КОРТУНКОВА В. С., КУЗЬМИНА У. В.
ОЦЕНКА ЗАЩИТЫ ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ В РАМКАХ ГОСТ Р 57580.1

УДК 004.738.5, ГРНТИ 50.37.23

Оценка защиты информации финансовых организаций в рамках ГОСТ Р 57580.1

В. С. Кортункова, У. В. Кузьмина

Магнитогорский государственный технический университет им. Г.И. Носова, г. Магнитогорск

В условиях стремительного развития цифровых технологий финансовые организации Российской Федерации выполняют ключевую функцию в обеспечении стабильности экономики. Защита персональных данных, финансовых операций и конфиденциальной информации становится важнейшей задачей, а выполнение требований ГОСТ Р 57580.1 является необходимым условием обеспечения информационной безопасности. В статье анализируются процессы аудита финансовых организаций в рамках данного стандарта, описываются этапы оценки соответствия и потенциальные угрозы информационной безопасности. Новизна исследования заключается в рассмотрении практических аспектов оценки защиты информации финансовых организаций в соответствии с актуальными нормативными требованиями.

Ключевые слова: *информационная безопасность, финансовые организации, аудит, ГОСТ Р 57580.1, регуляторные требования, защита информации, киберугрозы*

Assessment of information security of financial organizations within the framework of GOST R 57580.1

V. S. Kortunkova, U. V. Kuzmina

Nosov Magnitogorsk State Technical University, Magnitogorsk

In the context of the rapid development of digital technologies, financial institutions in the Russian Federation perform a key function in ensuring the stability of the economy. The protection of personal data, financial transactions and confidential information is becoming an essential task, and meeting the requirements of GOST R 57580.1 is a prerequisite for ensuring information security. The article analyzes the audit processes of financial organizations within the framework of this standard, describes the stages of compliance assessment and potential threats to information security. The novelty of the research lies in the consideration of practical aspects of assessing the information security of financial organizations in accordance with current regulatory requirements.

Keywords: *information security, financial organizations, audit, GOST R 57580.1, regulatory requirements, information security, cyber threats*

Введение

В процессе управления информационной безопасностью, как и любым направлением целенаправленной деятельности, необходимы разработка и принятие эффективных решений, обеспечивающих достижения поставленных целей. В условиях развитой информационной инфраструктуры объектов информатизации, большого числа потенциальных целей атак нарушителей, разнородной деятельности подразделений организаций, оценка соответствия обеспечения информационной безопасности связана с выполнением большего объема работ, и следовательно, с пропорциональными финансовыми расходами, требует тщательного анализа процесса их действия, ожидаемых и возможных последствий.

Финансовые организации ежедневно обрабатывают значительные объемы конфиденциальных данных, что повышает их уязвимость перед киберугрозами. В условиях цифровизации экономики обеспечение безопасности данных является не только вопросом соблюдения нормативных требований, но и фактором устойчивости организации. ГОСТ Р 57580.1 устанавливает требования к обеспечению информационной безопасности в кредитных и некредитных финансовых организациях, регламентируя порядок аудита и анализа защищенности информационных систем [2]. Основная цель данного аудита — оценка текущего уровня защиты, выявление несоответствий нормативным требованиям и анализ потенциальных угроз.

Особенности аудита информационной безопасности в финансовых организациях

Аудит информационной безопасности в финансовом секторе имеет принципиальные отличия от аналогичных процедур, проводимых в других отраслях. Эти различия продиктованы как регуляторными особенностями, так и спецификой функционирования финансовых организаций, обладающих высокой степенью цифровизации, интеграции с государственными информационными системами и жёсткими требованиями к защите данных.

Одним из ключевых факторов, определяющих специфику аудита в банках и кредитно-финансовых учреждениях, является наличие обязательных требований со стороны Центрального банка Российской Федерации. В отличие от большинства коммерческих организаций, где стандарты ИБ чаще всего носят рекомендательный характер, в банковской сфере аудит должен проводиться в соответствии с несколькими слоями нормативных документов. Как отмечается в исследовании, «главной особенностью проведения аудита в кредитно-финансовой сфере является необходимость проведения аудита не только согласно требованиям стандартов ГОСТ, но и согласно нормативным документам Банка России» [6].

В частности, аудит информационной безопасности в банках должен учитывать положения стандартов СТО БР ИББС, что расширяет рамки применяемых требований. «Аудит ИБ организации банковской сферы РФ должен проводиться в соответствии с требованиями стандартов СТО БР ИББС-

1.0, СТО БР ИББС-1.1 и СТО БР ИББС-1.2» [6]. В то время как организации в других секторах могут ограничиваться применением ISO/IEC 27001 или внутренними корпоративными стандартами, финансовым структурам требуется соответствие целому комплексу отраслевых регламентов.

Дополнительным отличием является характер взаимодействия с ГОСТ Р 57580.1, который был разработан специально с учётом особенностей финансовых организаций. Как подчёркивают специалисты, «ГОСТ Р 57580.1-2017 будет наиболее полезен аудиторам, работающим непосредственно с финансовыми организациями» [10].

Сравнительный анализ стандартов оценки безопасности информации

Для оценки эффективности аудита в рамках ГОСТ Р 57580.1 важно рассмотреть его отличия от других стандартов. В рамках исследовательской работы был проведен сравнительный анализ российского стандарта с аналогичными международными стандартами, такими как ISO/IEC 27001 и PCI DSS. Данный анализ позволил выявить особенности подходов к обеспечению безопасности данных в различных отраслях и определить, насколько ГОСТ Р 57580.1 адаптирован к специфике финансового сектора. Сравнительный анализ также помог обосновать выбор данного стандарта как наиболее эффективного. Результаты анализа представлены в Таблице 1.

Таблица 1. Результаты сравнительного анализа стандартов

Критерий сравнения	**ГОСТ Р 57580.1**	**ISO/IEC 27001**	**PCI DSS**
Область применения	Финансовые организации РФ	Все отрасли	Организации, работающие с платежными картами
Регулирующий орган	Центральный банк РФ	Международная организация по стандартизации (ISO)	Совет по стандартам безопасности PCI
Цель стандарта	Защита данных в финансовом секторе	Общая система управления информационной безопасностью	Защита данных держателей карт
Детализация требований	Высокая, с учетом специфики финансового сектора	Общие требования	Высокая, но ограниченная областью платежных данных
Обязательность	Обязателен для российских финансовых организаций	Добровольный, но широко применяемый	Обязателен для участников платежных систем
Подход к оценке	Регулярный аудит и отчетность в ЦБ РФ	Внутренний и внешний аудит	Прохождение сертификационного аудита

Результаты сравнения стандартов показали, что аудит по ГОСТ Р 57580.1 обладает высокой степенью детализации и учитывает специфику отечественного финансового сектора, что делает его наиболее релевантным для российских финансовых организаций. Данный вид оценки соответствия можно выделить как наиболее эффективный по ряду причин:

1. Регулируемость и соответствие нормативным требованиям. ГОСТ Р 57580.1 является официальным стандартом, утвержденным Центральным банком России, что делает его обязательным для исполнения финансовыми организациями. В отличие от многих международных стандартов, таких как ISO/IEC 27001, данный регламент адаптирован к российскому законодательству и учитывает специфические требования к защите информации в финансовом секторе.

2. Комплексный подход к аудиту. Методология аудита по ГОСТ Р 57580.1 охватывает не только анализ технических мер защиты, но и проверку организационных аспектов, процессов управления рисками, соответствия нормативным актам и устойчивости к угрозам информационной безопасности. Это позволяет получить всестороннюю оценку уровня безопасности финансовой организации.

3. Четко определенные критерии оценки. В отличие от более гибких международных стандартов, ГОСТ Р 57580.1 содержит четкие количественные и качественные критерии соответствия. Стандарт указывает минимальные требования к защите данных, уровню резервирования систем, управлению доступом и мониторингу угроз. Это снижает субъективность при проведении аудита и обеспечивает единообразие требований.

4. Обязательность аудита и контроль со стороны регулятора. Выполнение требований ГОСТ Р 57580.1 контролируется Центральным банком РФ, что относит аудит не просто к формальной процедуре, а служит инструментом повышения защищенности. Финансовые организации обязаны предоставлять отчетность и устранять выявленные несоответствия в установленные сроки. Это гарантирует не просто соответствие стандарту, но и постоянное совершенствование механизмов информационной безопасности.

5. Ориентация на финансовый сектор. Множество международных стандартов информационной безопасности являются универсальными, в то время как ГОСТ Р 57580.1 разрабатывался специально для финансовых организаций. Это свидетельствует о том, что, что в нем учтены специфические угрозы и требования отрасли, включая защиту платежных систем, предотвращение мошенничества и минимизацию финансовых рисков.

6. Интеграция с другими методологиями и стандартами. ГОСТ Р 57580.1 совместим с подобными стандартами информационной безопасности, такими как ISO/IEC 27001 и NIST SP 800-53, а также с требованиями Центрального банка РФ (802-П, 821-П, 851-П, 757-П). Данные интеграции позволят организациям одновременно соблюдать как российские, так и международные нормы, создавая многоуровневую систему защиты.

Заключение

Аудит финансовых организаций в рамках ГОСТ Р 57580.1 представляет собой не только регуляторное требование, но и стратегический инструмент повышения уровня информационной безопасности. Его проведение позволяет выявлять потенциальные угрозы, оценивать эффективность существующих механизмов защиты и разрабатывать стратегии по устранению уязвимостей.

Эффективность аудита обусловлена его комплексностью: анализируются как технические меры защиты, так и организационные аспекты управления информационной безопасностью. Внедрение рекомендаций, полученных в ходе аудита, не только минимизирует риски утечек данных и финансовых потерь, но и способствует повышению доверия клиентов и партнеров.

Таким образом, оценка защищенности в соответствии с ГОСТ Р 57580.1 играет ключевую роль в обеспечении устойчивости финансовых организаций к современным угрозам информационной безопасности, позволяя создать безопасную среду для обработки конфиденциальной информации и поддерживать стабильность финансового сектора в условиях цифровой трансформации.

Список использованных источников и литературы:

1. Аудит информационной безопасности финансовых организаций: не только затраты [Электронный ресурс]: Цибит – https://www.cibit.ru/stati-ekspertov/audit-informacionnoj-bezopasnosti-finansovyx-organizacij/ (дата обращения: 15.03.2025).

2. ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.

3. Баранкова И. И., Семавина Е. А., Михайлова У. В. Аудит информационной безопасности промышленных предприятий, направленный на оценку соответствия требованиям российского и международного законодательства // Вестник УРФО. Безопасность в информационной сфере. — 2022. — №. 3 (45). — С. 76-82.

4. Баранкова И. И., Сергеев С. С. Моделирование систем защиты информации на основе теории графов // Актуальные проблемы современной науки, техники и образования. Тезисы 80-й международной научно-технической конференции. — 2022. — Том № 1. — С. 373.

5. Михайлова У. В., Афанасьева М. В. Аудит информационной безопасности предприятия ООО "Ансер" // Актуальные проблемы современной науки, техники и образования. Тезисы 77-й международной научно-технической конференции. — 2019. — Том № 1. — С. 417-418.

6. Фомин А. В., Резниченко С. А. «Особенности аудита информационной безопасности на предприятиях кредитно-финансовой сферы» // Вестник науки. — 2024.

7. Гильманова Э. А., Ахметшина Р. И. «Роль аудита информационной безопасности в жизненном цикле системы обеспечения информационной

безопасности объектов критической информационной инфраструктуры» // Форум молодых учёных. — 2022. — №2(66).

8. Сиротский А. А. «Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов» // Безопасность информационных технологий. 2021. Т. 28. №3. С. 103–117.

9. Баранова Е. М. и др. «Применение методов статистики в ходе аудита информационных систем» // Известия Тульского государственного университета. Технические науки. 2022. №10. С. 245–253.

10. Ситская, А. В. Вопросы автоматизации проведения аудита в соответствии с ГОСТ р 57580.2-2018 / А. В. Ситская, В. А. Табакаева, В. В. Селифанов // Интерэкспо Гео-Сибирь. – 2021. – Т. 6. – С. 268-275.

List of references

1. Cibit, "Information security audit for financial organizations: Not just costs," [Online]. Available: https://www.cibit.ru/stati-ekspertov/audit-informacionnoj-bezopasnosti-finansovyx-organizacij/ (Accessed: Mar. 15, 2025).

2. *GOST R 57580.1-2017*, "Security of financial (banking) operations. Information security of financial organizations. Basic set of organizational and technical measures," 2017.

3. I. I. Barankova, E. A. Semavina, and U. V. Mikhailova, "Information security audit for industrial enterprises aimed at assessing compliance with Russian and international legislation," *Bulletin of Ural Federal District. Information Security*, no. 3 (45), pp. 76–82, 2022.

4. I. I. Barankova and S. S. Sergeev, "Modeling of information protection systems based on graph theory," in *Proc. 80th Int. Sci. Tech. Conf. Current Problems of Modern Science, Technology, and Education*, vol. 1, 2022, p. 373.

5. U. V. Mikhailova and M. V. Afanasyeva, "Information security audit of 'Anser' LLC," in *Proc. 77th Int. Sci. Tech. Conf. Current Problems of Modern Science, Technology, and Education*, vol. 1, 2019, pp. 417–418.

6. A. V. Fomin and S. A. Reznichenko, "Features of information security audit in credit and financial sector enterprises," *Science Bulletin*, 2024.

7. E. A. Gilmanova and R. I. Akhmetshina, "The role of information security audit in the lifecycle of critical information infrastructure security systems," *Forum of Young Scientists*, no. 2(66), 2022.

8. A. A. Sirotsky, "Formalized model of an organization's information security audit for compliance with standards," *Information Technology Security*, vol. 28, no. 3, pp. 103–117, 2021.

9. E. M. Baranova et al., "Application of statistical methods in information systems audit," *News of Tula State University. Technical Sciences*, no. 10, pp. 245–253, 2022.

10. A. V. Sitskaya, V. A. Tabakaeva, and V. V. Selifanov, "Automation of audit in accordance with GOST R 57580.2-2018," *Interexpo Geo-Siberia*, vol. 6, pp. 268–275, 2021.