Белова Н. Н., Староверова Д. Ю.* Оценка методов обеспечения стабильной работы информационных систем в условиях киберугроз // Технологии в управлении. – 2025. – Т. 2. – № 2. – С. 5–14.

2. *Дубень А. К.* Правовое обеспечение информационной безопасности в системе информационного права в Российской Федерации : дисс ... канд. юрид. наук. – Москва, 2023.

3. *Киян М. В., Павлов Н. В.* Правовые аспекты административной ответственности за распространение фейковых новостей в Российской Федерации // Вестник экономики и права. – 2025. – № 100. – С. 29–35.

4. *Коровина Я. Е.*, *Кочетков И. А.*, *Митрясов А. С.* Особенности использования терминов «информационная безопасность» и «кибербезопасность» // Информационные технологии в науке, бизнесе и образовании. Возможности и безопасность технологий искусственного интеллекта : материалы XV

Международной научно-практической конференции студентов, аспирантов и молодых ученых (Москва, 14–15 ноября 2024 г.). – М. : МГЛУ, 2025. – С. 92–97.

5. *Лемешко Д. В.* Безопасность технологий искусственного интеллекта на объектах критической информационной инфраструктуры // Информационные технологии в науке, бизнесе и образовании. Возможности и безопасность технологий искусственного интеллекта : материалы XV Международной научно-практической конференции студентов, аспирантов и молодых ученых (Москва, 14–15 ноября 2024 г.). – М. : МГЛУ, 2025. – С. 121–125.

6. *Оносов А. Г.* Какие технологии применяются для обеспечения информационной безопасности и защиты данных на предприятиях и в организациях? // Управление качеством. – 2025. – № 2 (252). – С. 18–23.

7. *Пьянков М. О., Никитина Е. Ю.* Защита информации в условиях удаленной работы сотрудников // Актуальные проблемы информационной безопасности : сборник статей. – Вып. 1. – Пермь, 2024. – URL: http://www.psu.ru/files/docs/science/books/sbornik-2024.pdf

8. *Савенков А. Н.* Государство и право в период кризиса современной цивилизации. – М., 2020.

9. *Староверова Е. Н.* Обеспечение информационной безопасности в работе критической информационной инфраструктуры // Экономика и предпринимательство. – 2025. – № 1 (174). – С. 1109–1112.