ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Методические рекомендации по расчету значений показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в целях составления отчетности об оценке выполнения требований к обеспечению защиты информации некредитными финансовыми организациями

20.06.2023 № 8-МР

Глава 1. **Общие положения**

1.1. Настоящие Методические рекомендации разработаны в целях обеспечения единства подходов к расчету значений показателей оценки выполнения требований к технологическим мерам защиты информации (направление «Технологические меры») и требований к прикладному программному обеспечению автоматизированных систем и приложений (направление «Безопасность программного обеспечения») при составлении отчетности об оценке выполнения требований к обеспечению защиты информации некредитными финансовыми организациями.

1.2. Настоящими Методическими рекомендациями рекомендуется руководствоваться следующим отчитывающимся организациям:

профессиональным участникам рынка ценных бумаг, организаторам торговли, клиринговым организациям при составлении отчетности по

форме 0420433 «Сведения об оценке выполнения требований к обеспечению защиты информации профессиональными участниками рынка ценных бумаг, организаторами торговли, клиринговыми организациями»;

негосударственным пенсионным фондам при составлении отчетности по форме 0420266 «Сведения об оценке выполнения требований к обеспечению защиты информации негосударственным пенсионным фондом»;

операторам инвестиционной платформы, операторам финансовой платформы, операторам информационных систем, в которых осуществляется выпуск цифровых финансовых активов, операторам обмена цифровых финансовых активов при составлении отчетности (отчета) по форме 0420722 «Сведения об оценке выполнения требований к обеспечению защиты информации оператором инвестиционной платформы, оператором финансовой платформы, оператором информационных систем, в которых осуществляется выпуск цифровых финансовых активов, и оператором обмена цифровых финансовых активов»;

страховым организациям при составлении отчетности по форме 0420175 «Сведения об оценке выполнения требований к обеспечению защиты информации страховой организацией».

Глава 2. **Рекомендации по расчету значений показателей оценки выполнения требований к технологическим мерам защиты информации (направление «Технологические меры»)**

2.1. Расчет значений показателей оценки выполнения требований к технологическим мерам защиты информации по направлению «Технологические меры» рекомендуется осуществлять в отношении требований, указанных в приложении 1 к настоящим Методическим рекомендациям (далее для целей настоящей главы – требования).

2.2. По направлению «Технологические меры» осуществляется расчет значений следующих показателей:

$E_{ТМП}$ – оценка, характеризующая выполнение требований в рамках

процесса планирования применения мер защиты информации;

$E_{ТМР}$ – оценка, характеризующая выполнение требований в рамках процесса реализации применения мер защиты информации;

$E_{ТМК}$ – оценка, характеризующая выполнение требований в рамках процесса контроля применения мер защиты информации;

$E_{ТМС}$ – оценка, характеризующая выполнение требований в рамках процесса совершенствования применения мер защиты информации;

$E_{ТМ}$ – обобщающий показатель уровня оценки соответствия по направлению «Технологические меры».

2.3. Значение оценки, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации ($E_{ТМП}$), рекомендуется рассчитывать по формуле:

$$E_{ТМП} = \frac{\sum_{i=1}^{N} E_{По_i} + \sum_{i=1}^{N} E_{Пп_i}}{2N}, \text{ где}$$

i – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{По_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации по вопросу определения области применения меры защиты информации;

$E_{Пп_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации по вопросу определения порядка применения меры защиты информации.

В рамках процесса планирования применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Определена ли область применения меры защиты информации?»;

«Определен ли порядок применения меры защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («определено»);

0 – «нет» («не определено»).

2.4. Значение оценки, характеризующей выполнение требований в рамках процесса реализации мер защиты информации ($E_{ТМР}$), рекомендуется рассчитывать по формуле:

$$E_{ТМР} = \frac{\sum_{i=1}^{N} E_{Рм_i}}{N}, \text{ где}$$

i – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{Рм_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса реализации мер защиты информации.

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («постоянно», «всегда», «в полном объеме»);

0,75 – «в основном да» («почти постоянно», «почти всегда», «почти в полном объеме»);

0,5 – «частично» («отчасти да», «не всегда», «в некоторых случаях»);

0,25 – «в основном нет» («непостоянно», «почти никогда»);

0 – «нет» («никогда», «ни в каких случаях»).

2.5. Значение оценки, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации ($E_{ТМК}$), рекомендуется рассчитывать по формуле:

$$E_{ТМК} = \frac{\sum_{i=1}^{N} E_{Ко_i} + \sum_{i=1}^{N} E_{Кп_i} + \sum_{i=1}^{N} E_{Кз_i}}{3N}, \text{ где}$$

i – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{Ко_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля области применения меры защиты информации;

$E_{Кп_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля надлежащего применения меры защиты информации;

$E_{Кз_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля знаний работников некредитной финансовой организации в части применения меры защиты информации.

В рамках процесса контроля применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Обеспечен ли контроль области применения меры защиты информации?»;

«Обеспечен ли контроль надлежащего применения меры защиты информации?»;

«Обеспечен ли контроль знаний работников некредитной финансовой организации в части применения меры защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («контроль обеспечен»);

0 – «нет» («контроль не обеспечен»).

2.6. Значение оценки, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации ($E_{ТМС}$), рекомендуется рассчитывать по формуле:

$E_{ТМС} = \frac{\sum_{i=1}^{N} E_{Си_i} + \sum_{i=1}^{N} E_{Сн_i}}{2N}$, где

i – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{Си_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации по вопросу анализа необходимости

совершенствования меры защиты информации в случае обнаружения инцидентов защиты информации;

$E_{Сн_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации по вопросу анализа необходимости совершенствования меры защиты информации в случае обнаружения недостатков в рамках контроля применения мер защиты информации.

В рамках процесса совершенствования применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Осуществляется ли анализ необходимости совершенствования меры защиты информации в случае обнаружения инцидентов защиты информации?»;

«Осуществляется ли анализ необходимости совершенствования меры защиты информации в случае обнаружения недостатков в рамках контроля применения мер защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («анализ совершенствования осуществляется»);

0 – «нет» («анализ совершенствования не осуществляется»).

2.7. Значение обобщающего показателя уровня оценки соответствия по направлению «Технологические меры» ($E_{ТМ}$) рекомендуется рассчитывать по формуле:

$E_{ТМ} = 0{,}2E_{ТМП} + 0{,}4E_{ТМР} + 0{,}25E_{ТМК} + 0{,}15E_{ТМС}$, где

$E_{ТМП}$ – значение оценки, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации, рассчитанное в соответствии с пунктом 2.3 настоящей главы;

$E_{ТМР}$ – значение оценки, характеризующей выполнение требований в рамках процесса реализации мер защиты информации, рассчитанное в соответствии с пунктом 2.4 настоящей главы;

$E_{ТМК}$ – значение оценки, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации, рассчитанное в соответствии с пунктом 2.5 настоящей главы;

$E_{ТМС}$ – значение оценки, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации, рассчитанное в соответствии с пунктом 2.6 настоящей главы.

Глава 3. **Рекомендации по расчету значений показателей оценки выполнения требований к прикладному программному обеспечению автоматизированных систем и приложений (направление «Безопасность программного обеспечения»)**

3.1. Расчет значений показателей оценки выполнения требований к прикладному программному обеспечению автоматизированных систем и приложений по направлению «Безопасность программного обеспечения» рекомендуется осуществлять в отношении требований, указанных в приложении 2 к настоящим Методическим рекомендациям (далее для целей настоящей главы – требования).

3.2. По направлению «Безопасность программного обеспечения» осуществляется расчет значений следующих показателей:

$E_{ПОП}$ – оценка, характеризующая выполнение требований в рамках процесса планирования применения мер защиты информации;

$E_{ПОР}$ – оценка, характеризующая выполнение требований в рамках процесса реализации применения мер защиты информации;

$E_{ПОК}$ – оценка, характеризующая выполнение требований в рамках процесса контроля применения мер защиты информации;

$E_{ПОС}$ – оценка, характеризующая выполнение требований в рамках процесса совершенствования применения мер защиты информации;

$E_{ПО}$ – обобщающий показатель уровня оценки соответствия по направлению «Безопасность программного обеспечения».

3.3. Значение оценки, характеризующей выполнение требований в

рамках процесса планирования применения мер защиты информации ($E_{ПОП}$), рекомендуется рассчитывать по формуле:

$$E_{ПОП} = \frac{\sum_{i=1}^{N} E_{По_i} + \sum_{i=1}^{N} E_{Пп_i}}{2N}$$, где

i – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{По_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации по вопросу определения области применения меры защиты информации;

$E_{Пп_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации по вопросу определения порядка применения меры защиты информации.

В рамках процесса планирования применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Определена ли область применения меры защиты информации?»;

«Определен ли порядок применения меры защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («определено»);

0 – «нет» («не определено»).

3.4. Значение оценки, характеризующей выполнение требований в рамках процесса реализации мер защиты информации ($E_{ПОР}$), рекомендуется рассчитывать по формуле:

$$E_{ПОР} = \frac{\sum_{i=1}^{N} E_{Рм_i}}{N}$$, где

i – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{Рм_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса реализации мер защиты

информации.

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («постоянно», «всегда», «в полном объеме»);

0,75 – «в основном да» («почти постоянно», «почти всегда», «почти в полном объеме»);

0,5 – «частично» («отчасти да», «не всегда», «в некоторых случаях»);

0,25 – «в основном нет» («непостоянно», «почти никогда»);

0 – «нет» («никогда», «ни в каких случаях»).

3.5. Значение оценки, характеризующей выполнение требований в рамках процесса контроля реализации мер защиты информации ($E_{ПОК}$), рекомендуется рассчитывать по формуле:

$$E_{ПОК} = \frac{\sum_{i=1}^{N} E_{Ко_i} + \sum_{i=1}^{N} E_{Кп_i} + \sum_{i=1}^{N} E_{Кз_i}}{3N}, \text{ где}$$

i – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{Ко_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля области применения меры защиты информации;

$E_{Кп_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля надлежащего применения меры защиты информации;

$E_{Кз_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля знаний работников некредитной финансовой организации в части применения меры защиты информации.

В рамках процесса контроля применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Обеспечен ли контроль области применения меры защиты информации?»;

«Обеспечен ли контроль надлежащего применения меры защиты информации?»;

«Обеспечен ли контроль знаний работников некредитной финансовой организации в части применения меры защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («контроль обеспечен»);

0 – «нет» («контроль не обеспечен»).

3.6. Значение оценки, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации ($E_{ПОС}$), рекомендуется рассчитывать по формуле:

$$E_{ПОС} = \frac{\sum_{i=1}^{N} E_{Си_i} + \sum_{i=1}^{N} E_{Сн_i}}{2N}$$, где

i – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{Си_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации по вопросу анализа необходимости совершенствования меры защиты информации в случае обнаружения инцидентов защиты информации;

$E_{Сн_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации по вопросу анализа необходимости совершенствования меры защиты информации в случае обнаружения недостатков в рамках контроля применения мер защиты информации.

В рамках процесса совершенствования применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Осуществляется ли анализ необходимости совершенствования меры защиты информации в случае обнаружения инцидентов защиты информации?»;

«Осуществляется ли анализ необходимости совершенствования меры защиты информации в случае обнаружения недостатков в рамках контроля применения мер защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («анализ совершенствования осуществляется»);

0 – «нет» («анализ совершенствования не осуществляется»).

3.7. Значение обобщающего показателя уровня оценки соответствия по направлению «Безопасность программного обеспечения» ($Е_{ПО}$) рекомендуется рассчитывать по формуле:

$Е_{ПО} = 0,2Е_{ПОП} + 0,4Е_{ПОР} + 0,25Е_{ПОК} + 0,15Е_{ПОС}$, где

$Е_{ПОП}$ – значение оценки, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации, рассчитанное в соответствии с пунктом 3.3 настоящей главы;

$Е_{ПОР}$ – значение оценки, характеризующей выполнение требований в рамках процесса реализации мер защиты информации, рассчитанное в соответствии с пунктом 3.4 настоящей главы;

$Е_{ПОК}$ – значение оценки, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации, рассчитанное в соответствии с пунктом 3.5 настоящей главы;

$Е_{ПОС}$ – значение оценки, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации, рассчитанное в соответствии с пунктом 3.6 настоящей главы.

Глава 4. **Заключительные положения**

Настоящие Методические рекомендации подлежат размещению на

официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

Заместитель Председателя
Банка России Г.А. Зубарев

Приложение 1
к Методическим рекомендациям по расчету значений показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в целях составления отчетности об оценке выполнения требований к обеспечению защиты информации некредитными финансовыми организациями

Перечень требований к технологическим мерам защиты информации по направлению «Технологические меры»

1. Рекомендуемый перечень требований, установленных Положением Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (далее – Положение Банка России № 757-П) в отношении некредитных финансовых организаций, выполнение которых оценивается при выборе соответствующего аналитического признака, характеризующего вид деятельности отчитывающейся организации[1], приведен в таблице 1.1.

[1] Аналитические признаки, характеризующие вид деятельности отчитывающихся организаций определены пунктом 3 порядка и сроков составления отчетности по форме 0420433 «Сведения об оценке выполнения требований к обеспечению защиты информации профессиональными участниками рынка ценных бумаг, организаторами торговли, клиринговыми организациями», пунктом 3 порядка и сроков составления отчетности по форме 0420175 «Сведения об оценке выполнения требований к обеспечению защиты информации страховой организацией», пунктом 3 порядка и сроков составления отчетности по форме 0420266 «Сведения об оценке выполнения требований к обеспечению защиты информации негосударственным пенсионным фондом», пунктом 3 порядка составления отчетности (отчета) по форме 0420722 «Сведения об оценке выполнения требований к обеспечению защиты информации оператором инвестиционной платформы, оператором финансовой платформы, оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, и оператором обмена цифровых финансовых активов».

Таблица 1.1

№ п/п	Требования к технологическим мерам защиты информации
Общие требования к обеспечению защиты информации	
1	Требование подпункта 1.10.1 пункта 1.10
Требования к обеспечению защиты информации, применяемые на технологическом участке идентификации, аутентификации и авторизации клиентов некредитных финансовых организаций в целях осуществления финансовых операций	
2	Требование абзаца второго подпункта 1.10.2 пункта 1.10
3	Требование абзаца третьего подпункта 1.10.2 пункта 1.10
Требования к обеспечению защиты информации, применяемые на технологическом участке формирования (подготовки), передачи и приема электронных сообщений	
4	Требование абзаца второго подпункта 1.10.3 пункта 1.10
5	Требование абзаца третьего подпункта 1.10.3 пункта 1.10
6	Требование абзаца четвертого подпункта 1.10.3 пункта 1.10
7	Требование абзаца пятого подпункта 1.10.3 пункта 1.10
8	Требование абзаца шестого подпункта 1.10.3 пункта 1.10
Требования к обеспечению защиты информации, применяемые на технологическом участке удостоверения права клиентов некредитных финансовых организаций распоряжаться денежными средствами, ценными бумагами или иным имуществом	
9	Требование абзаца второго подпункта 1.10.4 пункта 1.10
10	Требование абзаца третьего подпункта 1.10.4 пункта 1.10
Требования к обеспечению защиты информации, применяемые на технологическом участке осуществления финансовой операции, учета результатов ее осуществления (при наличии учета)	
11	Требование абзаца второго подпункта 1.10.5 пункта 1.10
12	Требование абзаца третьего подпункта 1.10.5 пункта 1.10
13	Требование абзаца четвертого подпункта 1.10.5 пункта 1.10
14	Требование абзаца пятого подпункта 1.10.5 пункта 1.10

2. Рекомендуемый перечень дополнительных требований, установленных Положением Банка России № 757-П в отношении некредитных финансовых организаций, являющихся операторами финансовой платформы, приведен в таблице 1.2.

Таблица 1.2

№ п/п	Требования к технологическим мерам защиты информации
1	Требование абзаца второго подпункта 2.2.1 пункта 2.2
2	Требование абзаца третьего подпункта 2.2.1 пункта 2.2
3	Требование абзаца четвертого подпункта 2.2.1 пункта 2.2
4	Требование абзаца пятого подпункта 2.2.1 пункта 2.2
5	Требование подпункта 2.2.2 пункта 2.2
6	Требование пункта 2.3

3. Рекомендуемый перечень дополнительных требований, установленных Положением Банка России № 757-П в отношении некредитных финансовых организаций, являющихся операторами информационной системы, в которых осуществляется выпуск цифровых финансовых активов, операторами обмена цифровых финансовых активов, приведен в таблице 1.3.

Таблица 1.3

№ п/п	Требования к технологическим мерам защиты информации
1	Требование абзаца второго пункта 3.2
2	Требование абзаца третьего пункта 3.2
3	Требование абзаца четвертого пункта 3.2
4	Требование абзаца пятого пункта 3.2
5	Требование абзаца шестого пункта 3.2
6	Требование абзаца седьмого пункта 3.2
7	Требование абзаца восьмого пункта 3.2
8	Требование абзаца девятого пункта 3.2
9	Требование абзаца второго пункта 3.3
10	Требование абзаца третьего пункта 3.3
11	Требование абзаца четвертого пункта 3.3 (до дня вступления указанного абзаца в силу может не учитываться при оценке выполнения требования)

Приложение 2
к Методическим рекомендациям по расчету значений показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в целях составления отчетности об оценке выполнения требований к обеспечению защиты информации некредитными финансовыми организациями

Перечень требований к прикладному программному обеспечению автоматизированных систем и приложений по направлению «Безопасность программного обеспечения»

Рекомендуемый перечень требований, установленных Положением Банка России № 757-П в отношении некредитных финансовых организаций, выполнение которых оценивается при выборе соответствующего аналитического признака, характеризующего вид деятельности отчитывающейся организации[2], приведен в таблице 2.1.

Таблица 2.1

№ п/п	Требования к прикладному программному обеспечению автоматизированных систем и приложений
1	Требование пункта 1.8 (в отношении прикладного программного обеспечения автоматизированных систем и приложений, распространяемых некредитными финансовыми организациями своим клиентам для совершения действий в целях осуществления финансовых операций)
2	Требование пункта 1.8 (в отношении программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет»)

[2] Аналитические признаки, характеризующие вид деятельности отчитывающихся организаций определены пунктом 4 порядка и сроков составления отчетности по форме 0420433 «Сведения об оценке выполнения требований к обеспечению защиты информации профессиональными участниками рынка ценных бумаг, организаторами торговли, клиринговыми организациями», пунктом 4 порядка и сроков составления отчетности по форме 0420175 «Сведения об оценке выполнения требований к обеспечению защиты информации страховой организацией», пунктом 4 порядка и сроков составления отчетности по форме 0420266 «Сведения об оценке выполнения требований к обеспечению защиты информации негосударственным пенсионным фондом», пунктом 4 порядка составления отчетности (отчета) по форме 0420722 «Сведения об оценке выполнения требований к обеспечению защиты информации оператором инвестиционной платформы, оператором финансовой платформы, оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, и оператором обмена цифровых финансовых активов».