DOI 10.37882/2223-2966.2025.06-2.09

РАЗРАБОТКА МЕТОДИКИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ ФИНАНСОВОГО СЕКТОРА

DEVELOPMENT OF A METHODOLOGY FOR CONDUCTING AN INFORMATION SECURITY AUDIT IN FINANCIAL SECTOR ORGANIZATIONS

I. Gorbachev
M. Rytov
O. Golembiovskaya
E. Gorbachev

Summary. The number of successful cyber attacks in the financial sector is growing year by year. The more comprehensive and complete an object's security system is, the higher its security against external interference will be. At the same time, in real business conditions, it is possible to assess the completeness of protection only through regular checks and periodic in-depth audits of the effectiveness of the entire information security system. The article proposes a methodology for conducting an information security audit in financial sector organizations, which allows for the most comprehensive assessment of the facility's information security system, based on comprehensive requirements of GOST R 57580. The compliance assessment algorithm presented in the framework of the methodology helps simplify the audit procedure for financial organizations and make it more systematic.

Keywords: audit, financial sector, information security.

Горбачев Иван Владимирович
Аспирант,
Брянский государственный технический университет
ivan1.ru@mail.ru
Рытов Михаил Юрьевич
Доцент,
Брянский государственный технический университет
rmy@tu-bryansk.ru
Голембиовская Оксана Михайловна
Кандидат технических наук,
Брянский государственный технический университет
golembiovskaya@tu-bryansk.ru
Горбачев Егор Павлович
Финансовый университет при Правительстве РФ
me@septembernocturne.ru

Аннотация. Количество успешных кибератак в финансовом секторе год от года растет. Чем более комплексной и полной будет система защиты объекта, тем выше будет его защищенность от внешнего вмешательства, при этом в реальных условиях функционирования бизнеса оценить полноту защиты можно только посредством регулярных проверок и периодического глубокого аудита эффективности всей системы защиты информации. В рамках статьи предложена методика проведения аудита информационной безопасности в организациях финансового сектора, которая позволяет наиболее комплексно оценить систему защиты информации объекта, опираясь на всеобъемлющий по требованиям ГОСТ Р 57580. Представленный в рамках методики алгоритм проведения оценки соответствия требованиям помогает упростить процедуру аудита для финансовых организаций и сделать ее более системной.

Ключевые слова: аудит, финансовый сектор, информационная безопасность.

Информатизация как явление в настоящее время затронула все процессы нашей жизни. Не является исключением и сфера финансовой и банковской деятельности. Именно в данной сфере перевод в цифровой формат происходит быстрее всего, поскольку деятельность связана с большим количеством оформляемой документации, также с удобством обслуживаемых клиентов, большинство из которых предпочитают электронные платежные системы наличному расчету.

По данным Positive Technologies [1] количество успешных кибератак в финансовом секторе год от года растет. Среди последствий атак чаще других выделяются утечки данных (64 %), а также остановка работы отдельных сервисов или ключевых бизнес-процессов (40 %). Подавляющее большинство утечек содержат персональные данные клиентов и коммерческую информацию организаций. Кроме того, среди утечек нередко можно обнаружить номера платежных карт и учетные данные, в утечках страховых компаний присутствует и медицинская информация.

Чем более комплексной и полной будет система защиты объекта, тем выше будет его защищенность от внешнего вмешательства, при этом в реальных условиях функционирования бизнеса оценить полноту защиты можно только посредством регулярных проверок и периодического глубокого аудита эффективности всей системы защиты информации.

Процедура аудита позволяет не только оценить, насколько защищена инфраструктура объекта, но и при

необходимости в ходе проверки внести в нее коррективы, закрывая обнаруженные пробелы.

Нормативно-правовая база определяет ключевые принципы проведения аудита информационной безопасности в организациях финансового сектора. Анализ отечественных нормативных правовых актов в этой сфере позволяет выявить основные требования, в соответствии с которыми производится процедура аудита, а также отметить ключевые особенности его реализации.

На основе анализа требований нормативно-правовой базы и научной литературы [2; 3; 4; 5; 6; 7; 8, с. 90; 9, с. 183; 10; с. 195] в отношении проведения аудита ИБ организаций финансового сектора сделан вывод о том, что аудит информационной безопасности организаций, связанных с финансовой и банковской деятельностью целесообразно производить посредством оценки их соответствия требованиям ГОСТ Р 57580.

По результатам оценки направлений защиты, описанных в вышеуказанном ГОСТ производится итоговая оценка соответствия, которая включает в себя качественную оценку уровня соответствия процессов системы защиты информации, а также числовую итоговую оценку соответствия защиты информации. После чего принимается решение о необходимости совершенствования системы защиты информации

Далее будет кратко описан порядок реализации каждого из этапов оценки.

Стандарт 57580.1–2017 определяет три уровня защиты информации, минимальный, стандартный, усиленный.

В финансовой организации формируются один или несколько контуров безопасности, для которых может быть установлен разный уровень защиты информации. Уровень защиты информации финансовой организации для конкретного контура безопасности устанавливается нормативными актами Банка России на основе:

- вида деятельности финансовой организации, состава предоставляемых финансовых услуг, реализуемых бизнес-процессов и (или) технологических процессов в рамках данного контура безопасности;
- объема финансовых операций;
- размера организации, отнесения финансовой организации к категории малых предприятий и микропредприятий;
- значимости финансовой организации для финансового рынка и национальной платежной системы.

На основе Положений Банка России [4; 5; 6; 7] разработана анкета (таблица 1), позволяющая однозначно на основе специфики деятельности организации сделать вывод о необходимом уровне защиты информации в соответствии со стандартом. Важно последовательно ответить на все вопросы с первого до получения результата об актуальном уровне защиты, а не выбирать отдельные вопросы, поскольку анкета простроена в иерархическом порядке.

Таблица 1.

Фрагмент анкеты оценки уровня защиты контур(-ов) безопасности объекта для организаций финансового сектора

№ п/п	Вопрос / варианты	
1	Объект относится к системно значимым кредитным организациям / кредитным организациям, выполняющим функции оператора услуг платежной инфраструктуры системно значимых платежных систем / кредитным организациям, значимым на рынке платежных услуг?	
	Да	Нет
	Для объекта актуален 1 уровень защиты	Перейдите к вопросу 2
2	Объект участвует в предоставлении операционных услуг и услуг платежного клиринга (ОПКЦ)?	
	Да	Нет
	Для объекта актуален 1 уровень защиты	Перейдите к вопросу 3
..	…	…
11	Объект относится к банковским платежным агентам (субагентам) и привлекается в целях осуществления переводов денежных средств?	
	Да	Нет
	Для объекта актуален 3 уровень защиты	

Использование анкеты позволяет установить уровень защиты контур(-ов) безопасности объекта, не прибегая к анализу отдельных положений Банка России.

Оценка выбора финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему ЗИ финансовой организации, полноты реализации организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему организации и управления ЗИ финансовой организации, а также оценка защиты информации на этапах жизненного цикла АС финансовой организации осуществля-

ются на основе таблиц, представленных в рамках ГОСТ Р 57580.1–2017. Для оптимизации и упрощения данных этапов и рассмотрения таблиц стандарта, рекомендуется разработать расширенные таблицы-анкеты, в которых каждая из мер дополнена конкретными рекомендациями, позволяющими оценить выполнено ли данное требование и составить план совершенствования системы защиты информации объекта, если ряд необходимых требований не реализован. В таблице 2 приведен фрагмент оценочной таблицы-анкеты для раздела «Оценка выбора финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему ЗИ финансовой организации».

Каждую из мер необходимо оценить:

0 — не выбрана (при отсутствии у проверяемой организации свидетельств ее реализации),

1 — выбрана (при предъявлении проверяемой организацией свидетельств ее реализации).

Условное обозначение в рамках таблицы:

— «О» — реализация путем применения организационной меры защиты информации;
— «Т» — реализация путем применения технической меры защиты информации;
— «Н» — реализация является необязательной.

После заполнения анкет числовые значения оценки каждого из трех процессов рассчитываются по формулам, описанным в рамках ГОСТ Р 57580.1–2017.

Итоговая оценка соответствия ГОСТ Р 57580 включает в себя качественную оценку уровня соответствия процессов системы защиты информации (на основе показателя E_i) и числовую оценку соответствия системы защиты информации рассматриваемому ГОСТу (R).

Показатель E_i рассчитывается по каждому процессу отдельно по формуле 1.

$$E_i = \frac{E_{\text{пзи}_i} + \left(0,2E_{\text{п}_i} + 0,4E_{p_i} + 0,25E_{k_i} + 0,15E_{c_i}\right)}{2}, \quad (1)$$

где $E_{\text{пзи}_i}$ — числовое значение оценки, рассчитанной по итогам этапа «Оценка выбора финансовой организа-

Таблица 2.

Фрагмент анкеты оценки выбора финансовой организацией организационных и технических мер ЗИ (фрагмент)

Обозначение и № меры	Содержание мер системы защиты информации	Уровень защиты информации			Отметка о реализации (1/0)
		1	2	3	
Процесс 1 «Обеспечение защиты информации при управлении доступом»					
УЗП — Управление учетными записями и правами субъектов логического доступа					
Базовый состав мер по организации и контролю использования учетных записей субъектов логического доступа					
УЗП.1	Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями	Т	Т	Т	
		Реализуется путем регистрации персонифицированной учетной записи с помощью технических решений таких как Active Directory, встроенных в АС, СУБД, ОС, средств виртуализации подсистемы управления доступом, средств для реализации персонифицированного доступа, например: Secret Net Studio (для Windows) Secret Net LSP (для Linux). Или его аналогами.			
УЗП.2	Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа	0	0	Т	
		Реализуется путем закрепления меры в Политике управления доступом, должны быть закреплены порядок, периодичность контроля состава и прав учетных записей субъектов доступа с формированием отчетного документа. А также назначен ответственный за предоставление доступа к системе (например, администратор ИБ), данная обязанность закрепляется в должностной инструкции.		Мера реализуется применением систем управления идентификацией и аутентификацией (систем IdM), например Ankey IDM или аналоги. При этом необходим обмен данными с системой учета персонала в организации (например, 1С).).	
…	…	…		…	…

цией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему ЗИ финансовой организации». отдельно по каждому из процессов.

$E_п$, $E_р$, $E_к$, $E_с$ — числовые значение оценок, рассчитанных по итогам этапа «Оценка полноты реализации организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему организации и управления ЗИ финансовой организации» для *i*-того процесса.

i — номер процесса, для которого рассчитывается E_i.

В случае если на объекте несколько контуров безопасности, то E_i вычисляется отдельно для каждого контура, а потом складывается с учетом весовых коэффициентов для разных уровней защиты.

В случае если на объекте три контура с 1, 2 и 3 уровнем защиты, то показатель E_i вычисляется по формуле 2, если два контура с 1 и 2 уровнем защиты, то показатель E_i вычисляется по формуле 3, если два контура с 1 и 3 уровнем защиты, то показатель E_i вычисляется по формуле 4, если два контура со 2 и 3 уровнем защиты, то показатель E_i вычисляется по формуле 5.

$$E_i = 0,6E_{1_i} + 0,3E_{2_i} + 0,1E_{3_i} \quad (2)$$

$$E_i = 0,7E_{1_i} + 0,3E_{2_i} \quad (3)$$

$$E_i = 0,8E_{1_i} + 0,2E_{3_i} \quad (4)$$

$$E_i = 0,6E_{2_i} + 0,4E_{3_i} \quad (5)$$

где E_{1_i} — контур с первым уровнем защиты, E_{2_i} — контур со вторым уровнем защиты, E_{3_i} — контур с третьим уровнем защиты.

Качественная оценка уровня соответствия процессов системы защиты информации вычисляется на основе таблицы, представленной в ГОСТ Р 57580.2–2018 (таблица 3).

Таблица 3.

Качественная оценка уровня соответствия процессов системы ЗИ

E_i	Уровень соответствия
$E_i = 0$	нулевой
$0 < E_i \leq 0,5$	первый
$0,5 < E_i \leq 0,7$	второй
$0,7 < E_i \leq 0,85$	третий
$0,85 < E_i \leq 0,9$	четвертый
$0,9 < E_i \leq 1$	пятый

Числовую итоговую оценку соответствия защиты информации *R* вычисляют по формуле (6) как среднеарифметическое значение оценок E_i для всех процессов системы ЗИ и оценки $E_{AC,}$ полученной на этапе «Оценка защиты информации на этапах жизненного цикла АС финансовой организации».

$$R = \frac{\sum_{i=1}^{T} E_i + E_{AC}}{T + 1} - 0,01Z, \quad (6)$$

где *E* — оценка соответствия защиты информации *i*-го процесса системы защиты информации;

i — номер процесса системы защиты информации;

T — количество процессов системы защиты информации. вошедших в область оценки соответствия защиты информации.

E_{AC} — оценка полноты применения организационных и технических мер защиты информации на этапах жизненного цикла АС финансовой организации.

Z — количество нарушений защиты информации. выявленных членами проверяющей группы в процессе оценки соответствия защиты информации. Перечень возможных нарушений представлен в приложении Б ГОСТ Р 57580.2 — 2018.

В случае, если полноту применения организационных и технических мер защиты информации на этапах жизненного цикла АС финансовой организации не оценивают ($E_{AC} = 0$), то в знаменателе формулы (6) указывают только значение Т.

Числовые оценки соответствия защиты информации R превышающие числовое значение 0.85, соответствуют уровню, рекомендуемому Банком России.

По результатам проведенной оценки должны быть заполнены отчетные формы, шаблоны которых представлены в приложениях А и В ГОСТ Р 57580.2–2018.

Таким образом, описанная методика проведения аудита информационной безопасности в организациях финансового сектора позволяет наиболее комплексно оценить систему защиты информации объекта, опираясь на всеобъемлющий по требованиям ГОСТ Р 57580. Представленный алгоритм значительно упростит процедуру проведения аудита в соответствии с рассматриваемым ГОСТом, а также создаст базу для автоматизации проведения данной оценки.

ЛИТЕРАТУРА

1. Киберугрозы финансовой отрасли [Электронный ресурс] — режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (Дата обращения: 15.02.2025)
2. ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (утв. и введен в действие Приказом Росстандарта от 08.08.2017 N 822-ст).
3. ГОСТ Р 57580.2-2018 Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия (утв. и введен в действие Приказом Росстандарта от 22.03.2018 N 156-ст).
4. Приказ Минцифры России № 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации».
5. Положение Банка России от 25 июля 2022 г. N 802-П «О требованиях к защите информации в платежной системе Банка России».
6. Положение Банка России от 4 июня 2020 г. № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».
7. Положение Банка России от 17 апреля 2019 г. N 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».
8. Гулак М. Л. Аудит информационной безопасности. Прикладная статистика: учебное пособие / М.Л. Гулак, М.Ю. Рытов, О.М. Голембиовская. — Москва: Ай Пи Ар Медиа, 2020. — 121 с. — ISBN 978-5-4497-0713-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/97630.html (дата обращения: 06.02.2025).
9. Швецов, А.Н. К оценке процесса распространения дезинформации в социальных сетях / А.Н. Швецов // Вестник МАНЭБ. — 2023. — Т. 28, № 3. — С. 89–91. — EDN ANSSBA.
10. Жидко Е.А. Методология исследований информационной безопасности экологически опасных и экономически важных объектов: монография / Е.А. Жидко. — Воронеж: Воронежский государственный архитектурно-строительный университет, ЭБС АСВ, 2015. — 183 с. — ISBN 978-5-89040-535-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/55011.html (дата обращения: 06.02.2025).
11. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие / Ю.Н. Сычев. — Саратов: Вузовское образование, 2018. — 195 с. — ISBN 978-5-4487-0128-3. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/72345.html (дата обращения: 06.02.2025).