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

02.11.2022 № 12-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.

1.2. Настоящими Методическими рекомендациями рекомендуется руководствоваться следующим отчитывающимся организациям:

кредитным организациям при составлении отчетности по форме 0409071 «Сведения об оценке выполнения кредитными организациями требований к обеспечению защиты информации»;

операторам услуг платежной инфраструктуры, осуществляющим деятельность операционных центров и (или) платежных клиринговых центров, не являющимся кредитными организациями, при составлении отчетности по форме 0403202 «Сведения об оценке выполнения операторами

услуг платежной инфраструктуры требований к обеспечению защиты информации при осуществлении деятельности операционного центра, платежного клирингового центра».

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:

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

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:

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

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:

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

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 кредитной 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 кредитной 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, указанных в приложении 2 к настоящим методическим рекомендациям;

$E_{Рм_i}$ – 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:

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

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;

$Е_{Кп_i}$ – 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;

$Е_{Кз_i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля знаний работников кредитной 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 кредитной 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 ($Е_{ПОС}$), рекомендуется рассчитывать по формуле:

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

где i – порядковый номер оцениваемых требований;

N – общее количество требований;

$Е_{Си_i}$ – 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» ($E_{ПО}$) рекомендуется рассчитывать по формуле:

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

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

$E_{ПОР}$ – значение оценки, характеризующей выполнение требований в

рамках процесса реализации мер защиты информации, рассчитанное в соответствии с пунктом 3.4 настоящей главы;

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

$E_{ПОС}$ – 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**

4.1. Настоящие Методические рекомендации подлежат официальному опубликованию на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

Заместитель Председателя
Банка России Р.Н. Вестеровский

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

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

1. Рекомендуемый перечень требований, установленных Положением Банка России от 17.04.2019 № 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» (с изменениями) (далее – Положение Банка России № 683-П) в отношении кредитных организаций, выполнение которых оценивается при выборе кода вида деятельности «Банк»[1], приведен в таблице 1.1 настоящего приложения.

2. Рекомендуемый перечень требований, установленных Положением Банка России от 04.06.2020 № 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» (далее – Положение Банка России № 719-П) в отношении кредитных организаций, выполнение которых оценивается

[1] Коды вида деятельности отчитывающихся кредитных организаций определены пунктом 4.2 порядка составления и представления отчетности по форме 0409071 «Сведения об оценке выполнения кредитными организациями требований к обеспечению защиты информации».

при выборе кода вида деятельности «ОПДС», приведен в таблице 1.2 настоящего приложения.

3. Рекомендуемый перечень требований, установленных Положением Банка Росси от 23.12.2020 № 747-П «О требованиях к защите информации в платежной системе Банка России»[2] (далее – Положение Банка России № 747-П) в отношении кредитных организаций, выполнение которых оценивается при выборе кода вида деятельности «Участник ПС БР», приведен в таблице 1.3 настоящего приложения.

4. Рекомендуемый перечень требований, установленных Положением Банка России № 719-П в отношении операторов услуг платежной инфраструктуры, осуществляющих деятельность расчетного центра, выполнение которых оценивается при выборе кода вида деятельности «ОУПИ РЦ», приведен в таблице 1.4 настоящего приложения.

5. Рекомендуемый перечень требований, установленных Положением Банка России № 719-П в отношении операторов услуг платежной инфраструктуры, осуществляющих деятельность операционного центра, выполнение которых оценивается при выборе кода вида деятельности «ОУПИ ОЦ», «ОЦ»[3], приведен в таблице 1.5 настоящего приложения.

6. Рекомендуемый перечень требований, установленных Положением Банка России № 719-П в отношении операторов услуг платежной инфраструктуры, осуществляющих деятельность платежного клирингового центра, выполнение которых оценивается при выборе кода вида

---

[2] С даты признания утратившим силу Положения Банка России № 747-П расчет значений показателей оценки выполнения требований по направлению «Технологические меры» необходимо осуществлять в отношении аналогичных требований Положения Банка России от 25.07.2022 № 802-П «О требованиях к защите информации в платежной системе Банка России».

[3] Коды вида деятельности отчитывающихся организаций, не являющихся кредитными организациями, определены пунктом 1.1 методики составления отчетности по форме 0403202 «Сведения об оценке выполнения операторами услуг платежной инфраструктуры требований к обеспечению защиты информации при осуществлении деятельности операционного центра, платежного клирингового центра».

деятельности «ОУПИ ПКЦ», «ПКЦ», приведен в таблице 1.6 настоящего приложения.

Таблица 1.1. Перечень требований, установленных Положением Банка России № 683-П в отношении кредитных организаций

№ п/п	Требование к технологическим мерам защиты информации
Общие требования к обеспечению защиты информации	
1	Требование подпункта 5.1 пункта 5
2	Требование пункта 6
Требования к обеспечению защиты информации, применяемые на всех технологических участках, указанных в пункте 5.2	
3	Требование абзаца третьего подпункта 5.2.1 пункта 5
4	Требование абзаца семнадцатого подпункта 5.2.1 пункта 5
Требования к обеспечению защиты информации, применяемые на технологическом участке идентификации, аутентификации и авторизации клиентов при совершении действий в целях осуществления банковских операций	
5	Требование абзаца второго подпункта 5.2.1 пункта 5
Требования к обеспечению защиты информации, применяемые на технологическом участке формирования (подготовки), передачи и приема документов, связанных с осуществлением переводов денежных средств, составленных в электронном виде (далее – электронные сообщения)	
6	Требование абзаца пятого подпункта 5.2.1 пункта 5
7	Требование абзаца шестого подпункта 5.2.1 пункта 5
8	Требование абзаца седьмого подпункта 5.2.1 пункта 5
9	Требование абзаца восьмого подпункта 5.2.1 пункта 5
10	Требование абзаца девятого подпункта 5.2.1 пункта 5
Требования к обеспечению защиты информации, применяемые на технологическом участке удостоверения права клиентов кредитных организаций распоряжаться денежными средствами	
11	Требование абзаца одиннадцатого подпункта 5.2.1 пункта 5
12	Требование абзаца двенадцатого подпункта 5.2.1 пункта 5
Требования к обеспечению защиты информации, применяемые на технологическом участке осуществления банковской операции и учета результатов ее осуществления	
13	Требование абзаца четырнадцатого подпункта 5.2.1 пункта 5
14	Требование абзаца пятнадцатого подпункта 5.2.1 пункта 5
15	Требование абзаца шестнадцатого подпункта 5.2.1 пункта 5

Таблица 1.2. Перечень требований, установленных Положением Банка России № 719-П в отношении кредитных организаций

№ п/п	Требование к технологическим мерам защиты информации
1	Требование абзаца второго пункта 2.9
2	Требование абзаца третьего пункта 2.9
3	Требование абзаца четвертого пункта 2.9
4	Требование абзаца пятого пункта 2.9
5	Требование абзаца шестого пункта 2.9

№ п/п	Требование к технологическим мерам защиты информации
6	Требование абзаца седьмого пункта 2.9
7	Требование абзаца восьмого пункта 2.9
8	Требование абзаца девятого пункта 2.9

Таблица 1.3. Перечень требований, установленных Положением Банка России № 747-П в отношении кредитных организаций

№ п/п	Требование к технологическим мерам защиты информации
Требования к обеспечению защиты информации в платежной системе Банка России для участника обмена, осуществляющего переводы денежных средств с использованием сервиса срочного перевода и сервиса несрочного перевода (далее – участник ССНП), и для участника обмена, осуществляющего переводы денежных средств с использованием сервиса быстрых платежей (далее – участник СБП)	
1	Требование абзаца второго подпункта 7.2 пункта 7
2	Требование абзаца третьего подпункта 7.2 пункта 7
3	Требование абзаца четвертого подпункта 7.2 пункта 7
Требования к обеспечению защиты информации в платежной системе Банка России для участника СБП при обмене электронными сообщениями при осуществлении переводов денежных средств	
4	Требование подпункта 14.1 пункта 14
5	Требование абзаца второго подпункта 14.2 пункта 14
6	Требование абзаца третьего подпункта 14.2 пункта 14
7	Требование абзаца четвертого подпункта 14.2 пункта 14
Требования к обеспечению защиты информации в платежной системе Банка России для участника ССНП при передаче электронных сообщений в Банк России	
8	Требование абзаца второго подпункта 14.3 пункта 14
9	Требование абзаца третьего подпункта 14.3 пункта 14
10	Требование абзаца четвертого подпункта 14.3 пункта 14
11	Требование абзаца пятого подпункта 14.3 пункта 14
12	Требование абзаца шестого подпункта 14.3 пункта 14

Таблица 1.4. Перечень требований, установленных Положением Банка России № 719-П в отношении операторов услуг платежной инфраструктуры, осуществляющих деятельность расчетного центра

№ п/п	Требование к технологическим мерам защиты информации
Требования по реализации технологических мер защиты информации при осуществлении операторами услуг платежной инфраструктуры, осуществляющими деятельность расчетных центров (далее – РЦ), операций по исполнению поступивших от платежного клирингового центра (далее – ПКЦ) электронных сообщений ПКЦ, операторов по переводу денежных средств посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств	

№ п/п	Требование к технологическим мерам защиты информации
Требования к обеспечению защиты информации, применяемые на технологическом участке формирования (подготовки), передачи и приема электронных сообщений	
1	Требование подпункта 1.3 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при приеме РЦ поступивших от ПКЦ, операционных центров (далее – ОЦ) электронных сообщений ПКЦ, операторов по переводу денежных средств в целях списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств
2	Требование подпункта 1.3 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при направлении РЦ в адрес ПКЦ электронных сообщений, содержащих извещения об исполнении посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств, поступивших от ПКЦ электронных сообщений
3	Требование подпункта 1.4 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при приеме РЦ поступивших от ПКЦ, ОЦ электронных сообщений ПКЦ, операторов по переводу денежных средств в целях списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств
4	Требование подпункта 1.4 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при направлении РЦ в адрес ПКЦ электронных сообщений, содержащих извещения об исполнении посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств, поступивших от ПКЦ электронных сообщений
5	Требование подпункта 1.6 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при приеме РЦ поступивших от ПКЦ, ОЦ электронных сообщений ПКЦ, операторов по переводу денежных средств в целях списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств
6	Требование подпункта 1.6 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при направлении РЦ в адрес ПКЦ электронных сообщений, содержащих извещения об исполнении посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств, поступивших от ПКЦ электронных сообщений
7	Требование подпункта 1.8 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при направлении РЦ в адрес ПКЦ электронных сообщений, содержащих извещения об исполнении посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств, поступивших от ПКЦ электронных сообщений

№ п/п	Требование к технологическим мерам защиты информации
8	Требование подпункта 1.9 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению № Банка России 719-П при направлении РЦ в адрес ПКЦ электронных сообщений, содержащих извещения об исполнении посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств, поступивших от ПКЦ электронных сообщений
Требования к обеспечению защиты информации, применяемые на технологическом участке осуществления операций по переводу денежных средств, учета результатов их осуществления	
9	Требование подпункта 1.3 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при исполнении РЦ поступивших от ПКЦ электронных сообщений ПКЦ, операторов по переводу денежных средств посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств
10	Требование подпункта 1.8 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при исполнении РЦ поступивших от ПКЦ электронных сообщений ПКЦ, операторов по переводу денежных средств посредством списания и зачисления денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств
Требования к обеспечению защиты информации, применяемые на технологическом участке хранения электронных сообщений и информации об осуществленных переводах денежных средств	
11	Требование подпункта 1.10 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при хранении РЦ информации об осуществленных списаниях и зачислениях денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств
12	Требование подпункта 1.10 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при хранении РЦ электронных сообщений, обмен которыми осуществлялся при взаимодействии РЦ с операторами услуг платежной инфраструктуры
13	Требование подпункта 1.11 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 10 приложения 2 к Положению Банка России № 719-П при хранении РЦ информации об осуществленных списаниях и зачислениях денежных средств по банковским (корреспондентским) счетам операторов по переводу денежных средств

Таблица 1.5. Перечень требований, установленных Положением Банка России № 719-П в отношении операторов услуг платежной инфраструктуры, осуществляющих деятельность операционного центра

№ п/п	Требование к технологическим мерам защиты информации
Требования к обеспечению защиты информации при обмене электронными сообщениями между операторами по переводу денежных средств, между операторами по переводу денежных средств и их клиентами, ПКЦ, РЦ, между ПКЦ и РЦ	
Требования к обеспечению защиты информации, применяемые на технологическом участке формирования (подготовки), передачи и приема электронных сообщений	
1	Требование подпункта 1.3 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 6 приложения 2 к Положению Банка России № 719-П при приеме и передаче электронных сообщений между операторами по переводу денежных средств и их клиентами, операторами услуг платежной инфраструктуры
2	Требование подпункта 1.4 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 6 приложения 2 к Положению Банка России № 719-П при приеме и передаче электронных сообщений между операторами по переводу денежных средств и их клиентами, операторами услуг платежной инфраструктуры
3	Требование подпункта 1.6 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 6 приложения 2 к Положению Банка России № 719-П при приеме и передаче электронных сообщений между операторами по переводу денежных средств и их клиентами, операторами услуг платежной инфраструктуры
4	Требование подпункта 1.9 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 6 приложения 2 к Положению Банка России № 719-П при приеме и передаче электронных сообщений между операторами по переводу денежных средств и их клиентами, операторами услуг платежной инфраструктуры
Требования к обеспечению защиты информации, применяемые на технологическом участке хранения электронных сообщений и информации об осуществленных переводах денежных средств	
5	Требование подпункта 1.10 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 6 приложения 2 к Положению Банка России № 719-П при хранении ОЦ электронных сообщений, обмен которыми осуществлялся при взаимодействии ОЦ с операторами по переводу денежных средств, их клиентами, операторами услуг платежной инфраструктуры
6	Требование подпункта 1.11 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 6 приложения 2 к Положению Банка России № 719-П при хранении ОЦ электронных сообщений, обмен которыми осуществлялся при взаимодействии ОЦ с операторами по переводу денежных средств, их клиентами, операторами услуг платежной инфраструктуры

Таблица 1.6. Перечень требований, установленных Положением Банка России № 719-П в отношении операторов услуг платежной инфраструктуры, осуществляющих деятельность платежного клирингового центра

№ п/п	Требование к технологическим мерам защиты информации
Требования к обеспечению защиты информации при осуществлении операций по выполнению процедур приема к исполнению электронных сообщений операторов по переводу денежных средств, включая проверку соответствия электронных сообщений операторов по переводу денежных средств установленным требованиям, определение достаточности денежных средств для исполнения электронных сообщений операторов по переводу денежных средств и определение платежных клиринговых позиций	
Требования к обеспечению защиты информации, применяемые на технологическом участке формирования (подготовки), передачи и приема электронных сообщений	
1	Требование подпункта 1.3 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при приеме ПКЦ электронных сообщений операторов по переводу денежных средств
2	Требование подпункта 1.3 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при направлении ПКЦ в адрес операторов по переводу денежных средств электронных сообщений, содержащих извещения, касающиеся приема к исполнению электронных сообщений операторов по переводу денежных средств
3	Требование подпункта 1.4 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при приеме ПКЦ электронных сообщений операторов по переводу денежных средств
4	Требование подпункта 1.6 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при приеме ПКЦ электронных сообщений операторов по переводу денежных средств
5	Требование подпункта 1.6 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при направлении ПКЦ в адрес операторов по переводу денежных средств электронных сообщений, содержащих извещения, касающиеся приема к исполнению электронных сообщений операторов по переводу денежных средств
6	Требование подпункта 1.8 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при направлении ПКЦ в адрес операторов по переводу денежных средств электронных сообщений, содержащих извещения, касающиеся приема к исполнению электронных сообщений операторов по переводу денежных средств
7	Требование подпункта 1.9 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при направлении ПКЦ в адрес операторов по переводу денежных средств электронных сообщений, содержащих извещения, касающиеся приема к исполнению электронных сообщений операторов по переводу денежных средств

№ п/п	Требование к технологическим мерам защиты информации
Требования к обеспечению защиты информации, применяемые на технологическом участке осуществления операций по переводу денежных средств, учета результатов их осуществления	
8	Требование подпункта 1.3 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при проверке ПКЦ соответствия электронных сообщений операторов по переводу денежных средств установленным требованиям
9	Требование подпункта 1.3 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при определении ПКЦ достаточности денежных средств для исполнения электронных сообщений операторов по переводу денежных средств, в том числе путем обмена электронными сообщениями с операторами услуг платежной инфраструктуры
10	Требование подпункта 1.3 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при определении ПКЦ платежных клиринговых позиций для исполнения принятых электронных сообщений операторов по переводу денежных средств
11	Требование подпункта 1.4 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при определении ПКЦ достаточности денежных средств для исполнения электронных сообщений операторов по переводу денежных средств, в том числе путем обмена электронными сообщениями с операторами услуг платежной инфраструктуры
12	Требование подпункта 1.6 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при определении ПКЦ достаточности денежных средств для исполнения электронных сообщений операторов по переводу денежных средств, в том числе путем обмена электронными сообщениями с операторами услуг платежной инфраструктуры
13	Требование подпункта 1.8 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при определении ПКЦ достаточности денежных средств для исполнения электронных сообщений операторов по переводу денежных средств, в том числе путем обмена электронными сообщениями с операторами услуг платежной инфраструктуры
14	Требование подпункта 1.8 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при определении ПКЦ платежных клиринговых позиций для исполнения принятых электронных сообщений операторов по переводу денежных средств
15	Требование подпункта 1.9 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при определении ПКЦ достаточности денежных средств для исполнения электронных сообщений операторов по переводу денежных средств, в том числе путем обмена электронными сообщениями с операторами услуг платежной инфраструктуры
Требования к обеспечению защиты информации, применяемые на технологическом участке хранения электронных сообщений и	

№ п/п	Требование к технологическим мерам защиты информации
информации об осуществленных переводах денежных средств	
16	Требование подпункта 1.10 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению Банка России № 719-П при хранении ПКЦ электронных сообщений, обмен которыми осуществлялся при взаимодействии ПКЦ с операторами услуг платежной инфраструктуры
17	Требование подпункта 1.11 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 7 приложения 2 к Положению № 719-П при хранении ПКЦ электронных сообщений, обмен которыми осуществлялся при взаимодействии ПКЦ с операторами услуг платежной инфраструктуры
Требования к обеспечению защиты информации при передаче РЦ для исполнения электронных сообщений ПКЦ, принятых электронных сообщений операторов по переводу денежных средств	
Требования к обеспечению защиты информации, применяемые на технологическом участке формирования (подготовки), передачи и приема электронных сообщений	
18	Требование подпункта 1.3 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 8 приложения 2 к Положению Банка России № 719-П при формировании ПКЦ электронных сообщений по осуществлению операций по банковским (корреспондентским) счетам операторов по переводу денежных средств, передаче электронных сообщений в адрес операторов услуг платежной инфраструктуры
19	Требование подпункта 1.4 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 8 приложения 2 к Положению Банка России № 719-П при формировании ПКЦ электронных сообщений по осуществлению операций по банковским (корреспондентским) счетам операторов по переводу денежных средств, передаче электронных сообщений в адрес операторов услуг платежной инфраструктуры
20	Требование подпункта 1.6 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 8 приложения 2 к Положению Банка России № 719-П при формировании ПКЦ электронных сообщений по осуществлению операций по банковским (корреспондентским) счетам операторов по переводу денежных средств, передаче электронных сообщений в адрес операторов услуг платежной инфраструктуры
21	Требование подпункта 1.8 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 8 приложения 2 к Положению Банка России № 719-П при формировании ПКЦ электронных сообщений по осуществлению операций по банковским (корреспондентским) счетам операторов по переводу денежных средств, передаче электронных сообщений в адрес операторов услуг платежной инфраструктуры
22	Требование подпункта 1.9 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 8 приложения 2 к Положению Банка России № 719-П при формировании ПКЦ электронных сообщений по осуществлению операций по банковским (корреспондентским) счетам операторов по переводу денежных средств, передаче электронных сообщений в адрес операторов услуг платежной инфраструктуры

№ п/п	Требование к технологическим мерам защиты информации
Требования к обеспечению защиты информации, применяемые на технологическом участке хранения электронных сообщений и информации об осуществленных переводах денежных средств	
23	Требование подпункта 1.10 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 8 приложения 2 к Положению Банка России № 719-П при хранении ПКЦ электронных сообщений, обмен которыми осуществлялся при взаимодействии ПКЦ с операторами услуг платежной инфраструктуры
24	Требование подпункта 1.11 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 8 приложения 2 к Положению Банка России № 719-П при хранении ПКЦ электронных сообщений, обмен которыми осуществлялся при взаимодействии ПКЦ с операторами услуг платежной инфраструктуры
Требования к обеспечению защиты информации при направлении операторам по переводу денежных средств извещений (подтверждений), касающихся приема к исполнению электронных сообщений операторов по переводу денежных средств, а также передаче извещений (подтверждений), касающихся исполнения электронных сообщений операторов по переводу денежных средств	
Требования к обеспечению защиты информации, применяемые на технологическом участке формирования (подготовки), передачи и приема электронных сообщений	
25	Требование подпункта 1.3 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 9 приложения 2 к Положению Банка России № 719-П при направлении ПКЦ в адрес операторов по переводу денежных средств электронных сообщений, содержащих извещения о приеме, об исполнении принятых электронных сообщений операторов по переводу денежных средств
26	Требование подпункта 1.4 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 9 приложения 2 к Положению Банка России № 719-П при направлении ПКЦ в адрес операторов по переводу денежных средств электронных сообщений, содержащих извещения о приеме, об исполнении принятых электронных сообщений операторов по переводу денежных средств
27	Требование подпункта 1.6 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 9 приложения 2 к Положению Банка России № 719-П при направлении ПКЦ в адрес операторов по переводу денежных средств электронных сообщений, содержащих извещения о приеме, об исполнении принятых электронных сообщений операторов по переводу денежных средств
28	Требование подпункта 1.8 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 9 приложения 2 к Положению Банка России № 719-П при направлении ПКЦ в адрес операторов по переводу денежных средств электронных сообщений, содержащих извещения о приеме, об исполнении принятых электронных сообщений операторов по переводу денежных средств
Требования к обеспечению защиты информации, применяемые на технологическом участке хранения электронных сообщений и информации об осуществленных переводах денежных средств	
29	Требование подпункта 1.10 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 9 приложения 2 к

№ п/п	Требование к технологическим мерам защиты информации
	Положению Банка России № 719-П при хранении ПКЦ электронных сообщений, обмен которыми осуществлялся при взаимодействии ПКЦ с операторами услуг платежной инфраструктуры
30	Требование подпункта 1.11 пункта 1 приложения 1 к Положению Банка России № 719-П, реализуемое в соответствии со строкой 9 приложения 2 к Положению Банка России № 719-П при хранении ПКЦ электронных сообщений, обмен которыми осуществлялся при взаимодействии ПКЦ с операторами услуг платежной инфраструктуры

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 Банка России об оценке выполнения требований к обеспечению защиты информации

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

1. Рекомендуемый перечень требований, установленных Положением Банка России № 683-П в отношении кредитных организаций, оцениваемый при выборе кода вида деятельности «Банк»[4], приведен в таблице 2.1 настоящего приложения.

2. Рекомендуемый перечень требований, установленных Положением Банка России № 719-П в отношении операторов по переводу денежных средств, операторов услуг платежной инфраструктуры, выполнение которых оценивается при выборе кода вида деятельности «ОПДС», «ОУПИ РЦ», «ОУПИ ОЦ», «ОУПИ ПКЦ», «ОЦ» или «ПКЦ»[5], приведен в таблице 2.2 настоящего приложения.

---

[4] Коды вида деятельности отчитывающихся кредитных организаций определены пунктом 5.2 порядка составления и представления отчетности по форме 0409071 «Сведения об оценке выполнения кредитными организациями требований к обеспечению защиты информации».

[5] Коды вида деятельности отчитывающихся организаций, не являющихся кредитными организациями, определены пунктом 1.1 методики составления отчетности по форме 0403202 «Сведения об оценке выполнения операторами услуг платежной инфраструктуры требований к обеспечению защиты информации при осуществлении деятельности операционного центра, платежного клирингового центра».

Таблица 2.1. Перечень требований, установленных Положением Банка России № 683-П в отношении кредитных организаций

№ п/п	Требование к прикладному программному обеспечению автоматизированных систем и приложений
1	Требование подпункта 4.1 пункта 4 Положения Банка России № 683-П (в отношении прикладного программного обеспечения автоматизированных систем и приложений, распространяемых кредитной организацией клиентам для совершения действий в целях осуществления банковских операций)
2	Требование подпункта 4.1 пункта 4 Положения Банка России № 683-П (в отношении программного обеспечения, обрабатывающего защищаемую информацию на участках, используемых для приема электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет»)

Таблица 2.2. Перечень требований, установленных Положением Банка России № 719-П в отношении операторов по переводу денежных средств, операторов услуг платежной инфраструктуры

№ п/п	Требование к прикладному программному обеспечению автоматизированных систем и приложений
1	Требование пункта 1.2 Положения Банка России № 719-П (в отношении прикладного программного обеспечения автоматизированных систем и приложений, распространяемых клиентам операторов по переводу денежных средств для совершения действий, непосредственно связанных с осуществлением переводов денежных средств)
2	Требование пункта 1.2 Положения Банка России № 719-П (в отношении программного обеспечения, эксплуатируемого на участках, используемых для приема электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет»)