М Е Т О Д И К А

анализа и оценки риска информационной безопасности в Платежной системе «КП Ритейл»

г. Москва, 2023 г.

ОГЛАВЛЕНИЕ

1. Общие положения

1.1. Настоящая Методика анализа и оценки риска информационной безопасности в Платежной системе «КП Ритейл» (далее по тексту – Методика, платежная система) определяет порядок (процедуру) выявления наиболее критичных угроз информационной безопасности и уязвимостей в отношении Объектов информационной инфраструктуры субъекта платежной системы и выбор мер противодействия данным угрозам, а также основные понятия и роли, задает инфраструктуру по анализу и оценке риска информационной безопасности, вводит разграничение ответственности.

1.2. Реализация положений настоящей Методики предназначена для достижения следующих целей:

- своевременного выявления риска информационной безопасности;
- разработки и внедрения мер и средств по обеспечению информационной безопасности, направленных на снижение выявленного риска информационной безопасности;
- регламентации методологии анализа и оценки риска информационной безопасности и порядка документирования результатов.

1.3. Общее руководство и контроль выполнения положений настоящей Методики возложены на Оператора платежной системы.

1.4. Пересмотр положений настоящей Методики проводится по мере необходимости, в том числе:

- при внесении изменений в законодательство Российской Федерации и нормативные акты Банка России в области информационной безопасности;
- при изменении Бизнес-процессов, осуществляемых в рамках платежной системы;
- при изменении используемых технологий работы в платежной системе;
- при изменении структуры информационных и/или телекоммуникационных систем (или при введении новых), применении новых технологий передачи, хранения и обработки информации в платежной системе;
- по фактам возникновения уязвимостей и иных значимых событий риска информационной безопасности по решению Оператора платежной системы.

1.5. Предложения по пересмотру или внесению изменений в настоящую Методику могут вносить все субъекты платежной системы.

1.6. Термины используются в значении, определенном в составе Методики анализа и реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе «КП Ритейл», утверждаемой Оператором платежной системы.

2. Порядок проведения анализа и оценки риска информационной безопасности

2.1. Общие положения

2.1.1.Анализ риска информационной безопасности проводится не реже, чем 1 (Один) раз в год, а также по мере необходимости, при наступлении нижеперечисленных событий для полной или частичной переоценки риска и уточнения плана обработки риска информационной безопасности:

- изменение политики информационной безопасности Субъекта платежной системы;
- изменение шкалы оценки важности объектов среды Субъекта платежной системы;
- существенное изменение порядка ведения Бизнес-процессов в платежной системе;
- внесение изменений в состав критичных объектов среды, появление новых групп и/или новых объектов среды;
- внесение изменений в операционные и технологические средства и процедуры платежной системы, применение новых технологий передачи, хранения и обработки информации;

– по фактам возникновения уязвимостей и иных значимых событий риска информационной безопасности;
– изменение внешних условий (появление высокомотивированных источников угроз и т.п.).

2.1.2.Процесс анализа риска информационной безопасности состоит из следующих этапов:

– подготовительный этап (утверждение шкал и пороговых значений, пересмотр каталогов угроз и уязвимостей);
– идентификация и оценка важности объектов среды;
– разработка сценариев угроз для Объектов информационной инфраструктуры;
– оценка уровня риска информационной безопасности;
– обработка риска информационной безопасности.

2.1.3.Оценка (переоценка) риска информационной безопасности должна проводиться на регулярной основе, а также, при необходимости, в следующих случаях:

– появление новых Бизнес-процессов/существенное изменение существующих Бизнес-процессов у Субъекта платежной системы;
– появление новых/модернизация существующих автоматизированных систем у Субъекта платежной системы, входящих в состав информационной инфраструктуры платежной системы;
– изменение в организационной структуре Субъекта платежной системы;
– изменение внешних факторов (экономическая, социальная, политическая обстановка), способных привести к появлению новых источников риска для Субъекта платежной системы.

2.1.4.Оценка риска информационной безопасности проводится в отношении всех информационных активов Субъекта платежной системы. Перечень типов информационных активов формируется на основе результатов проведения Субъектом платежной системы классификации информационных активов. Информационные активы Субъекта платежной системы рассматриваются в совокупности с соответствующими им объектами среды. При этом обеспечение свойств информационной безопасности для информационных активов выражается в создании необходимой защиты соответствующих им объектов среды.

2.1.5.Для каждого идентифицированного информационного актива, должны быть определены бизнес-требования и требования законодательства Российской Федерации и оценен возможный ущерб для Системы, возникающий вследствие нарушения конфиденциальности, целостности или доступности информационного актива, а также несоблюдения требований законодательства Российской Федерации и договорных обязательств. Величина вероятного ущерба определяет ценность информационного актива.

2.1.6.Для каждого информационного актива производится идентификация и анализ угроз и уязвимостей, включая оценку вероятности осуществления угроз. Для идентификации угроз безопасности за основу берутся «модель угроз» и «модель нарушителя». В качестве исходных данных для анализа угроз и уязвимостей могут использоваться результаты внутреннего и внешнего аудитов, данные об уязвимостях и событиях риска информационной безопасности, внешние авторитетные источники информации, а также экспертные оценки пользователей и владельцев информационных активов, специалистов в области информационной безопасности и информационных технологий, внешних консультантов.

2.1.7.Величина риска информационной безопасности определяется размером возможного ущерба от реализации угроз информационной безопасности, использующих уязвимости информационных активов. Эта величина напрямую зависит от ценности информационного актива, которому может быть нанесен ущерб и вероятности осуществления угрозы.

2.1.8.Все выявленные источники риска информационной безопасности подлежат ранжированию в порядке убывания их величины и должны быть формализованы в виде отчета об уровне риска информационной безопасности, в котором должны быть отмечены риски, превышающие максимально допустимый уровень остаточных рисков, утвержденный Субъектом платежной системы, и, следовательно, требующие обработки.

2.1.9.Ответственным за процесс анализа и оценки риска информационной безопасности является структурное подразделение, отвечающее за управление риском информационной безопасности, которое совместно с владельцами объектов среды осуществляет анализ и оценку риска, разработку мер по обработке риска, и предоставляет результаты для анализа руководству Субъекта платежной системы и Оператору платежной системы.

2.2. Подготовительный этап

2.2.1. Обновление каталога угроз информационной безопасности

2.2.1.1. На данном этапе должен быть разработан, а затем периодически обновляться каталог угроз информационной безопасности, характерных для Объектов информационной инфраструктуры Субъекта платежной системы. Обновление каталога угроз информационной безопасности осуществляется по результатам:

- анализа событий риска информационной безопасности;
- анализа результатов аудитов;
- сообщений пользователей;
- собственных предположений и/или предположений владельцев процессов о возможных или новых угрозах для Объектов информационной инфраструктуры.

2.2.1.2. На данном этапе также определяются и возможные уязвимости, через которые реализуются угрозы информационной безопасности.

2.2.1.3. Результатом данного этапа является актуальный каталог угроз и уязвимостей информационной безопасности.

2.2.2. Пересмотр шкал

2.2.2.1. Перед каждым очередным анализом риска информационной безопасности необходимо пересматривать основные шкалы оценки:

- шкала важности объектов среды;
- шкала вероятности реализации сценариев;
- шкала последствий реализации угрозы;
- шкала штрафных санкций регуляторов (Банк России, ФСБ, ФСТЭК).

2.2.2.2. Перед проведением очередного анализа риска информационной безопасности, вышеперечисленные шкалы формируются или пересматриваются, а затем утверждаются руководством Субъекта платежной системы.

2.3. Идентификация и оценка важности объекта среды

2.3.1.Идентификации подлежат все информационные активы, используемые Субъектом Системы, а также объекты среды. Все объекты среды должны пройти оценку важности.

2.3.2.Для каждого информационного актива, внесенного в реестр, определяются его объекты среды. К перечню объектов среды информационного актива можно отнести:

- линии связи, аппаратные и технические средства;
- маршрутизаторы, коммутаторы, концентраторы;
- программные компоненты передачи данных по компьютерным сетям (сетевые сервисы);
- файлы данных;
- базы данных;
- прикладные программы доступа и обработки информации;
- автоматизированные рабочие места;
- бумажные документы.

2.3.3.Идентификация объектов среды осуществляется техническими специалистами Субъекта платежной системы. Формат перечня объектов среды с указанием их владельцев и важности приведен в Таблице 1:

Таблица 1

Перечень объектов среды

№	Наименование объекта среды	Владелец объекта среды (ФИО, должность, структурное подразделение)	Важность объекта среды
1.	линии связи, аппаратные и технические средства		
2.	маршрутизаторы, коммутаторы, концентраторы		
3.	программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)		
4.	файлы данных		
5.	базы данных		
6.	прикладные программы доступа и обработки информации		
7.	автоматизированные рабочие места		
8.	бумажные документы		

2.3.4.При наличии большого количества однотипных объектов среды (например, типовые автоматизированные рабочие места, типовая документация и т.д.) допускается их группировка, которая осуществляется по согласованию со структурным подразделением, ответственным за управление риском информационной безопасности.

2.3.5.Не допускается группирование объектов среды, разнящихся по следующим признакам:

- по типу представления (например, в бумажном или электронном виде);
- по порядку обработки (обрабатываются с использованием различных средств, сервисов или оборудования);
- по классу важности.

2.3.6.Для каждого выявленного объекта среды (или группы объектов среды) их владельцами должна быть дана экспертная оценка его важности. Важность объекта среды определяется, исходя из ущерба, который будет нанесен Субъекту платежной системы и/или платежной системе, в случае потери свойств информационной безопасности объекта среды. Оценка важности объекта среды проводится в соответствии со шкалой, представленной в Таблице 2:

Таблица 2

Шкала оценки важности объекта среды

Обозначение класса (уровня) важности объекта среды	Возможный ущерб в денежном эквиваленте (млн. рублей)
A (низкий)	
B (средний)	
C (высокий)	

2.3.7.Для дальнейшего анализа риска информационной безопасности берутся объекты среды класса важности B и C.

2.4. Разработка сценариев угроз для идентифицированных объектов среды и/или групп объектов среды

2.4.1.После проведения инвентаризации информационных активов и объектов среды структурное подразделение, отвечающее за управление риском информационной безопасности, составляет следующую таблицу:

Таблица 3

Шаблон таблицы результатов анализа риска информационной безопасности

№ п.п.	Наименование объекта среды (группы объектов среды)	Важность объекта среды	Угроза	Вероятность	Оценка воздействия	Штрафные санкции регуляторов	Текущие контрмеры
1.	линии связи, аппаратные и технические средства						
2.	маршрутизаторы, коммутаторы, концентраторы						
3.	программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)						
4.	файлы данных						
5.	базы данных						
6.	прикладные программы доступа и обработки информации						
7.	автоматизированные рабочие места						
8.	бумажные документы						

2.4.2.В Таблице 3 графа «Угроза» заполняется из актуального каталога угроз (возможный перечень приведен в Приложении № 1 к настоящей Методике), графа

«Важность» заполняется согласно Таблице 2, графа «Вероятность»[1] заполняется для каждого сценария «объект среды - угроза», для которого необходимо экспертно оценить возможность его успешной реализации, заполнив соответствующую ячейку в таблице по шкале, приведенной в Таблице 4.

2.4.3.Оценка возможности реализации данного конкретного сценария определяется экспертным путем на основе:

- мотивации, знаний, возможностей и ресурсов, доступных нарушителю, а также привлекательности информационных активов;
- статистики по имевшим место событиям риска информационной безопасности, как в платежной системе, так и при наличии возможности в международной практике;
- накопленного опыта в данной области.

2.4.4.Возможность реализации угроз также зависит от имеющихся уязвимостей Объектов информационной инфраструктуры, т.е. насколько легко может быть использована та или иная уязвимость (Таблица 4):

Таблица 4

Шкала вероятностей реализации сценария

Высокая вероятность	Угроза ожидаема в любое время; **Или** Подобные инциденты защиты информации происходили ранее, имеется информация по статистике или другая информация, указывающая на то, что угроза, вероятно, произойдет; **Или** Внедренные меры защиты не эффективны; **Или** Имеются веские причины и поводы у нарушителя для выполнения таких действий (высокая мотивация нарушителя); **Или** Для реализации угрозы не требуются специальные навыки, инструменты, знания или финансирование.
Средняя вероятность	Возникновение угрозы зависит от определенных обстоятельств или от последовательности событий с низкой вероятностью возникновения; **Или** Подобные угрозы еще не происходили в платежной системе или у Субъекта платежной системы, но были идентифицированы другими источниками; **Или** Защитные меры если не предотвращают, то значительно препятствуют реализации угрозы; **Или** Есть некоторые причины у нарушителя для выполнения таких действий (средняя мотивация нарушителя); **Или** Реализация угрозы требует специальных навыков, инструментов, финансирования, а также специальных знаний об уязвимостях Объектов информационной инфраструктуры.

[1] Под термином «вероятность» в данном случае понимается степень возможности реализации данной угрозы через данную уязвимость для данного Объекта информационной инфраструктуры, определяемая на основании экспертной оценки.

Низкая вероятность	Угроза реализуема теоретически, но практически это событие едва ли может произойти; **Или** Нет данных по имевшим место событиям риска информационной безопасности, статистики и т.д. либо подобные угрозы очень редки и для реализации требуют наличия специальных предварительных условий; **Или** Внедренные защитные меры предотвращают реализацию угрозы; **Или** Реализация угрозы требует высококвалифицированных специалистов (таких как разработчики программного обеспечения), специальных инструментов или значительного финансирования, недоступного конкурентам.

В графе **«Оценка воздействия»** отражаются последствия реализации угрозы через данную уязвимость, оценка которых производится экспертным методом (Таблица 5):

Таблица 5

Шкала последствий реализации угрозы

Серьезное	Происшествие приводит к невозможности решения критически важных задач, угроза выполнения своих обязательств Субъектом платежной системы.
Среднее	Происшествие с умеренными результатами: ликвидация последствий не связана со значительными затратами для выполнения своих обязательств Субъектом платежной системы в целом, воздействие на Субъекта платежной системы не является критическим и не затрагивает критически важные задачи.
Незначительное	Воздействием можно пренебречь, не существенно для платежной системы в целом.

В графе **«Ущерб от штрафных санкций регуляторов»** отражается оценка влияния ущерба от штрафных санкций регуляторов, которая проводится на основании документов регуляторов по следующим единым критериям (Таблица 6):

Таблица 6

Шкала штрафных санкций регуляторов

Максимальные	Невыполнение требований регуляторов
Минимальные	Выполнение требований регуляторов

В графе **«Текущие контрмеры»** указываются все текущие контрмеры, направленные на снижение вероятности возникновения рассматриваемой угрозы, в том числе в обязательном порядке должны быть указаны как технические меры, так и организационные меры, установленные требованиями Положения Банка России № 719-П от 04.06.2020 «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».

2.5. Оценка уровня риска информационной безопасности

Оценка уровня риска информационной безопасности и риска штрафных санкций регуляторов проводится на основании информации об объектах среды. Для проведения оценки используется табличный метод.

2.5.1. Оценка уровня риска информационной безопасности

2.5.1.1. Величина риска определяется с использованием Таблицы 7 и Таблицы 8.

2.5.1.2. Посредством Таблицы 7 определяется финансовый ущерб для Субъекта платежной системы в результате единичной реализации сценария «объект среды-угроза-уязвимость». На пересечении строк и столбцов матрицы стоят качественные значения ущерба, соответствующие финансовым потерям. Данные качественные значения финансового ущерба совпадают со значениями определения шкалы важности объекта среды.

Примечание: в качестве важности объектов среды, берется максимальное значение из оценок для свойств безопасности, перечисленных в графе «Важность объекта среды» Таблицы 7 для данного информационного актива.

Таблица 7

Значение ущерба для Субъекта платежной системы

Оценка воздействия / **Важность объекта среды**	**Серьезное**	**Среднее**	**Незначительное**
С (высокий)	Высокий	Высокий	Средний
В (средний)	Высокий	Средний	Низкий

2.5.1.3. После определения ущерба, производится оценка риска информационной безопасности в соответствии с матрицей, приведенной в Таблице 8:

Таблица 8

Уровни риска информационной безопасности

Вероятность возникновения угрозы / **Ущерб для Субъекта платежной системы**	**Высокая**	**Средняя**	**Низкая**
Высокий	Высокий	Высокий	Средний
Средний	Высокий	Средний	Низкий
Низкий	Средний	Низкий	Низкий

2.5.2. Оценка уровня риска штрафных санкций регуляторов

2.5.2.1. Для оценки уровня риска штрафных санкций регуляторов используется Таблица 9:

Таблица 9

Уровни риска штрафных санкций регуляторов

Вероятность возникновения угрозы / **Штрафные санкции регуляторов**	**Высокая**	**Средняя**	**Низкая**
Максимальные	Очень высокий	Высокий	Средний
Минимальные	Средний	Средний	Низкий

2.5.2.2. По результатам определения уровней риска заполняются графы «Риск информационной безопасности» и «Риск штрафных санкций регуляторов» для каждого сценария «объект среды-угроза-уязвимость».

2.6. Разработка отчета об уровне риска информационной безопасности

2.6.1.После определения уровней риска информационной безопасности и риска штрафных санкций регуляторов структурное подразделение, ответственное за управление риском информационной безопасности, оформляет сводный отчет об уровне риска информационной безопасности.

2.6.2. В отчете (Таблица 10) обязательно дается ссылка на запись (акт) с утвержденными шкалами, которые использовались при проведении анализа риска информационной безопасности, приводится перечень информационных активов, объектов среды, для которых проводился анализ риска информационной безопасности, приводятся угрозы и уязвимости объектов среды, указывается текущий уровень риска информационной безопасности и риска штрафных санкций регуляторов, текущие контрмеры:

Таблица 10

Шаблон Отчета об уровне риска информационной безопасности

Информационный актив	**Объект среды**	**Важность объекта среды**	**Угроза**	**Уязвимость**	**Вероятность**	**Оценка воздействия**	**Уровень риска**		**Текущие контрмеры**
							Риск информационной безопасности	**Риск штрафных санкций регуляторов**	

2.6.3. Разработанный и согласованный работниками структурного подразделения, отвечающего за управление риском информационной безопасности, отчет передается на рассмотрение руководству Субъекта платежной системы, которое определяет приемлемый уровень риска информационной безопасности и риска штрафных санкций регуляторов.

2.6.4. Отчет подлежит хранению в течение 3 (Трех) лет.

2.7. Планирование мер по обработке риска информационной безопасности

2.7.1.После принятия решения об обработке риска информационной безопасности, превышающего приемлемый уровень, разрабатывается план обработки риска информационной безопасности (Таблица 11), в котором приводятся новые контрмеры для снижения уровня риска до приемлемого уровня (с указанием остаточного уровня риска).

2.7.2.Если для одного сценария «объект среды-угроза-уязвимость» определено более одного значения риска, то для обработки риска берется максимальное значение:

Таблица 11

Шаблон Плана обработки риска информационной безопасности

Информационный актив	Объект среды	Угроза	Уязвимость	Текущий уровень риска		Текущие контрмеры	Новые контрмеры	Срок	Ответственный	Остаточный уровень риска	
				Риск информационной безопасности	Риск штрафных санкций регуляторов					Риск информационной безопасности	Риск штрафных санкций регуляторов

2.7.3.План обработки риска информационной безопасности составляется на год и утверждается руководством Субъекта платежной системы.

Приложение № 1

к Методике анализа и оценки риска информационной безопасности
в Платежной системе «КП Ритейл»

Каталог возможных угроз и уязвимостей информационной безопасности

№	Угроза	Уязвимость
1.	Разглашение и несанкционированное копирование данных о держателях таможенных карт из-за отсутствия средств шифрования	Отсутствует один из следующих механизмов защиты: – стойкая однонаправленная хэш-функция; – усечение (truncation); – использование One-Time-Pad («одноразовые блокноты»), использование и хранение ссылок на данные вместо самих данных (index tokens); – стойкие криптографические алгоритмы совместно с процессами и процедурами
2.	Получение несанкционированного доступа к данным о держателях таможенных карт при помощи вредоносного ПО. Разглашение и несанкционированное копирование данных при помощи вредоносного ПО	Отсутствует ПО, которое обнаруживает и блокирует/удаляет вредоносный программный код
3.	Получение несанкционированного административного доступа к данным о держателях таможенных карт	Своевременно не устанавливаются программные коррекции безопасности
4.	НСД вследствие невыполнения парольной политики	Отсутствует регламент проверки подлинности пользователей перед сбросом их паролей
4.1.		Первоначальные пароли для каждого пользователя не уникальны и/или не изменяются сразу же после первого использования
4.2.		Использование групповых учетных записей и паролей
4.3.		Отсутствует механизм ведения истории паролей
4.4.		Блокирование пользователя после 6 (Шести) неудачных попыток ввода пароля не осуществляется
4.5.		Блокирование идентификатора пользователя продолжается менее 30 (Тридцати) минут либо не осуществляется
5.	Несвоевременное обнаружение попыток доступа к автоматизированным системам	Не активированы механизмы протоколирования действий, совершенных с административными полномочиями
5.1.		Не протоколируется доступ ко всем журналам регистрации событий информационной безопасности
5.2.		Не протоколируется использование механизмов идентификации и

		аутентификации
5.3.		Не протоколируется создание и удаление системных объектов
5.4.		Не протоколируются дата и время выполненной команды
5.5.		Не протоколируется индикатор успеха или отказа
5.6.		Идентификатор или название задействованных данных, системного компонента или ресурса не регистрируется в журналах регистрации событий информационной безопасности
5.7.		Не выполняется ежедневный просмотр журналов зарегистрированных событий информационной безопасности
6.	Уничтожение журналов регистрации событий	Отсутствует своевременное резервирование файлов с зарегистрированными событиями информационной безопасности на централизованный сервер или носители, где их сложнее изменить
7.	Несвоевременное обнаружение факта модификации журналов регистрации событий информационной безопасности	Не используется программное обеспечение контроля целостности файлов и обнаружения изменений
8.	Несвоевременное обнаружение факта удаления/модификации критичных файлов	Не используется программное обеспечение контроля целостности файлов и обнаружения изменений
9.	НСД с помощью выявленных злоумышленником уязвимостей в автоматизированных системах. Несвоевременное обнаружение новых уязвимостей	Не проводится ежеквартальный инструментальный анализ защищенности
9.1.		Внешний и внутренний тест на проникновение не проводится или проводится нерегулярно