

*Анисимов С.И.
магистрант 3 курса,
ИГСУ РАНХиГС,
г. Москва, РФ*

**АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ПУТИ СОВЕРШЕНСТВОВАНИЯ
СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

***Аннотация:** Стремительное развитие информационно-коммуникационных технологий и цифровизация отраслей российской экономики значительно повышают риски реализации угроз информационной безопасности. В статье приведены результаты анализа современного состояния системы обеспечения информационной безопасности Российской Федерации и предложены меры по ее совершенствованию.*

***Ключевые слова:** Информационная безопасность, кибербезопасность, защита информации, угрозы безопасности, персональные и биометрические данные.*

***Annotation:** The rapid development of information and communication technologies and the digitalization of sectors of the Russian economy significantly increase the risks of the implementation of information security threats. The results of the analysis of the current state of the information security system of the Russian Federation are presented and measures for its improvement are proposed.*

***Keywords:** Information security, cybersecurity, information protection, security threats, personal and biometric data.*

Стремительное развитие информационно-коммуникационных технологий (ИКТ) и цифровизация общества, с одной стороны, и рост

международной напряжённости, с другой, значительно повышают риски информационной безопасности (ИБ) Российской Федерации. Злоумышленники постоянно совершенствуют свои методы, применяя новые тактики и техники атак, используют социальную инженерию, ИИ, машинное обучение, «программы-вымогатели». Компьютерные атаки становятся всё сложнее, а их исполнителями выступают не только хакерские группировки, но и идеологически мотивированные сообщества людей (например, «ИТ-армия Украины»), координируемые спецслужбами иностранных государств.

В этих условиях особую актуальность приобретают вопросы совершенствования обеспечения ИБ РФ, в первую очередь в части защиты цифровых активов и электронных информационных ресурсов и систем.

В соответствии с положениями Доктрины информационной безопасности РФ¹ создана и функционирует система обеспечения ИБ РФ (СОИБ) – совокупность сил обеспечения ИБ (подразделений и должностных лиц государственных органов, органов местного самоуправления, организаций, уполномоченных в области ИБ), и используемых ими правовых, организационных, технических и других средств.

Состав СОИБ РФ определяется Президентом РФ. Ее организационную основу составляют: Совет Федерации; Государственная Дума; Правительство РФ; Совет Безопасности; межведомственные органы; федеральные органы исполнительной и судебной власти; Центральный банк РФ (Банк России); Военно-промышленная комиссия РФ; органы исполнительной власти субъектов РФ; органов местного самоуправления.

Участниками СОИБ РФ являются: собственники и эксплуатанты объектов критической информационной инфраструктуры; средства массовой информации и массовых коммуникаций; организации финансового рынка; операторы связи, информационных систем (ИС); организации, осуществляющие деятельность по созданию и эксплуатации ИС и сетей связи,

¹ Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. N 50. ст. 7074.

по разработке, производству и эксплуатации средств защиты информации и оказанию услуг в области ИБ; образовательные и иные организации, а также граждане, которые в соответствии с законодательством РФ участвуют в решении задач по обеспечению ИБ.

Отдельное положение или концепция о СОИБ РФ в настоящее время отсутствуют. Правовую основу СОИБ РФ составляют: федеральные законы от 28.06.2014 N 172-ФЗ «О стратегическом планировании в Российской Федерации»², от 28.12.2010 N 390-ФЗ «О безопасности»³, от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»⁴, от 27.07.2006 N 152-ФЗ «О персональных данных»⁵, Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне»⁶ и др., Указы Президента РФ от 15.01.2013 N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»⁷, от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»⁸ и др., а также постановления Правительства РФ, приказы органов государственной власти, уполномоченных в области обеспечения ИБ.

Анализ нормативно правовых актов (НПА) в области обеспечения ИБ, а также основных направлений обеспечения ИБ РФ показывает, что основными

² Федеральный закон от 28.06.2014 N 172-ФЗ (ред. от 13.07.2024) «О стратегическом планировании в Российской Федерации» // Российская газета. 03.07.2014. N 146.

³ Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 10.07.2023) «О безопасности» // Собрание законодательства РФ. 2011. N 1. Ст. 2.

⁴ Федеральный закон от 26.07.2017 N 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета. 31.07.2017. N 167.

⁵ Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 28.02.2025) «О персональных данных» // Российская газета. 29.07.2006. N 165.

⁶ Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.08.2024) «О государственной тайне» // Собрание законодательства РФ. 1997. N 41.

⁷ Указ Президента РФ от 15.01.2013 N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (выписка) // Собрание законодательства РФ. 21.01.2013. N 3. Ст. 178.

⁸ Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» // Собрание законодательства РФ. 2008. № 12. Ст. 1110.

структурно-функциональными элементами (подсистемами) СОИБ РФ являются:

- система стратегического планирования обеспечения ИБ РФ;
- система правового регулирования и стандартизации в области ИБ РФ; государственная система ГосСОПКА;
- система обеспечения целостности, устойчивости и безопасности функционирования сети связи общего пользования и российского сегмента сети «Интернет»;
- система защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации ограниченного доступа и распространения;
- государственная система защиты информации в РФ от иностранной технической разведки и от ее утечки по техническим каналам;
- система защиты персональных и биометрических данных;
- система защиты граждан от информации, распространение которой запрещено или ограничено законами РФ;
- государственная система противодействия противоправным деяниям, совершаемым с использованием ИКТ;
- система лицензирования деятельности, аккредитации, аттестации и сертификации в области ИБ;
- система научной и образовательной деятельности в области ИБ.

Действует система НПА, которыми определены полномочия и функции субъектов СОИБ, для эффективного осуществления их деятельности реализованы соответствующие ИС и технические средства.

Стратегический анализ информационной сферы РФ позволяет определить актуальные проблемы в области обеспечения ИБ РФ на современном этапе:

децентрализованная система управления обеспечением ИБ, отсутствие единого государственного органа, ответственного за обеспечение ИБ РФ;

слабая систематизация и отсутствие кодификации системы НПА информационной направленности [1, с. 9, 2];

технологическое отставание электронной промышленности, зависимость от зарубежных технологий и недостаточное инвестирование в информационные технологии и ИБ;

уход иностранных компаний и потеря доступа к зарубежным ИКТ и средствам обеспечения ИБ;

снижение уровня школьного образования и слабая подготовка в вузах, отток кадров высшей квалификации за рубеж;

освоение информационного пространства для ведения военных действий, рост числа компьютерных атак [];

внедрение программных «закладок» в программное обеспечение;

рост числа преступлений с использованием ИКТ и изменение тактики и техник их совершения.

В области обеспечения ИБ РФ существуют риски масштабных утечек персональных данных, финансовых потерь граждан и организаций, распространения дезинформации, пропаганды и манипуляций общественным мнением и сознанием граждан, дестабилизации российского общества, проведения успешных масштабных компьютерных атак на объекты критической информационной инфраструктуры РФ и выхода их из строя, управляемого нарушения функционирования государственных и корпоративных ИС, потери государственного управления экономическими и социальными процессами в стране.

Для совершенствования государственного регулирования в области обеспечения ИБ РФ и личной безопасности граждан, а также для снижения рисков негативных событий целесообразно проведение мероприятий по следующим направлениям:

общесистемные меры: разработка положения о системе обеспечения ИБ РФ и положений о ее подсистемах; создание государственной системы

обеспечения кибербезопасности с централизацией полномочий у единого государственного органа; проведения инвентаризации и оценки всех государственных и муниципальных цифровых активов и информационных ресурсов; оценки уязвимостей ИС и рисков кибербезопасности; формулирование целей, задач, основных направлений и приоритетов государственной политики в области обеспечения безопасности РФ в киберпространстве;

совершенствование правового регулирования общественных отношений в информационной сфере в части: введения актуальных терминов в области информационной и кибербезопасности; систематизации и кодификации НПА информационной направленности; разработки национальной стратегии кибербезопасности; доработки правовых государственных ИС, содержащих правовые акты и стандарты информационной направленности в части совершенствования семантического поиска, составления поисковых образов документов для отбора документов по тематикам, направлениям деятельности, защищаемым объектам;

создание условий для безопасного внедрения цифровых и платежных технологий и обеспечения технологического суверенитета в части: разработки собственных технологий и средств обработки и хранения данных, своей электронной компонентной базы, микроэлектроники, вычислителей в ходе программ по импортозамещению; цифровой трансформации российских организаций и предприятий при неукоснительном соблюдении требований кибербезопасности и применении эффективных сертифицированных средств защиты; привлечения государственных и частных инвестиций в разработку новых прорывных отечественных продуктов и сервисов в области ИТ и киберзащиты, включая технологии генеративного и сильного искусственного интеллекта; стимулирования спроса на отечественные продукты и сервисы в области ИТ и киберзащиты, в том числе через государственные заказы;

совершенствование системы защиты объектов информационной инфраструктуры РФ от компьютерных атак в части: создания и внедрения национальной платформы кибербезопасности РФ; разработки и создания средств защиты информации на основе перспективных технологий (искусственного интеллекта, аналитики больших данных и др.);

защита прав потребителей цифровых услуг и повышение уровня доверия к цифровым технологиям в части: совершенствования механизма защиты персональных и биометрических данных; повышения уровня зрелости граждан и организаций по вопросам кибербезопасности и цифровой гигиены; совершенствования системы противодействия преступности с применением ИКТ; развития института страхования цифровых активов, информационных ресурсов и рисков;

совершенствование кадрового обеспечения в части: проведения учета (переписи) специалистов, занятых в данной области, прогнозирования требуемого количества работников и необходимых специальностей на среднесрочный и долгосрочный периоды; повышения качества их подготовки в профессиональных и высших учебных заведениях; ускорения разработки и принятия новых, актуальных вызовов и угроз образовательных и профессиональных стандартов; внедрения новой модели образования «университеты как центры компетенций»; создания национальной платформы знаний в области ИБ;

совершенствование научного обеспечения ИБ в части: разработки проактивных алгоритмов обнаружения и предупреждения компьютерных атак; математического моделирования элементов национальной информационной инфраструктуры, ее функционирования в условиях осуществления компьютерных атак; создания учебно-тренировочных средств, цифровых двойников ИС и развертыванию сети киберполигонов для проведения учений специалистов, тестирования средств защиты и обновлений безопасности.

Таким образом, создана и функционирует система обеспечения ИБ РФ, нормативными правовыми актами определены полномочия и функции субъектов системы и ее подсистем, для эффективного осуществления их деятельности реализованы соответствующие информационные системы и технические средства, однако в связи с постоянным развитием ИКТ и появлением новых вызовов и угроз ИБ РФ и личной безопасности граждан.

Использованные источники

1. Бачило, И. Л. О подходах к систематизации и кодификации информационного законодательства / И. Л. Бачило // Систематизация и кодификация информационного законодательства / Отв. ред. И.Л. Бачило. Сб. науч. работ. – М.: ИГП РАН – изд-во Канон+, 2015 – 216 с.

2. Перспективы кодификации законодательства в сферах информационных технологий и цифрового развития // Совет Федерации Федерального Собрания Российской Федерации. – URL: <http://council.gov.ru/activity/activities/roundtables/158388/> (дата обращения 25.05.2025).

3. Специалисты РКН в 2024 году отразили почти 11 тыс. DDoS-атак на российские ресурсы // Агентство "Интерфакс". – URL: <https://www.interfax.ru/russia/1005362> (дата обращения: 14.01.2025)/