УДК 338.24

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аникина А.А.[1]

студент,

Елецкий государственный университет им. И.А. Бунина,

Елец, Россия

Лазарева Ю.Л.

студент,

Елецкий государственный университет им. И.А. Бунина,

Елец, Россия

Аннотация. В статье рассматриваются экономические механизмы, заложенные в российском законодательстве о защите данных государственных информационных систем. Показано, что требования федеральных законов № 149-ФЗ, № 152-ФЗ и № 187-ФЗ превращают обеспечение кибербезопасности из желательной меры в обязательную статью бюджетных расходов. На основе анализа механизма категорирования информационных систем, политики импортозамещения (распоряжение Правительства РФ № 2580-р) и функционирования ГосСОПКА делается вывод о соразмерности затрат и потенциальных рисков: чем выше класс защищённости системы, тем значительнее необходимые вложения. Одновременно создаётся гарантированный спрос на отечественное программное обеспечение и формируется общерыночное благо - информация о киберугрозах, доступная всем участникам системы. В конечном счёте правовое регулирование в этой области укрепляет технологический

[1] ***Научный руководитель: Воробьев С.В.,*** *канд. пед. наук, доцент, доцент кафедры экономики и управления им. Н.Г. Нечаева, ФГБОУ ВО «Елецкий государственный университет им. И.А. Бунина», ЕГУ им. И.А. Бунина, Россия, г. Елец*

суверенитет страны, а затраты на безопасность данных приобретают характер инвестиций, а не чистых издержек.

Ключевые слова: государственные информационные системы, защита данных, экономико-правовой анализ, информационная безопасность, критическая информационная инфраструктура, импортозамещение в IT, категорирование информационных систем.

DATA SECURITY IN PUBLIC INFORMATION SYSTEMS

Anikina A.A.[2]

Student,

Yelets State University named after I.A. Bunin,

Yelets, Russia

Lazareva Yu.L.

Student,

Yelets State University named after I.A. Bunin,

Yelets, Russia

Abstract. The article examines the economic mechanisms embedded in Russian legislation on the protection of data in state information systems. It is shown that the requirements of Federal Laws No. 149-FZ, No. 152-FZ, and No. 187-FZ transform cybersecurity from a desirable measure into a mandatory budget item. Based on the analysis of the mechanism for categorizing information systems, the import substitution policy (Government Order No. 2580-r), and the functioning of the State Information Security System, it is concluded that the costs and potential risks are commensurate: the higher the security class of the system, the greater the necessary investments. At the same time, a guaranteed demand for domestic

[2] ***Scientific supervisor: Vorobyev S.V.,*** *Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of the Department of Economics and Management named after N.G. Nechaev, Bunin Yelets State University, YelSU, Russia, Yelets*

software is created, and a market-wide benefit is formed: information about cyber threats that is accessible to all system participants. Ultimately, legal regulation in this area strengthens the country's technological sovereignty, and data security costs become investments rather than pure expenses.

Keywords: state information systems, data protection, economic and legal analysis, information security, critical information infrastructure, import substitution in IT, categorization of information systems.

В условиях цифровой трансформации государственного управления защита данных в государственных информационных системах (ГИС) перестала быть исключительно технической задачей. Федеральный закон № 149 и ряд подзаконных актов закрепили положение, согласно которому финансирование кибербезопасности становится для госорганов обязательной статьёй расходов - аналогично содержанию помещений или оплате коммунальных услуг [3]. Такой подход формирует устойчивый спрос на отечественные IT-продукты и одновременно минимизирует бюджетные потери от сбоев в работе критически важных систем.

Формирование затрат на безопасность данных прямо вытекает из требований федеральных законов в сфере информации и персональных данных [2, 3]. Любой государственный орган, эксплуатирующий информационную систему, обязан предусматривать в бюджете средства на сертифицированные средства защиты информации, аттестацию объектов информатизации и содержание профильных специалистов. Требование о назначении ответственного за обработку персональных данных влечёт расходы на обучение такого сотрудника, его регулярную аттестацию и оплату труда [2]. Аналогично обстоит ситуация с криптографическими средствами: их закупка и обслуживание включаются в себестоимость для коммерческих операторов ГИС либо покрываются из бюджета для

государственных учреждений, что в конечном счёте влияет на формирование налогооблагаемой базы этих операторов.

Экономическим стимулом выступает политика импортозамещения, закреплённая распоряжением Правительства РФ от 23.09.2020 № 2580-р [7]. Для государственных информационных систем вводится обязанность постепенной замены иностранного программного обеспечения российскими аналогами. Фактический переход на отечественную операционную систему или офисный пакет сопровождается единовременными затратами: переобучение персонала, миграция данных, доработка интеграционных решений. В долгосрочной перспективе такие меры создают гарантированный рынок для российских вендоров - «Лаборатория Касперского» , «1С:Предприятие» и других. Через систему госзаказа государство субсидирует развитие национальной IT-отрасли, и указанные расходы приобретают характер инвестиций в технологический суверенитет, а не чистых издержек.

Принцип соразмерности затрат и возможных последствий реализован в механизме категорирования информационных систем [1, 5]. Чем выше класс защищённости системы, тем строже меры по её охране. Для информационной системы управления распределительными сетями в энергетике или системы обработки данных оборонного предприятия устанавливается первый (высший) класс защищённости. Экономическая логика здесь определяется тем, что сбой или утечка данных в таких системах способны повлечь остановку целых отраслей, многомиллиардные убытки и прямые угрозы национальной безопасности. Соответственно, затраты на защиту подобной системы оказываются на порядок выше, чем для информационной системы районного архива. Законодательное регулирование заставляет государство и операторов критической информационной инфраструктуры распределять ресурсы экономически обоснованно: чем выше риск, тем дороже защита.

Отдельный экономический эффект создаётся государственной системой обнаружения и предупреждения кибератак (ГосСОПКА), введённой Указом Президента РФ № 31с [6]. Данная система аккумулирует информацию о компьютерных инцидентах в едином центре, обрабатывает её и распространяет сигналы об актуальных угрозах. Для частных компаний, подключённых к ГосСОПКА, возникает прямая экономическая выгода: снижаются собственные издержки на расследование атак и анализ новых угроз. При фиксации новой вредоносной программы в государственном секторе все участники системы получают оперативные данные о её признаках и способах блокировки без необходимости самостоятельного исследования. Таким образом, формируется общее благо в виде доступной информации об угрозах. Оно способствует экономии ресурсов как частного, так и государственного секторов.

Российское законодательство в области безопасности данных государственных информационных систем выстраивает целостную экономическую модель. В рамках этой модели защита информации выступает не как желательная инициатива, а как обязательное условие функционирования, подкреплённое бюджетными обязательствами. Одновременно создаются экономические стимулы для развития отечественной IT-индустрии и формируются механизмы коллективного противодействия угрозам. Совокупность перечисленных мер в конечном счёте укрепляет технологический суверенитет страны [4].

Анализ показывает, что при внешней стройности описанной экономико-правовой модели в ней сохраняются внутренние противоречия, которые пока не нашли законодательного разрешения. Конкретно необходимо обратить внимание на перечисленные ниже противоречия

1. Обязательное финансирование мер безопасности вступает в конфликт с режимом экономии бюджетных средств, декларируемым как приоритет государственной политики - на практике это приводит к

формальному выполнению требований при фактической нехватке ресурсов на полноценную защиту.

2. Механизм категорирования, обоснованный теоретически, на уровне рядовых государственных систем часто работает как бюрократическая процедура: класс защищённости присваивается исходя из шаблонных критериев, а не реального профиля угроз, что искажает саму идею соразмерности затрат и рисков.

3. Политика импортозамещения, безусловно необходимая для технологического суверенитета, одновременно создаёт ситуацию, при которой отечественные вендоры оказываются в положении «гарантированного получателя госзаказа» без достаточной конкуренции, что способно снижать стимулы к инновациям и качеству.

4. ГосСОПКА, формируя общерыночное благо в виде информации об угрозах, порождает классическую проблему «безбилетника» -частные компании получают выгоду без соразмерного участия в финансировании самой системы.

Таким образом, российская модель безопасности данных в ГИС эффективна как рамочное регулирование, но её практическая реализация требует дальнейшей настройки: увязки обязательных расходов с реальными бюджетными возможностями, дебюрократизации категорирования, внедрения конкурсных механизмов в импортозамещение и разработки справедливой модели распределения издержек на коллективную защиту от киберугроз.

Библиографический список

1. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон № 187-ФЗ : [принят Государственной Думой 19 июля 2017 г. : одобрен Советом Федерации 21 июля 2017 г.] : (ред. от 10.07.2023)

URL: https://www.consultant.ru/document/cons_doc_LAW_220886/ (дата обращения: 23.05.2026) .

2.О персональных данных : Федеральный закон № 152-ФЗ : [принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г.] :(ред. от 21.02.2024) . URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 24.05.2026) .

3.Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : [принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г.] : (ред. от 29.12.2025). - URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 22.05.2026) .

4. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ № 646 : (ред. от 19.06.2021). - URL: https://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 23.05.2026) .

5.О правилах категорирования объектов критической информационной инфраструктуры : Постановление Правительства РФ № 1746. - URL: https://www.consultant.ru/document/cons_doc_LAW_311385/ (дата обращения: 22.05.2026) .

6.О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак : Указ Президента РФ № 31с. - URL: https://www.consultant.ru/document/cons_doc_LAW_142050/ (дата обращения: 21.05.2026) .

7. Об утверждении перечня российских программ для ЭВМ и баз данных : Распоряжение Правительства РФ № 2580-р. - URL: https://www.consultant.ru/document/cons_doc_LAW_363501/ (дата обращения: 23.05.2026) .