УДК 04.056

СОВРЕМЕННЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И ЭФФЕКТИВНОСТЬ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Лужкова А.С., студентка гр. ИБс-211, V курс
Научный руководитель: Прокопенко Е.В., к.ф.-м.н., доцент
Кузбасский государственный технический университет
имени Т.Ф. Горбачева, г. Кемерово

Аннотация. В статье рассматриваются современные угрозы безопасности информационных систем в условиях цифровой трансформации и роста числа киберинцидентов. Проанализированы основные виды актуальных угроз, включая несанкционированный доступ, вредоносное программное воздействие, атаки на объекты критической информационной инфраструктуры и использование технологий искусственного интеллекта в противоправных целях. Особое внимание уделено нормативно-правовому обеспечению информационной безопасности в Российской Федерации, а также требованиям к защите информации, установленным федеральным законодательством и подзаконными актами. Исследуется роль криптографических средств защиты информации как ключевого элемента обеспечения конфиденциальности, целостности и аутентичности данных. Обоснована необходимость комплексного подхода к защите информационных систем, сочетающего правовые, организационные и технические меры. Сделан вывод о том, что эффективность криптографических механизмов определяется не только их алгоритмической стойкостью, но и корректностью внедрения, управлением ключевой информацией и соответствием актуальным моделям угроз.

Ключевые слова. Информационная безопасность; информационные системы; киберугрозы; критическая информационная инфраструктура; криптографические средства защиты информации; персональные данные; правовое регулирование; цифровая трансформация; защита информации; технологическая независимость.

В условиях стремительной цифровизации государственного управления, экономики и социальной сферы вопросы обеспечения безопасности информационных систем приобретают приоритетное значение. Информация становится стратегическим ресурсом, а устойчивость информационной инфраструктуры – одним из ключевых факторов национальной безопасности. Правовые основы защиты информации в Российской Федерации закреплены на конституционном уровне: Конституция Российской Федерации гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, а также защиту информации о частной жизни лица [1, ст. 23]. Развитие данных положений получило отражение в федеральном законодательстве, регулирующем отношения в сфере обработки и защиты информации.

Федеральный закон «Об информации, информационных технологиях и о защите информации» устанавливает принципы правового регулирования информационных отношений и определяет обязанности обладателей информации по обеспечению ее защиты [3, ст. 16]. В свою очередь, Федеральный закон «О персональных данных» закрепляет необходимость принятия организационных и технических мер по предотвращению несанкционированного доступа к персональным данным и иных неправомерных действий [2, ст. 19]. Указанные нормативные акты формируют базовую модель правового обеспечения информационной безопасности, ориентированную на минимизацию рисков утечки, модификации и уничтожения данных.

Современные угрозы безопасности информационных систем характеризуются усложнением методов кибератак, широким применением вредоносного программного обеспечения, социальной инженерии, а также использованием технологий искусственного интеллекта как в целях защиты, так и в целях совершения противоправных действий. В научных исследованиях подчеркивается, что правовое обеспечение информационной безопасности должно учитывать динамику цифровых трансформаций и развитие новых технологических рисков [12, с. 45]. Особое внимание уделяется перспективам применения технологий искусственного интеллекта для выявления аномалий, предотвращения атак и повышения адаптивности систем защиты [13, с. 18].

На фоне роста числа инцидентов в сфере критической информационной инфраструктуры усиливаются требования к обеспечению технологической независимости и устойчивости информационных систем. В этой связи принимаются дополнительные меры нормативного характера, направленные на укрепление безопасности критической информационной инфраструктуры и повышение уровня защищенности государственных информационных ресурсов [5, п. 1; 6, п. 2]. Существенную роль играет и деятельность уполномоченных органов по установлению обязательных требований и сертификации средств защиты информации [7; 8].

В системе мер обеспечения информационной безопасности ключевое место занимают криптографические средства защиты информации, позволяющие обеспечить конфиденциальность, целостность и аутентичность данных. Их применение регламентируется специальными требованиями, в том числе в сфере защиты персональных данных и информационных систем общего пользования [9; 10]. Эффективность криптографических механизмов во многом определяется корректностью их внедрения, соответствием установленным стандартам и уровню актуальных угроз.

Анализ современных угроз безопасности информационных систем и оценка эффективности криптографических средств защиты информации представляют собой актуальную научную и практическую задачу. Комплексный подход, сочетающий правовые, организационные и технические меры, позволяет сформировать устойчивую модель защиты информации в условиях цифровой трансформации и возрастающей киберугрозы.

Современные угрозы безопасности информационных систем носят комплексный и многоуровневый характер, что обусловлено как технологическим развитием, так и расширением сферы цифрового взаимодействия государства, бизнеса и граждан. Информационные системы становятся объектами целенаправленных атак, направленных на нарушение конфиденциальности, целостности и доступности информации. В соответствии с положениями Федерального закона «Об информации, информационных технологиях и о защите информации» защита информации представляет собой принятие правовых, организационных и технических мер, направленных на предотвращение неправомерного доступа, уничтожения, модификации и распространения информации [3, ст. 16].

Одной из наиболее распространённых угроз является несанкционированный доступ к данным, включая персональные данные граждан. Федеральный закон «О персональных данных» прямо возлагает на оператора обязанность принимать необходимые и достаточные меры для обеспечения безопасности персональных данных при их обработке [2, ст. 19]. Однако на практике реализация данных требований осложняется постоянной эволюцией методов кибератак, включая фишинг, эксплуатацию уязвимостей программного обеспечения, атаки типа «отказ в обслуживании» (DDoS), а также внедрение вредоносного кода в цепочки поставок программных продуктов.

Таблица 1. Соотношение угроз и криптографических мер защиты

Современная угроза	Возможные последствия	Криптографические меры защиты
Несанкционированный доступ	Утечка конфиденциальной информации	Шифрование данных, аутентификация, управление ключами
Модификация данных	Искажение или подмена информации	Электронная подпись, хэш-функции
Перехват трафика	Компрометация передаваемых сведений	Криптографические протоколы защищённой связи
Атаки на КИИ	Нарушение функционирования систем	Комплексное применение СКЗИ, сертифицированные средства защиты

Особую опасность представляют угрозы в отношении объектов критической информационной инфраструктуры (КИИ), поскольку их компрометация способна повлечь значительный ущерб обороноспособности, экономике и общественной безопасности государства. В целях повышения уровня защищённости КИИ принимаются дополнительные меры нормативного характера, включая установление требований к обеспечению технологической независимости и безопасности [5, п. 1]. Кроме того, усиление мер по обеспечению информационной безопасности закреплено на уровне указов Президента Рос-

сийской Федерации, предусматривающих комплекс организационных и технических мероприятий [6, п. 2].

Значительная роль в формировании устойчивой системы защиты информации принадлежит уполномоченным органам, устанавливающим обязательные требования к защите информации и процедурам сертификации средств защиты. Так, приказами ФСТЭК России утверждены требования по защите информации в государственных информационных системах и положения о системе сертификации средств защиты информации [7; 8]. Данные нормативные акты направлены на унификацию подходов к оценке защищённости информационных систем и подтверждению соответствия применяемых средств установленным стандартам безопасности.

В условиях усложнения угроз возрастает значение криптографических средств защиты информации (СКЗИ). Их применение обеспечивает реализацию базовых свойств информационной безопасности: конфиденциальности (посредством шифрования), целостности (за счёт использования механизмов хэширования и электронной подписи) и аутентичности (посредством криптографической идентификации и аутентификации). Порядок применения СКЗИ при защите персональных данных регламентирован специальными нормативными актами, устанавливающими состав и содержание организационных и технических мер [9]. Аналогичные требования предусмотрены и для информационных систем общего пользования [10].

Эффективность криптографических средств защиты информации определяется не только стойкостью используемых алгоритмов, но и корректностью их внедрения в архитектуру информационной системы. Нарушения в управлении ключевой информацией, ошибки конфигурации, использование устаревших протоколов или отсутствие своевременного обновления программного обеспечения существенно снижают уровень защищённости даже при формальном соблюдении нормативных требований. В этой связи особое значение приобретает системный подход к обеспечению информационной безопасности, включающий анализ угроз, моделирование нарушителя и выбор адекватных средств защиты.

Современные исследования подчёркивают необходимость интеграции интеллектуальных технологий в процессы защиты информации. Применение технологий искусственного интеллекта позволяет выявлять аномалии сетевого трафика, прогнозировать потенциальные инциденты и автоматизировать реагирование на атаки [13, с. 19]. Вместе с тем правовое обеспечение информационной безопасности должно учитывать риски, связанные с использованием новых технологий, включая вопросы ответственности, сертификации и контроля за их применением [12, с. 47].

Таким образом, современные угрозы безопасности информационных систем требуют постоянного совершенствования как нормативно-правовой базы, так и технических механизмов защиты. Криптографические средства защиты информации выступают ключевым элементом обеспечения безопасности, однако их эффективность достигается только при условии комплекс-

ного применения в сочетании с организационными мерами, сертифицированными средствами защиты и регулярной оценкой актуальных угроз. Формирование устойчивой и адаптивной системы информационной безопасности является необходимым условием обеспечения прав граждан, стабильности функционирования государственных институтов и технологического суверенитета Российской Федерации.

Список литературы:

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г.: основной закон РФ // Собрание законодательства Российской Федерации. — 1993. — № 32, ст. 2922.

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. — 2006. — № 31, ст. 3435.

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. — 2006. — № 31, ст. 4422.

4. Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ // Собрание законодательства Российской Федерации. — 2002. — № 52, ст. 5042.

5. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации. — 24.02.2026.

6. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. — 24.02.2026.

7. Приказ ФСТЭК России от 03.04.2018 № 55 (ред. 19.09.2022) «Об утверждении Положения о системе сертификации средств защиты информации» // ФСТЭК России.

8. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // ФСТЭК России.

9. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных… с использованием средств криптографической защиты информации» // ФСБ России.

10. Приказ ФСБ России и ФСТЭК России от 31.08.2010 № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» // СПС «КонсультантПлюс».

11. Методические рекомендации ФСТЭК России по подготовке планов при установлении уровня опасности КИИ (2021) // ФСТЭК России.

12. Дубень А. К. Отдельные аспекты правового обеспечения информационной безопасности в Российской Федерации // Закон и право. 2022. №7. URL: https://cyberleninka.ru/article/n/otdelnye-aspekty-pravovogo-obespecheniya-informatsionnoy-bezopasnosti-v-rossiyskoy-federatsii (дата обращения: 24.02.2026).

13. Мещеряков Р. В., Мельников С. Ю., Пересыпкин В. А., Хорев А. А. Перспективные направления применения технологий искусственного интеллекта при защите информации // Вопросы кибербезопасности. 2024. №4 (62). URL: https://cyberleninka.ru/article/n/perspektivnye-napravleniya-primeneniya-tehnologiy-iskusstvennogo-intellekta-pri-zaschite-informatsii (дата обращения: 24.02.2026).