ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р 57580.2— 2018**

# Безопасность финансовых (банковских) операций

# ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

## Методика оценки соответствия

Издание официальное

Москва
Стандартинформ
2018

## Предисловие

1 РАЗРАБОТАН Центральным банком Российской Федерации (Банком России) и Научно-производственной фирмой «КРИСТАЛЛ» (НПФ «КРИСТАЛЛ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 122 «Стандарты финансовых операций»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 г. № 156-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)*

## Содержание

## Введение

Развитие и укрепление банковской системы Российской Федерации, развитие и обеспечение стабильности финансового рынка Российской Федерации и национальной платежной системы являются целями деятельности Центрального банка Российской Федерации (Банка России) [1]. Одним из условий реализации целей деятельности кредитных организаций, некредитных финансовых организаций Российской Федерации, а также субъектов национальной платежной системы (далее при совместном упоминании — финансовые организации) является обеспечение необходимого и достаточного уровня защиты информации, а также сохранение этого уровня в течение длительного времени.

Требования к содержанию базового состава организационных и технических мер защиты информации, реализующих установленные Банком России требования к обеспечению защиты информации при осуществлении банковской деятельности и деятельности в сфере финансовых рынков, установлены ГОСТ Р 57580.1.

Способом проверки соответствия защиты информации является оценка выбора и реализации финансовой организацией организационных и технических мер защиты информации в соответствии с требованиями ГОСТ Р 57580.1 (далее — оценка соответствия защиты информации) независимой организацией, обладающей необходимым уровнем компетенции и имеющей лицензию на деятельность по технической защите конфиденциальной информации как минимум на один из следующих видов работ и услуг:

- контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
- проектирование в защищенном исполнении средств и систем информатизации;
- установка, монтаж, испытания, ремонт средств защиты информации [программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации].

Основными целями настоящего стандарта являются:

- установление единых требований к методике и оформлению результатов оценки соответствия защиты информации финансовой организации;
- установление способов оценки выбора и реализации финансовой организацией организационных и технических мер защиты информации в соответствии с требованиями ГОСТ Р 57580.1;
- определение итоговой оценки соответствия защиты информации финансовой организации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Безопасность финансовых (банковских) операций**

# ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

**Методика оценки соответствия**

Security of financial (banking) operations. Information protection of financial organizations. Conformity assessment methods

**Дата введения — 2018—09—01**

## 1 Область применения

Настоящий стандарт устанавливает требования к методике и оформлению результатов оценки соответствия защиты информации (ЗИ) финансовой организации при выборе и реализации организационных и технических мер ЗИ в соответствии с требованиями ГОСТ Р 57580.1, применяемых финансовой организацией для реализации требований к обеспечению ЗИ, установленных нормативными актами Банка России.

Требования к методике и оформлению результатов оценки соответствия ЗИ, устанавливаемые настоящим стандартом, предназначены для использования организациями, осуществляющими оценку соответствия ЗИ кредитных организаций, некредитных финансовых организаций, указанных в Федеральном законе [1] (статья 76.1, часть 1), а также субъектов национальной платежной системы, не являющихся кредитными организациями.

Область применения настоящего стандарта, определяющая обязанность финансовых организаций проводить оценку соответствия ЗИ для конкретной совокупности объектов информатизации, в том числе автоматизированных систем (АС), используемых финансовыми организациями для предоставления финансовых услуг, устанавливается в нормативных актах Банка России путем включения нормативной ссылки на настоящий стандарт, приводимой на основании статьи 27 Федерального закона [2].

Настоящий стандарт устанавливает требования к методике оценки соответствия ЗИ, применение которой обеспечивает определение итоговой оценки соответствия ЗИ финансовой организации требованиям ГОСТ Р 57580.1.

Настоящий стандарт предназначен для применения путем включения нормативных ссылок на него и/или прямого использования устанавливаемых в нем требований в нормативных актах Банка России, во внутренних документах финансовых организаций, а также в договорах.

## 2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 34.11 Информационная технология. Криптографическая защита информации. Функция хэширования

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

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный

**Издание официальное**

стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

## 3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 57580.1, а также следующие термины с соответствующими определениями:

3.1 **оценка соответствия защиты информации:** Процесс оценки выбора и реализации финансовой организацией организационных и технических мер защиты информации в соответствии с требованиями ГОСТ Р 57580.1, выполняемой проверяющей организацией.

3.2 **проверяющая организация:** Организация, проводящая оценку соответствия ЗИ финансовой организации и являющаяся независимой от проверяемой организации и от организаций, осуществлявших или осуществляющих оказание услуг проверяемой организации в области реализации информатизации и защиты информации (в части внедрения и/или сопровождения систем, средств, процессов информатизации и защиты информации, используемых в финансовой организации в период проведения проверки и входящих в область оценки соответствия ЗИ).

3.3 **проверяющая группа:** Группа, состоящая из сотрудников проверяющей организации, а также (при необходимости) иных лиц, уполномоченных проверяющей организацией проводить оценку соответствия защиты информации финансовой организации.

3.4 **проверяемая организация:** Финансовая организация, в отношении которой проводится оценка соответствия защиты информации.

## 4 Сокращения

В настоящем стандарте использованы следующие сокращения:

АС — автоматизированная система;

ЗИ — защита информации;

МНИ — машинные носители информации;

ПО — программное обеспечение;

СВТ — средство вычислительной техники.

## 5 Назначение и структура настоящего стандарта

Раздел 6 содержит описание общей методологии оценки соответствия ЗИ.

Раздел 7 содержит:

- требования к методике оценки соответствия ЗИ;
- описание методологии определения итоговой оценки соответствия ЗИ.

Раздел 8 содержит требования к оформлению результатов оценки соответствия ЗИ.

В приложении А приведена форма листов для сбора свидетельств оценки соответствия ЗИ, которые оформляются как приложения к отчету по результатам оценки соответствия ЗИ.

В приложении Б приведен примерный перечень нарушений ЗИ, которые могли или могут привести к инцидентам ЗИ, наносящим ущерб финансовой организации или ее клиентам.

В приложении В приведены формы таблиц оценок, которые оформляются как приложения к отчету по результатам оценки соответствия ЗИ.

## 6 Общие положения

6.1 В область оценки соответствия ЗИ входит совокупность объектов информатизации, включая АС и приложения, используемые финансовыми организациями для выполнения бизнес-процессов и/или технологических процессов, связанных с предоставлением финансовых и банковских услуг, а так-

же услуг по осуществлению переводов денежных средств (далее при совместном упоминании — АС). Область оценки соответствия ЗИ должна совпадать с областью применения ГОСТ Р 57580.1. Количество и выборку проверяемых подразделений, объектов информатизации, АС и СВТ, входящих в область оценки соответствия ЗИ, определяет проверяющая организация самостоятельно с учетом предложений проверяемой организации и обеспечения достоверности итоговой оценки соответствия ЗИ.

Проверяемая организация для планирования мероприятий по проведению оценки соответствия ЗИ предоставляет проверяющей организации (проверяющей группе) достоверные исходные данные и документальные свидетельства, связанные с количеством проверяемых подразделений, объектов информатизации, АС и СВТ, входящих в область оценки соответствия ЗИ[1)].

6.2 Оценку соответствия ЗИ осуществляют по следующим направлениям:

- выбор финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему ЗИ финансовой организации (ГОСТ Р 57580.1—2017, раздел 7);
- полнота реализации организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему организации и управления ЗИ финансовой организации (ГОСТ Р 57580.1—2017, раздел 8);
- обеспечение ЗИ на этапах жизненного цикла АС финансовой организации (ГОСТ Р 57580.1—2017, раздел 9).

6.3 Оценку выбора финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему ЗИ финансовой организации, осуществляют отдельно для следующих процессов ЗИ:

- процесс 1 «Обеспечение защиты информации при управлении доступом»;
- процесс 2 «Обеспечение защиты вычислительных сетей»;
- процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»;
- процесс 4 «Защита от вредоносного кода»;
- процесс 5 «Предотвращение утечек информации»;
- процесс 6 «Управление инцидентами защиты информации»;
- процесс 7 «Защита среды виртуализации»;
- процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств».

6.4 Оценку выбора финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему ЗИ финансовой организации, для процесса 1 «Обеспечение защиты информации при управлении доступом» осуществляют отдельно для следующих подпроцессов системы ЗИ:

- «Управление учетными записями и правами субъектов логического доступа»;
- «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»;
- «Защита информации при осуществлении физического доступа»;
- «Идентификация, классификация и учет ресурсов и объектов доступа».

6.5 Оценку выбора финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему ЗИ финансовой организации, для процесса 2 «Обеспечение защиты вычислительных сетей» осуществляют отдельно для следующих подпроцессов системы ЗИ:

- «Сегментация и межсетевое экранирование вычислительных сетей»;
- «Выявление вторжений и сетевых атак»;
- «Защита информации, передаваемой по вычислительным сетям»;
- «Защита беспроводных сетей».

6.6 Оценку выбора финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему ЗИ финансовой организации, для процесса 6 «Управление инцидентами защиты информации» осуществляют отдельно для следующих подпроцессов системы ЗИ:

- «Мониторинг и анализ событий защиты информации»,

---

[1)] Рекомендуемые типовые действия при проведении оценки соответствия приведены в стандарте [3], раздел 6.

- «Обнаружение инцидентов защиты информации и реагирование на них».

6.7 Оценку полноты реализации организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему организации и управления ЗИ финансовой организации, осуществляют отдельно для каждого из процессов ЗИ, указанных в 6.3, по следующим направлениям:

- направление 1 «Планирование процесса системы защиты информации» (см. ГОСТ Р 57580.1—2017, подраздел 8.2);
- направление 2 «Реализация процесса системы защиты информации» (см. ГОСТ Р 57580.1—2017, подраздел 8.3);
- направление 3 «Контроль процесса системы защиты информации» (см. ГОСТ Р 57580.1—2017, подраздел 8.4);
- направление 4 «Совершенствование процесса системы защиты информации» (см. ГОСТ Р 57580.1—2017, подраздел 8.5).

6.8 Оценку ЗИ на этапах жизненного цикла АС финансовой организации осуществляют в случаях распространения (в соответствии с требованиями нормативных актов Банка России) области применения ГОСТ Р 57580.1 на АС, используемые финансовой организацией для выполнения отдельных видов бизнес-процессов или технологических процессов.

6.9 Для оценки полноты реализации процессов системы ЗИ используют следующую качественную модель оценивания:

а) **нулевой уровень соответствия:** организационные и технические меры процесса системы ЗИ не реализуются или реализуются в единичных случаях. Общие подходы (способы) реализации организационных и технических мер процесса системы ЗИ не установлены. Контроль и совершенствование реализации организационных и технических мер процесса системы ЗИ не осуществляются,

б) **первый уровень соответствия:** организационные и технические меры процесса системы ЗИ реализуются в незначительном количестве, бессистемно и/или эпизодически. Общие подходы (способы) реализации организационных и технических мер процесса системы ЗИ не установлены. Контроль и совершенствование реализации организационных и технических мер процесса системы ЗИ не осуществляются;

в) **второй уровень соответствия:** организационные и технические меры процесса системы ЗИ реализуются в значительном количестве на постоянной основе. Общие подходы (способы) реализации организационных и технических мер процесса системы ЗИ установлены в единичных случаях. Реализация организационных и технических мер процесса системы ЗИ осуществляется на усмотрение исполнителя. Контроль и совершенствование реализации организационных и технических мер процесса системы ЗИ практически не осуществляются;

г) **третий уровень соответствия:** организационные и технические меры процесса системы ЗИ реализуются в значительном количестве на постоянной основе в соответствии с общими подходами (способами), установленными в финансовой организации. Контроль и совершенствование реализации организационных и технических мер процесса системы ЗИ осуществляются бессистемно и/или эпизодически;

д) **четвертый уровень соответствия:** организационные и технические меры процесса системы ЗИ реализуются в полном объеме на постоянной основе в соответствии с общими подходами (способами), установленными в финансовой организации. В финансовой организации в основном реализованы контроль и совершенствование реализации организационных и технических мер процесса системы ЗИ;

е) **пятый уровень соответствия:** организационные и технические меры процесса системы ЗИ реализуются в полном объеме на постоянной основе в соответствии с общими подходами (способами), установленными в финансовой организации. В финансовой организации реализованы постоянный контроль и необходимое своевременное совершенствование реализации организационных и технических мер процесса системы ЗИ.

6.10 Оценку соответствия процессов (подпроцессов) системы ЗИ и направлений ЗИ осуществляют в соответствии со следующим общим подходом.

6.10.1 Оценку, характеризующую выбор финансовой организацией каждой из организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ, входящих в систему ЗИ финансовой организации и установленных в ГОСТ Р 57580.1—2017 (раздел 7), $E_{МЗИ}$ определяют путем использования следующих числовых значений:

- 0 — не выбрана (при отсутствии у проверяемой организации свидетельств выбора),
- 1 — выбрана (при предъявлении проверяемой организацией свидетельств выбора).

Значения оценок заносят в формы, приведенные в таблицах В.1 — В.8 (приложение В), для каждого из процессов системы ЗИ.

6.10.2 Оценку, характеризующую полноту реализации каждой из организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ, входящих в систему организации и управления ЗИ финансовой организации и установленных в ГОСТ Р 57580.1—2017 (раздел 8), $E_{МОУ}$ определяют путем использования следующих числовых значений:

- 0 — полностью не реализуется;
- 0,5 — реализуется не в полном объеме;
- 1,0 — реализуется в полном объеме.

Значения оценок заносят в формы, приведенные в таблицах В.10 — В.13 (приложение В), для каждого направления ЗИ системы организации и управления ЗИ и каждого процесса системы ЗИ.

6.10.3 Оценку, характеризующую реализацию каждой из организационных и технических мер ЗИ, применяемых на этапах жизненного цикла АС и установленных в ГОСТ Р 57580.1—2017 (раздел 9), $E_{МАС}$ определяют путем использования следующих числовых значений:

- 0 — полностью не реализуется;
- 0,5 — реализуется не в полном объеме;
- 1,0 — реализуется в полном объеме.

Значения оценок заносят в форму, приведенную в таблице В.9 (приложение В).

6.11 Перед определением оценок $E_{МЗИ}$, $E_{МОУ}$ и $E_{МАС}$ для соответствующих процессов (подпроцессов) системы ЗИ и направлений ЗИ проверяющей группой совместно с проверяемой организацией может быть определен перечень неоцениваемых областей оценки соответствия ЗИ (процессов системы ЗИ, подпроцессов системы ЗИ, направлений ЗИ, мер ЗИ).

В перечень неоцениваемых областей оценки соответствия ЗИ могут быть включены организационные и технические меры ЗИ:

- непосредственно связанные с информационными технологиями, не используемыми в проверяемой организации;
- реализация которых не является необходимой для нейтрализации актуальных угроз безопасности, определенных в модели угроз и нарушителей безопасности информации финансовой организации. При этом проверяющая группа должна проверить актуальность и обоснованность действующей модели угроз и нарушителей безопасности информации проверяемой организации.

Перечень неоцениваемых областей оценки соответствия ЗИ с обоснованием их исключения из области оценки соответствия ЗИ включают в отчет по результатам оценки соответствия ЗИ.

6.12 В случае, если в соответствии с ГОСТ Р 57580.1—2017 (пункт 6.4) вместо организационных и технических мер ЗИ, предусмотренных ГОСТ Р 57580.1, применяют иные (компенсирующие) меры ЗИ, при определении оценок $E_{МЗИ}$, $E_{МОУ}$ и $E_{МАС}$ для соответствующих процессов (подпроцессов) системы ЗИ и направлений ЗИ осуществляют оценку компенсирующих мер в соответствии с 6.10.1 — 6.10.3.

Обоснование применения компенсирующих мер ЗИ включают в отчет по результатам оценки соответствия ЗИ.

6.13 Оценку соответствия ЗИ следует основывать на свидетельствах, в качестве основных источников которых рекомендуется использовать:

- документы проверяемой организации и иные материалы проверяемой организации в бумажном или электронном виде и, при необходимости, документы третьих лиц, относящиеся к обеспечению ЗИ финансовой организации и находящиеся в распоряжении проверяемой организации;
- устные высказывания сотрудников проверяемой организации в процессе проводимых опросов в области оценки соответствия ЗИ;
- результаты наблюдений членов проверяющей группы за процессами системы ЗИ и деятельностью сотрудников проверяемой организации в области оценки соответствия ЗИ;
- параметры конфигураций и настроек технических объектов информатизации и средств ЗИ;
- технические и программные средства сбора свидетельств полноты реализации мер ЗИ (анализ электронных журналов регистрации, анализ фактических настроек, анализ уязвимостей, проведение тестирования на проникновение и т.п.).

Выбор конкретных источников свидетельств при проведении оценки соответствия ЗИ осуществляет проверяющая организация (проверяющая группа) с учетом предложений проверяемой организации и обеспечения максимальной достоверности оценки соответствия ЗИ.

6.14 При проведении оценки соответствия ЗИ сотрудники проверяющей организации (проверяющая группа) при сборе свидетельств выбора и реализации финансовой организацией организационных

и технических мер ЗИ в соответствии с требованиями ГОСТ Р 57580.1 по согласованию с проверяемой организацией могут использовать технические и программные средства для анализа параметров конфигураций, фактических настроек и электронных журналов регистрации технических объектов информатизации и средств ЗИ, а также результаты анализа уязвимостей и проведения тестирования на проникновение.

Проверку параметров конфигураций, фактических настроек и электронных журналов регистрации технических объектов информатизации и средств ЗИ проверяемой организации, а также результатов анализа уязвимостей и проведения тестирования на проникновение осуществляют в присутствии уполномоченных сотрудников проверяемой организации.

6.15 Полученные свидетельства и источники их получения должны быть задокументированы путем составления листов для сбора свидетельств оценки процессов системы ЗИ и направлений ЗИ, форма которых приведена в приложении А. При заполнении листов для сбора свидетельств необходимо указать ссылки на соответствующие документы и иные материалы проверяемой организации или документы третьих лиц, результаты опроса сотрудников проверяемой организации, результаты наблюдений членов проверяющей группы, а также результаты работы технических и программных средств в соответствии с 6.14. Результаты опроса должны быть подтверждены подписями члена (членов) проверяющей группы и опрашиваемого сотрудника (сотрудников) проверяемой организации.

## 7 Требования к методике оценки соответствия ЗИ

7.1 Числовое значение оценки, характеризующей выбор финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему ЗИ финансовой организации, $E_{\text{пзи}_i}$ ($E_{\text{ппзи}_i}$) вычисляют отдельно по каждому из процессов (подпроцессов) системы ЗИ по формуле (1) как среднеарифметическое значение оценок $E_{\text{мзи}_j}$ для каждой из организационных и технических мер ЗИ, установленных в ГОСТ Р 57580.1—2017 (раздел 7) и входящих в состав оцениваемого процесса (подпроцесса) системы ЗИ.

$$E_{\text{пзи}_i}(E_{\text{ппзи}_i}) = \frac{\sum_{j=1}^{N} E_{\text{мзи}_j}}{N}, \quad (1)$$

где $E_{\text{мзи}_j}$ — оценка выбора $j$-й меры ЗИ, оцениваемой в рамках $i$-го процесса (подпроцесса) системы ЗИ для соответствующего уровня ЗИ. Соответствующие значения $E_{\text{мзи}_j}$ берут из таблиц В.1—В.8 (приложение В);

$i$ — порядковый номер процесса (подпроцесса) системы ЗИ;

$j$ — порядковый номер меры ЗИ в процессе (подпроцессе) системы ЗИ, оцениваемой в рамках процесса (подпроцесса) системы ЗИ для соответствующего уровня ЗИ;

$N$ — общее количество мер ЗИ, выбор которых оценивается в рамках процесса (подпроцесса) системы ЗИ для соответствующего уровня ЗИ.

Числовые значения оценок $E_{\text{пзи}_i}$ по процессам 1, 2 и 6, указанным в 6.3, вычисляют по формуле (2) как среднеарифметическое значение оценок $E_{\text{ппзи}_k}$ для каждого из подпроцессов системы ЗИ, указанных в 6.4 — 6.6 и входящих в состав оцениваемого процесса системы ЗИ.

$$E_{\text{пзи}_i} = \frac{\sum_{k=1}^{M} E_{\text{ппзи}_k}}{M}, \quad (2)$$

где $E_{\text{ппзи}_k}$ — оценка выбора организационных и технических мер ЗИ $k$-го подпроцесса системы ЗИ в $i$-м процессе системы ЗИ;

$i$ — порядковый номер процесса системы ЗИ;

$k$ — порядковый номер подпроцесса системы ЗИ в процессе системы ЗИ;

$M$ — общее количество подпроцессов системы ЗИ в процессе системы ЗИ.

Значения оценок $E_{\text{пзи}_i}$ ($E_{\text{ппзи}_i}$) заносят в формы, приведенные в таблицах В.1 — В.8 (приложение В), а оценки $E_{\text{пзи}_i}$ также заносят в форму, приведенную в таблице В.14 (приложение В).

7.2 Числовое значение оценки, характеризующей планирование процесса системы ЗИ, $E_{П_i}$ вычисляют по формуле (3) отдельно по каждому из процессов системы ЗИ как среднеарифметическое значение оценок для организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ, входящих в систему организации и управления ЗИ финансовой организации и установленных в ГОСТ Р 57580.1—2017 (подраздел 8.2).

$$E_{П_i} = \frac{\sum_{n=1}^{F} E_{МОУ_n}}{F}, \quad (3)$$

где $E_{МОУ_n}$ — оценка полноты реализации $n$-й меры ЗИ, оцениваемой в рамках направления 1 «Планирование процесса системы защиты информации» для соответствующего уровня ЗИ. Соответствующие значения $E_{МОУ_n}$ берут из таблицы В.10 (приложение В);

$i$ — порядковый номер процесса системы ЗИ;

$n$ — порядковый номер меры ЗИ, оцениваемой в рамках направления 1 «Планирование процесса системы защиты информации» для соответствующего уровня ЗИ;

$F$ — общее количество мер ЗИ, реализация которых оценивается в рамках направления 1 «Планирование процесса системы защиты информации» для соответствующего уровня ЗИ.

Значения оценок $E_{П_i}$ заносят в формы, приведенные в таблицах В.10 и В.14 (приложение В).

7.3 Числовое значение оценки, характеризующей реализацию процесса системы ЗИ, $E_{Р_i}$ вычисляют по формуле (4) отдельно по каждому из процессов системы ЗИ как среднеарифметическое значение оценок для организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ, входящих в систему организации и управления ЗИ финансовой организации и установленных в ГОСТ Р 57580.1—2017 (подраздел 8.3).

$$E_{Р_i} = \frac{\sum_{j=1}^{P} E_{МОУ_j}}{P}, \quad (4)$$

где $E_{МОУ_j}$ — оценка полноты реализации $j$-й меры ЗИ, оцениваемой в рамках направления 2 «Реализация процесса системы защиты информации» для соответствующего уровня ЗИ. Соответствующие значения $E_{МОУ_j}$ берут из таблицы В.11 (приложение В);

$i$ — порядковый номер процесса системы ЗИ;

$j$ — порядковый номер меры ЗИ, оцениваемой в рамках направления 2 «Реализация процесса системы защиты информации» для соответствующего уровня ЗИ;

$P$ — общее количество мер, реализация которых оценивается в рамках направления 2 «Реализация процесса системы защиты информации» для соответствующего уровня ЗИ.

Значения оценок $E_{Р_i}$ заносят в формы, приведенные в таблицах В.11 и В.14 (приложение В).

7.4 Числовое значение оценки, характеризующей контроль процесса системы ЗИ, $E_{К_i}$ вычисляют по формуле (5) отдельно по каждому из процессов системы ЗИ как среднеарифметическое значение оценок для организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему организации и управления ЗИ финансовой организации и установленных в ГОСТ Р 57580.1—2017 (подраздел 8.4).

$$E_{К_i} = \frac{\sum_{k=1}^{S} E_{МОУ_k}}{S}, \quad (5)$$

где $E_{МОУ_k}$ — оценка полноты реализации $k$-ой меры ЗИ, оцениваемой в рамках направления 3 «Контроль процесса системы защиты информации» для соответствующего уровня ЗИ. Соответствующие значения $E_{МОУ_k}$ берут из таблицы В.12 (приложение В);

$i$ — порядковый номер процесса системы ЗИ;

$k$ — порядковый номер меры ЗИ, оцениваемой в рамках направления 3 «Контроль процесса системы защиты информации» для соответствующего уровня ЗИ;

$S$ — общее количество мер, реализация которых оценивается в рамках направления 3 «Контроль процесса системы защиты информации» для соответствующего уровня ЗИ.

Значения оценок $E_{K_i}$ заносят в формы, приведенные в таблицах В.12 и В.14 (приложение В).

7.5 Числовое значение оценки, характеризующей совершенствование процесса ЗИ, $E_{C_i}$ вычисляют по формуле (6) отдельно по каждому из процессов системы ЗИ как среднеарифметическое значение оценок для организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему организации и управления ЗИ финансовой организации и установленных в ГОСТ Р 57580.1—2017 (подраздел 8.5).

$$E_{C_i} = \frac{\sum_{m=1}^{Q} E_{МОУ_m}}{Q}, \quad (6)$$

где $E_{МОУ_m}$ — оценка полноты реализации $m$-й меры ЗИ, оцениваемой в рамках направления 4 «Совершенствование процесса системы защиты информации» для соответствующего уровня ЗИ. Соответствующие значения $E_{МОУ_m}$ берут из таблицы В.13 (приложение В);

$i$ — порядковый номер процесса системы ЗИ;

$m$ — порядковый номер меры ЗИ, оцениваемой в рамках направления 4 «Совершенствование процесса системы защиты информации» для соответствующего уровня ЗИ;

$Q$ — общее количество мер ЗИ, реализация которых оценивается в рамках направления 4 «Совершенствование процесса системы защиты информации» для соответствующего уровня ЗИ.

Значения оценок $E_{C_i}$ заносят в формы, приведенные в таблицах В.13 и В.14 (приложение В).

7.6 Числовое значение оценки, характеризующей применение организационных и технических мер ЗИ на этапах жизненного цикла АС финансовой организации, $E_{АС}$ вычисляют по формуле (7) как среднеарифметическое значение оценок $E_{МАС}$ для всех мер ЗИ, применяемых на этапах жизненного цикла АС и установленных в ГОСТ Р 57580.1—2017 (раздел 9).

$$E_{АС} = \frac{\sum_{j=1}^{L} E_{МАС_j}}{L}, \quad (7)$$

где $E_{МАС_j}$ — оценка применения $j$-й меры ЗИ, оцениваемой в рамках применения на этапах жизненного цикла АС для соответствующего уровня ЗИ. Соответствующие значения $E_{МАС_j}$ берут из таблицы В.9 (приложение В);

$j$ — порядковый номер меры ЗИ, оцениваемой в рамках применения на этапах жизненного цикла АС для соответствующего уровня ЗИ;

$L$ — общее количество мер ЗИ, применение которых оценивается в рамках применения на этапах жизненного цикла АС для соответствующего уровня ЗИ.

Значение оценки $E_{АС}$ заносят в формы, приведенные в таблицах В.9 и В.14 (приложение В).

7.7 Числовое значение оценки соответствия каждого процесса системы ЗИ $E_i$ вычисляют по формуле (8) отдельно по каждому из $i$-го процессов системы ЗИ как среднеарифметическое значение числовой оценки $E_{ПЗИ_i}$ и суммы числовых значений оценок $E_{П_i}$, $E_{Р_i}$, $E_{К_i}$, $E_{С_i}$ с учетом их весовых коэффициентов.

$$E_i = \frac{E_{ПЗИ_i} + (0{,}2E_{П_i} + 0{,}4E_{Р_i} + 0{,}25E_{К_i} + 0{,}15E_{С_i})}{2}. \quad (8)$$

7.8 В случае если в область оценки соответствия ЗИ входят несколько контуров безопасности с различными уровнями ЗИ, сформированными финансовой организацией в соответствии с требованиями ГОСТ Р 57580.1—2017 (пункт 6.7) для реализации требований к обеспечению ЗИ, установленных нормативными актами Банка России, числовое значение оценки каждого процесса системы ЗИ $E_i$ вычисляют по формуле (8) отдельно по контурам безопасности с одинаковым установленным уровнем ЗИ. Общее числовое значение оценки каждого процесса системы ЗИ $E_i$ (в зависимости от различных вариантов наличия у проверяемой организации контуров безопасности с разными установленными

уровнями ЗИ) вычисляют по формулам (9)—(12) как сумму числовых значений оценок $E_i$ для контура (контуров) безопасности с учетом их весовых коэффициентов:

- при оценке контуров безопасности с первым, вторым и третьим уровнями ЗИ:

$$E_i = 0{,}6E_{1i} + 0{,}3E_{2i} + 0{,}1E_{3i}; \quad (9)$$

- при оценке контуров безопасности с первым и вторым уровнями ЗИ:

$$E_i = 0{,}7E_{1i} + 0{,}3E_{2i}; \quad (10)$$

- при оценке контуров безопасности с первым и третьим уровнями ЗИ:

$$E_i = 0{,}8E_{1i} + 0{,}2E_{3i}; \quad (11)$$

- при оценке контуров безопасности со вторым и третьим уровнями ЗИ:

$$E_i = 0{,}6E_{2i} + 0{,}4E_{3i}; \quad (12)$$

где $E_{1i}$ — оценка каждого процесса системы ЗИ по контуру (контурам) безопасности, для которого (которых) установлен первый уровень ЗИ;

$E_{2i}$ — оценка каждого процесса системы ЗИ по контуру (контурам) безопасности, для которого (которых) установлен второй уровень ЗИ;

$E_{3i}$ — оценка каждого процесса системы ЗИ по контуру (контурам) безопасности, для которого (которых) установлен третий уровень ЗИ.

Значения оценок $E_i$ заносят в форму, приведенную в таблице В.14 (приложение В).

7.9 Качественную оценку уровня соответствия каждого процесса системы ЗИ определяют по таблице 1 в соответствии с числовыми оценками $E_i$. Описание уровней соответствия содержится в качественной модели оценивания, приведенной в 6.9.

Таблица 1 — Качественная оценка уровня соответствия процессов системы ЗИ

| $E_i$ | Уровень соответствия |
|---|---|
| $E_i = 0$ | Нулевой |
| $0 < E_i \le 0{,}5$ | Первый |
| $0{,}5 < E_i \le 0{,}7$ | Второй |
| $0{,}7 < E_i \le 0{,}85$ | Третий |
| $0{,}85 < E_i \le 0{,}9$ | Четвертый |
| $0{,}9 < E_i \le 1$ | Пятый |

Значения качественных оценок заносят в форму, приведенную в таблице В.14 (приложение В).

7.10 Числовую итоговую оценку соответствия ЗИ $R$ вычисляют по формуле (13) как среднеарифметическое значение оценок $E_i$ для всех процессов системы ЗИ и оценки $E_{AC}$.

$$R = \frac{\sum_{i=1}^{T} E_i + E_{AC}}{T+1} - 0{,}01Z, \quad (13)$$

где $E_i$ — оценка соответствия ЗИ $i$-го процесса системы ЗИ;

$i$ — номер процесса системы ЗИ;

$T$ — количество процессов системы ЗИ, вошедших в область оценки соответствия ЗИ;

$E_{AC}$ — оценка полноты применения организационных и технических мер ЗИ на этапах жизненного цикла АС финансовой организации;

$Z$ — количество нарушений ЗИ, выявленных членами проверяющей группы в процессе оценки соответствия ЗИ.

При выявлении самостоятельно членами проверяющей группы в процессе оценки соответствия ЗИ фактов нарушений ЗИ, в результате которых имелась или имеется возможность наступления инци-

дентов ЗИ, наносящих ущерб финансовой организации или ее клиентам, числовую итоговую оценку соответствия ЗИ $R$ снижают на числовое значение, равное 0,01, за каждый выявленный факт нарушения.

Факты нарушений ЗИ, выявленные проверяемой организацией самостоятельно до начала и в процессе оценки соответствия ЗИ, по которым проведено разбирательство до окончания оценки соответствия ЗИ и приняты или запланированы с документальным оформлением соответствующие меры реагирования, при снижении итоговой оценки соответствия ЗИ не учитываются. Перечень нарушений приведен в приложении Б.

В случае, если полноту применения организационных и технических мер ЗИ на этапах жизненного цикла АС финансовой организации не оценивают ($E_{AC}$ = 0), в знаменателе формулы (13) указывают только значение $T$.

Значение итоговой оценки $R$ заносят в форму, приведенную в таблице В.14 (приложение В).

7.11 При вычислении оценок, указанных в разделе 7, их значения необходимо округлять до второго знака после запятой в соответствии с математическими правилами.

7.12 Заполненные формы, приведенные в приложениях А и В, являются приложением к отчету по результатам оценки соответствия ЗИ.

7.13 Числовые оценки соответствия ЗИ $R$, превышающие числовое значение 0,85, соответствуют уровню, рекомендуемому Банком России.

## 8 Требования к оформлению результатов оценки соответствия ЗИ

8.1 По результатам оценки соответствия ЗИ проверяющая организация должна подготовить отчет.

8.2 Отчет должен предоставлять полные, точные, четкие и достаточные записи по оценке соответствия ЗИ и включать следующие данные:

- сведения о проверяющей организации;
- сведения о руководителе и членах проверяющей группы;
- сведения о проверяемой организации;
- сведения о заказчике оценки соответствия ЗИ;
- цель оценки соответствия ЗИ;
- сроки проведения оценки соответствия ЗИ;
- область оценки соответствия ЗИ;
- перечень неоцениваемых областей оценки соответствия ЗИ (процессов системы ЗИ, подпроцессов системы ЗИ, направлений ЗИ, мер ЗИ) с обоснованием их исключения из области оценки соответствия ЗИ;
- обоснование применения компенсирующих мер ЗИ при невозможности реализации отдельных выбранных мер ЗИ;
- краткое изложение процесса оценки соответствия ЗИ, включая элемент неопределенности и/или проблемы, которые могут отразиться на надежности заключения по результатам оценки соответствия ЗИ;
- числовое значение итоговой оценки соответствия ЗИ, характеризующей соответствие ЗИ проверяемой организации установленным требованиям на дату завершения оценки соответствия ЗИ;
- подтверждение, что цель оценки соответствия ЗИ достигнута в области оценки соответствия ЗИ;
- неразрешенные разногласия между проверяющей группой и проверяемой организацией;
- перечень и сведения о представителях проверяемой организации, которые сопровождали проверяющую группу при проведении оценки соответствия ЗИ;
- сведения о конфиденциальном характере содержания отчета по результатам оценки соответствия ЗИ;
- опись документов (копий документов) на бумажных носителях, прилагаемых к отчету по результатам оценки соответствия ЗИ, с указанием общего количества томов приложений, количества и наименований документов, а также количества листов в каждом из них;
- опись машинных носителей информации, прилагаемых к отчету по результатам оценки соответствия ЗИ, с указанием их реквизитов (наименование, тип, учетный номер и т.п.) и содержащихся на них файлов данных, а также результатов вычисления по каждому из них хэш-функции, реализованной в соответствии с ГОСТ Р 34.11.

8.3 К отчету по результатам оценки соответствия ЗИ прилагаются и являются его неотъемлемой частью:

- заполненные листы для сбора свидетельств оценки процессов (подпроцессов) системы ЗИ и направлений ЗИ, подтверждающих выставленные оценки, по форме, приведенной в приложении А;

- перечень нарушений ЗИ, выявленных членами проверяющей группы в результате оценки соответствия ЗИ, которые могли или могут привести к инцидентам ЗИ, наносящим ущерб финансовой организации или ее клиентам;

- рекомендации по совершенствованию ЗИ и устранению выявленных нарушений;

- таблицы, содержащие числовые значения оценок процессов (подпроцессов) системы ЗИ и направлений ЗИ по результатам оценки соответствия ЗИ и заполненные по формам, приведенным в приложении В,

- копии документов проверяемой организации или документов третьих лиц на бумажных носителях, являющихся свидетельствами выполнения (невыполнения) требований ЗИ;

- машинные носители информации с электронными документами и файлами данных, являющихся свидетельствами выполнения (невыполнения) требований ЗИ.

8.4 Отчет по результатам оценки соответствия ЗИ должен иметь сквозную нумерацию страниц, регистрационный номер, должен быть прошит нитью, не имеющей разрывов, и скреплен печатью проверяющей организации с указанием количества листов в заверительной надписи, подписанной руководителем проверяющей группы.

8.5 Копии документов на бумажных носителях, прилагаемых к отчету по результатам оценки соответствия ЗИ, должны быть прошиты нитью, не имеющей разрывов, и скреплены печатью проверяемой организации с указанием количества листов документа в заверительной надписи, подписанной руководителем проверяемой организации или лицом им уполномоченным.

Тома с документами на бумажных носителях, прилагаемые к отчету по результатам оценки соответствия ЗИ, должны быть прошиты нитью, не имеющей разрывов, и скреплены печатью проверяющей организации с указанием количества листов тома в заверительной надписи, подписанной руководителем проверяющей группы.

Для каждого электронного документа, файла данных, прилагаемых к отчету по результатам оценки соответствия ЗИ, должны быть вычислены хэш-функции, реализованные в соответствии с ГОСТ Р 34.11.

8.6 Отчет по результатам оценки соответствия ЗИ должен быть подписан руководителем и всеми членами проверяющей группы, утвержден руководителем проверяющей организации и передан (направлен) проверяемой организации не позднее даты, установленной договором на проведение работ по оценке соответствия ЗИ.

8.7 Отчет по результатам оценки соответствия ЗИ является собственностью проверяемой организации. Члены проверяющей группы и все получатели отчета должны обеспечивать конфиденциальность содержания отчета, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

8.8 Порядок и сроки направления финансовой организацией отчета по результатам оценки соответствия ЗИ в Банк России, а также сроки его хранения проверяемой организацией определяются нормативными актами Банка России.

## Приложение А
## (справочное)

### Форма листов для сбора свидетельств оценки соответствия ЗИ

Процесс (подпроцесс) системы ЗИ, направление ЗИ

_____

| Условное обозначение и номер меры ЗИ | Источники свидетельств оценки соответствия ЗИ (документы, результаты опроса или наблюдений) | Ф.И.О. и должность сотрудника (сотрудников) проверяемой организации, предоставившего (предоставивших) свидетельства оценки соответствия ЗИ | Подписи члена (членов) проверяющей группы и сотрудника (сотрудников) проверяемой организации | Дата |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Приложение Б
## (справочное)

### Перечень нарушений ЗИ

Б.1 Осуществление логического доступа под учетными записями неопределенного целевого назначения.

Б.2 Осуществление логического доступа под коллективными неперсонифицированными учетными записями.

Б.3 Наличие незаблокированных учетных записей уволенных работников.

Б.4 Отсутствие разграничения логического доступа.

Б.5 Несанкционированное предоставление пользователям административных прав.

Б.6 Несанкционированное предоставление пользователям прав логического доступа.

Б.7 Хранение паролей субъектов доступа в открытом виде.

Б.8 Передача аутентификационных данных в открытом виде по каналам и линиям связи.

Б.9 Отсутствие регистрации персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации.

Б.10 Отсутствие разграничения физического доступа в помещения, в которых расположены объекты доступа.

Б.11 Несанкционированный физический доступ посторонних лиц в помещения, в которых расположены объекты доступа.

Б.12 Отсутствие логической сетевой изоляции внутренних вычислительных сетей финансовой организации и сети Интернет и/или беспроводных сетей.

Б.13 Передача информации конфиденциального характера с использованием сети Интернет, телекоммуникационных каналов и/или линий связи, не контролируемых финансовой организацией, в открытом виде.

Б.14 Наличие в контролируемой зоне финансовой организации незарегистрированных точек беспроводного доступа, имеющих подключение к локальной вычислительной сети финансовой организации.

Б.15 Использование нелицензионного ПО.

Б.16 Отсутствие применения средств защиты от воздействия вредоносного кода.

Б.17 Обработка информации конфиденциального характера с использованием неучтенных МНИ.

Б.18 Отсутствие гарантированного стирания информации конфиденциального характера с МНИ при осуществлении их вывода из эксплуатации или вывода из эксплуатации СВТ, в состав которого входят указанные МНИ, а также при необходимости их передачи в сторонние организации.

Б.19 Отсутствие реагирования на инциденты ЗИ.

## Приложение В
## (справочное)

### Формы таблиц оценок, входящих в отчет по результатам оценки соответствия ЗИ

В.1 Формы таблиц оценок, характеризующих выбор финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в процессы 1—8 системы ЗИ, приведены в таблицах В.1—В.8 соответственно.

Таблица В.1 — Форма таблицы оценок соответствия ЗИ для процесса 1

| Процесс 1 «Обеспечение защиты информации при управлении доступом» | | |
|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МЗИ_j}$ (0 или 1) |
| Подпроцесс «Управление учетными записями и правами субъектов логического доступа» | | |
| | | |
| | | |
| Итоговая оценка за подпроцесс $E_{ППЗИ_1}$ | | |
| Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа» | | |
| | | |
| | | |
| Итоговая оценка за подпроцесс $E_{ППЗИ_2}$ | | |
| Подпроцесс «Защита информации при осуществлении физического доступа» | | |
| | | |
| | | |
| Итоговая оценка за подпроцесс $E_{ППЗИ_3}$ | | |
| Подпроцесс «Идентификация и учет ресурсов и объектов доступа» | | |
| | | |
| | | |
| Итоговая оценка за подпроцесс $E_{ППЗИ_4}$ | | |
| **Итоговая оценка за процесс $E_{ПЗИ_1}$** | | |

Таблица В.2 — Форма таблицы оценок соответствия ЗИ для процесса 2

| Процесс 2 «Обеспечение защиты вычислительных сетей» | | |
|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МЗИ_j}$ (0 или 1) |
| Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей» | | |
| | | |
| | | |
| | | |
| | | |
| Итоговая оценка за подпроцесс $E_{ППЗИ_1}$ | | |
| Подпроцесс «Выявление вторжений и сетевых атак» | | |
| | | |
| | | |
| | | |
| | | |
| Итоговая оценка за подпроцесс $E_{ППЗИ_2}$ | | |
| Подпроцесс «Защита информации, передаваемой по вычислительным сетям» | | |
| | | |
| | | |
| | | |
| | | |
| Итоговая оценка за подпроцесс $E_{ППЗИ_3}$ | | |
| Подпроцесс «Защита беспроводных сетей» | | |
| | | |
| | | |
| | | |
| | | |
| Итоговая оценка за подпроцесс $E_{ППЗИ_4}$ | | |
| **Итоговая оценка за процесс $E_{ПЗИ_2}$** | | |

Таблица В.3 — Форма таблицы оценок соответствия ЗИ для процесса 3

| Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры» | | |
|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МЗИ_j}$ (0 или 1) |
| | | |
| | | |
| | | |
| | | |
| | **Итоговая оценка за процесс $E_{ПЗИ_3}$** | |

Таблица В.4 — Форма таблицы оценок соответствия ЗИ для процесса 4

| Процесс 4 «Защита от вредоносного кода» | | |
|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МЗИ_j}$ (0 или 1) |
| | | |
| | | |
| | | |
| | | |
| | **Итоговая оценка за процесс $E_{ПЗИ_4}$** | |

Таблица В.5 — Форма таблицы оценок соответствия ЗИ для процесса 5

| Процесс 5 «Предотвращение утечек информации» | | |
|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МЗИ_j}$ (0 или 1) |
| | | |
| | | |
| | | |
| | | |
| | **Итоговая оценка за процесс $E_{ПЗИ_5}$** | |

Таблица В.6 — Форма таблицы оценок соответствия ЗИ для процесса 6

| Процесс 6 «Управление инцидентами защиты информации» | | |
|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МЗИ_j}$ (0 или 1) |
| Подпроцесс «Мониторинг и анализ событий защиты информации» | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Итоговая оценка за подпроцесс $E_{ППЗИ_1}$ | | |
| Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них» | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Итоговая оценка за подпроцесс $E_{ППЗИ_2}$ | | |
| **Итоговая оценка за процесс $E_{ПЗИ_6}$** | | |

Таблица В.7 — Форма таблицы оценок соответствия ЗИ для процесса 7

| Процесс 7 «Защита среды виртуализации» | | |
|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МЗИ_j}$ (0 или 1) |
| | | |
| | | |
| | | |
| | | |
| | | |
| **Итоговая оценка за процесс $E_{ПЗИ_7}$** | | |

Таблица В.8 — Форма таблицы оценок соответствия ЗИ для процесса 8

| Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств» | | |
|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МЗИ_j}$ (0 или 1) |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| **Итоговая оценка за процесс $E_{ПЗИ_5}$** | | |

В.2 Форма таблицы значений оценок, характеризующих применение организационных и технических мер ЗИ на этапах жизненного цикла АС, приведена в таблице В.9.

Таблица В.9 — Форма таблицы оценок соответствия ЗИ на этапах жизненного цикла АС

| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МАС_j}$ (0, 0,5 или 1) |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| **Итоговая оценка $E_{АС}$** | | |

В.3 Формы таблиц оценок, характеризующих полноту реализации организационных и технических мер ЗИ, входящих в систему ЗИ по направлениям 1—4, приведены в таблицах В.10—В.13 соответственно.

Таблица В.10 — Форма таблиц оценок, характеризующих полноту реализации организационных и технических мер ЗИ, входящих в систему ЗИ по направлению 1

| Направление 1 «Планирование процесса системы защиты информации» | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МОУ_n}$ (0; 0,5 или 1) | | | | | | | |
| | | Процесс 1 | Процесс 2 | Процесс 3 | Процесс 4 | Процесс 5 | Процесс 6 | Процесс 7 | Процесс 8 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| **Итоговая оценка за процессы $E_{П_i}$** | | | | | | | | | |

Таблица В.11 — Форма таблиц оценок, характеризующих полноту реализации организационных и технических мер ЗИ, входящих в систему ЗИ по направлению 2

| Направление 2 «Реализация процесса системы защиты информации» | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МОУ_j}$ (0, 0.5 или 1) | | | | | | | |
| | | Процесс 1 | Процесс 2 | Процесс 3 | Процесс 4 | Процесс 5 | Процесс 6 | Процесс 7 | Процесс 8 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| **Итоговая оценка за процессы $E_{Р_i}$** | | | | | | | | | |

Таблица В.12 — Форма таблиц оценок, характеризующих полноту реализации организационных и технических мер ЗИ, входящих в систему ЗИ по направлению 3

| Направление 3 «Контроль процесса системы защиты информации» | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МОУ_k}$ (0; 0,5 или 1) | | | | | | | |
| | | Процесс 1 | Процесс 2 | Процесс 3 | Процесс 4 | Процесс 5 | Процесс 6 | Процесс 7 | Процесс 8 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| **Итоговая оценка за процессы $E_{K_j}$** | | | | | | | | | |

Таблица В.13 — Форма таблиц оценок, характеризующих полноту реализации организационных и технических мер ЗИ, входящих в систему ЗИ по направлению 4

| Направление 4 «Совершенствование процесса системы защиты информации» | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Условное обозначение и номер меры | Содержание мер системы защиты информации | Оценка $E_{МОУ_m}$ (0; 0,5 или 1) | | | | | | | |
| | | Процесс 1 | Процесс 2 | Процесс 3 | Процесс 4 | Процесс 5 | Процесс 6 | Процесс 7 | Процесс 8 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| **Итоговая оценка за процессы $E_{C_i}$** | | | | | | | | | |

В.4 Форма таблицы итоговых оценок по результатам оценки соответствия ЗИ приведена в таблице В.14.

Таблица В.14 — Форма таблицы итоговых оценок по результатам оценки соответствия ЗИ

| Наименование процесса системы ЗИ, направления ЗИ | Оценка, характеризующая выбор организационных и технических мер системы ЗИ $E_{ПЗИ_i}$ | Оценка по направлениям ЗИ системы организации и управления ЗИ | | | | Качественная оценка уровня соответствия процесса системы ЗИ | Числовое значение оценки соответствия процесса системы ЗИ $E_i$ |
|---|---|---|---|---|---|---|---|
| | | Планирование процесса системы ЗИ $E_{П_i}$ | Реализация процесса системы ЗИ $E_{Р_i}$ | Контроль процесса системы ЗИ $E_{К_i}$ | Совершенствование процесса системы ЗИ $E_{С_i}$ | | |
| Процесс 1 «Обеспечение защиты информации при управлении доступом» | | | | | | | |
| Процесс 2 «Обеспечение защиты вычислительных сетей» | | | | | | | |
| Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры» | | | | | | | |
| Процесс 4 «Защита от вредоносного кода» | | | | | | | |
| Процесс 5 «Предотвращение утечек информации» | | | | | | | |
| Процесс 6 «Управление инцидентами защиты информации» | | | | | | | |
| Процесс 7 «Защита среды виртуализации» | | | | | | | |
| Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств» | | | | | | | |
| Применение организационных и технических мер ЗИ на этапах жизненного цикла АС $E_{АС}$ | | | | | | | |
| **Итоговая оценка соответствия ЗИ с учетом выявленных нарушений ЗИ** | | | | | | | |
| Количество нарушений ЗИ, выявленных в результате оценки соответствия ЗИ $Z$ | | | | | | | |
| **Итоговая оценка соответствия ЗИ $R$** | | | | | | | |

## Библиография


[1] Федеральный закон от 10 июля 2002 г. № 86-ФЗ — О Центральном банке Российской Федерации (Банке России)

[2] Федеральный закон от 29 июня 2015 г. № 162-ФЗ — О стандартизации в Российской Федерации

[3] ГОСТ Р ИСО 19011—2012 — Руководящие указания по аудиту систем менеджмента

УДК 351.864.1:004:006.354

ОКС 03.060
35.240.40

Ключевые слова: безопасность финансовых (банковских) операций, защита информации, финансовые организации, методика оценки соответствия, система защиты информации, уровень защиты информации, требования к системе защиты информации, требования к системе организации и управления защитой информации, оценка соответствия выполнения требований защиты информации

**БЗ 4—2018/6**

Редактор *Л.И. Нахимова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 29.03.2018. Подписано в печать 04.04.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,95.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ», для комплектования Федерального информационного фонда стандартов, 123001 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru