МЕТОДИКА

реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе «КП Ритейл»

г. Москва, 2023 г.

ОГЛАВЛЕНИЕ

1. Общие положения

1.1 Настоящая Методика анализа и реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе «КП Ритейл» (далее по тексту – Методика, платежная система) устанавливает требования к организации процесса управления инцидентами защиты информации в платежной системе.

1.2 Настоящая Методика определяет требования к порядку:

- проведения мониторинга и анализа Событий защиты информации;
- обнаружения и реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в платежной системе.

1.3 Целями создания настоящей Методики являются:

- минимизация негативного влияния инцидентов на бизнес-процессы, реализуемые в платежной системе;
- обеспечение оперативной реакции на восстановление объектов информационной инфраструктуры, обеспечивающих ведение бизнес-процессов в платежной системе.

1.4 Положения настоящей Методики распространяются на все субъекты платежной системы.

1.5 Настоящая Методика подлежит пересмотру в связи со следующим:

- изменениями в законодательстве Российской Федерации в области защиты информации;
- изменениями в нормативных актах Банка России в области защиты информации при осуществлении переводов денежных средств;
- пересмотром области применения, целей и задач процесса системы защиты информации в платежной системе.

1.6 Ответственным субъектом платежной системы за актуализацию настоящей Методики является оператор платежной системы.

2. Термины и определения

Бизнес-процессы - взаимосвязанные, последовательные технологические процедуры, выполняемые субъектами платежной системы при оказании услуг платежной системы.

Объекты информационной инфраструктуры субъекта платежной системы, входящие в состав и обеспечивающие реализацию Бизнес-процессов, осуществляемых в рамках платежной системы (Объекты информационной инфраструктуры) - все, что имеет ценность для платежной системы и находится в распоряжении субъекта платежной системы, в том числе:

- аппаратные средства, программные средства, аппаратно-программные средства, прикладное программное обеспечение автоматизированных систем и приложений;
- телекоммуникационные средства, оборудование и пр.;
- информационные активы (платежная информация, информация об остатках денежных средств на банковских счетах участников платежной системы и их клиентов, информация о совершенных переводах денежных средств, информация о размере клиринговых позиций, информация, необходимая для удостоверения участниками платежной системы и их клиентами права распоряжения денежными средствами, в том числе данные держателей таможенных карт, ключевая информация СКЗИ, используемых при осуществлении переводов денежных средств, информация о конфигурации, определяющая параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, а также информации о конфигурации, определяющей параметры работы технических средств защиты информации, персональные данные, управляющая информация платежных, информационных и телекоммуникационных

систем (информация, используемая для технической настройки программно-аппаратных комплексов обработки, хранения и передачи информации);
- системы управления базами данных;
- сервисы;
- работники (персонал),

а также все прочие Объекты информационной инфраструктуры субъекта платежной системы, прямо или косвенно влияющие на доступность, целостность и конфиденциальность информационных активов, включая любые процессы или процедуры, посредством которых выполняется администрирование автоматизированных систем субъекта платежной системы или их сопровождение.

Субъект платежной системы – оператор платежной системы, осуществляющий согласно правилам платежной системы функции операционного центра и платежного клирингового центра, расчетный центр, участники платежной системы.

Инцидент - событие, которое привело к нарушению оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, в том числе вследствие нарушений требований к обеспечению защиты информации при осуществлении переводов денежных средств (инцидент защиты информации), в результате которых приостанавливалось оказание услуг платежной инфраструктуры и/или нарушался регламент выполнения процедур (время начала, время окончания, продолжительность и последовательность процедур, выполняемых операторами услуг платежной инфраструктуры при оказании операционных услуг, услуг платежного клиринга и расчетных услуг).

Инцидент защиты информации – примерный перечень типов инцидентов защиты информации приведен в Приложении № 1 к настоящей Методике.

Событие защиты информации - идентифицированное возникновение и (или) изменение состояния Объектов информационной инфраструктуры, действия работников Субъектов платежной системы и (или) иных лиц, указывающие на возможный (потенциальный) инцидент.

Реагирование на инцидент защиты информации – структурированная совокупность действий, направленная на установление деталей инцидента, минимизацию ущерба от инцидента и предотвращение повторения инцидента.

3. Жизненный цикл Инцидента защиты информации

3.1. Жизненный цикл Инцидента защиты информации состоит из следующих этапов:обнаружение и регистрация Инцидента защиты информации;
- информирование;
- реагирование, в том числе проведение анализа, решение и устранение последствий Инцидента защиты информации;
- закрытие Инцидента защиты информации.

4. Обнаружение и регистрация Инцидента защиты информации

4.1. Обнаружение Инцидента защиты информации должно осуществляться Субъектами платежной системы в режиме 24/7.

4.2. Источниками информации о Событиях защиты информации, потенциально связанных с Инцидентами защиты информации, в том числе несанкционированный доступ, являются:
- работники Субъекта платежной системы;
- внешние по отношению к Субъекту платежной системы лица – другие Субъекты платежной системы, клиенты участников платежной системы, и (или) контрагенты;
- Банк России, иные органы, осуществляющие контроль или надзор за деятельностью Субъекта платежной системы;

– журналы регистрации Событий защиты информации в рамках мониторинга и анализа Событий защиты информации;
– результаты проведения проверок действующего у Субъекта платежной системы порядка обеспечения информационной безопасности.

5. Информирование об Инциденте защиты информации

5.1. Для установления и применения единых правил получения от работников и внешних по отношению к Субъекту платежной системы лиц информации, связанной с Инцидентами защиты информации (в том числе потенциальными), Субъектом платежной системы должен быть определен номер электронной почты и телефон, иные каналы связи, по которым можно оставить соответствующую заявку. Координаты для обращений работников и внешних лиц могут быть размещены на сайте Субъекта Системы в сети интернет.

5.2. Порядок информационного взаимодействия между Субъектами платежной системы при выявлении Инцидента защиты информации установлен пунктом 11.6. Правил платежной системы.

6. Реагирование на инцидент защиты информации

6.1. Действия по Реагированию на инцидент защиты информации производятся Субъектами платежной системы в соответствии с внутренними регламентами по управлению инцидентами.

6.2. Субъектом платежной системы должны быть определены и назначены роли, связанные с Реагированием на инциденты защиты информации - роли группы Реагирования на инциденты защиты информации (ГРИ).

6.3. В составе ГРИ выделяются следующие основные роли и их обязанности:

Руководитель ГРИ - обеспечение оперативного руководства Реагированием на инциденты защиты информации, подготовка плана работ, контроль выполнения работ, контроль сроков решения Инцидентов защиты информации, не позднее максимально отведенного срока (установлены Приложением № 2 к настоящей Методике).

Оператор-диспетчер ГРИ - обеспечение сбора и регистрации информации об Инцидентах защиты информации, информирование Субъектов платежной системы об Инциденте защиты информации, фиксирование информации о ходе решения Инцидентов защиты информации, выявление подозрений на массовые сбои и верификация правомерности инициации обращений, взаимодействие с пользователями Объектов информационной инфраструктуры и работниками ИТ-подразделений при необходимости уточнения информации, формирование текста оповещения работников Субъекта платежной системы.

Аналитик ГРИ - знание специфики Бизнес-процесса, реализуемого в платежной системе со стороны Субъекта платежной системы на экспертном уровне, выполнение непосредственных действий по Реагированию на инцидент защиты информации, анализ Инцидента защиты информации, в том числе определение типа и критичности, определение источников и причин возникновения, оценка последствий инцидента на реализацию Бизнес-процесса в платежной системе, принятие мер по устранению последствий, решение проблемных ситуаций, возникающих в рамках решения Инцидентов защиты информации, планирование и принятие мер по предотвращению повторного возникновения Инцидента защиты информации.

Секретарь ГРИ - документирование результатов Реагирования на инциденты защиты информации, формирование аналитических отчетов, материалов.

6.4. Допускается назначение нескольких ролей ГРИ одному работнику, общее количество членов ГРИ не должны быть меньше 2 (Двух).

6.5. При возникновении Инцидентов защиты информации должно обеспечиваться оперативное оповещение членов ГРИ о выявленных Инцидентах защиты информации.

6.6. При возникновении Инцидентов защиты информации обеспечивается предоставление членам ГРИ прав логического и физического доступа и административных полномочий, необходимых для проведения Реагирования на инциденты защиты информации.

6.7. В случае необходимости к процессу Реагирования на инциденты защиты информации могут быть привлечены внешние эксперты. В случае привлечения внешних экспертов такое решение должно быть обосновано, согласовано руководителем Субъекта платежной системы, получено соглашение о конфиденциальности между Субъектом платежной системы и привлекаемыми внешними экспертами.

6.8. В процессе реагирования собирается информация об Инциденте защиты информации, проводится определение причин его возникновения, источник Инцидента защиты информации (нарушитель), цели и способы реализации Инцидента защиты информации. После подтверждения факта устранения Инцидента защиты информации, производится его закрытие.

6.9. Для каждого Инцидента защиты информации должна быть определена его критичность с учетом степени влияния на Бизнес-процесс, реализуемый Субъектом платежной системы. Категории критичности, ожидаемые сроки реакции/решения Инцидента защиты информации и сроки устранения последствий приведены в Приложении № 2 к настоящей Методике.

6.10. Перечень типов Инцидентов защиты информации приведен в Приложении № 1 к настоящей Методике. Первичная критичность Инцидента защиты информации определяется в ходе Реагирования на инцидент.

6.11. Каждая заявка об Инциденте защиты информации или подозрении на инцидент должна быть зарегистрирована Субъектом платежной системы в соответствии с внутренним порядком.

6.12. Для установления и применения единых правил регистрации и классификации инцидентов в части состава и содержания атрибутов, описывающих Инцидент защиты информации, и их возможных значений в Приложении № 3 к настоящей Методике содержится рекомендуемый шаблон карточки инцидента.

6.13. Восстановление Объектов информационной инфраструктуры после Инцидентов защиты информации, приведших к их неработоспособности, осуществляется в соответствии с Планом ОНиВД Субъекта платежной системы.

6.14. Все процессы Реагирования на инциденты защиты информации фиксируются в карточке инцидента.

7. Закрытие Инцидента защиты информации

7.1. Решение о закрытии Инцидента защиты информации принимается на основании результатов решения инцидентов и подтверждения пользователями Объектов информационной инфраструктуры.

7.2. По результатам реагирования проводится переоценка рисков, повлекших Инцидент защиты информации, готовность защитных мер для минимизации выявленных рисков, определяется необходимость корректирующих мероприятий по снижению вероятности повторного возникновения инцидента.

7.3. После закрытия Инцидента защиты информации составляется отчет по инциденту, содержащий в том числе следующую информацию:

- описание инцидента;
- фактическое время простоя (недоступности) или деградации (ухудшения качества) Объектов информационной инфраструктуры;
- влияние на Бизнес-процесс, ведение которого осуществляется в платежной системе;
- хронологическое описание этапов решения инцидента.

7.4. По завершению мероприятий, направленных на устранение последствий Инцидента защиты информации Субъект платежной системы проводит итоговый анализ причин возникновения инцидента. Целью такого анализа является выработка организационных и технических решений, направленных на предотвращение и минимизацию последствий возможных нарушений в будущем. В рамках такого анализа могут проводиться следующие мероприятия:

- переоценка рисков, повлекших возникновение Инцидента защиты информации;
- подготовка перечня защитных мер для минимизации выявленных рисков в случае повторения инцидента;
- актуализация внутренних документов Субъекта платежной системы, затрагивающих вопросы обеспечения защиты информации при осуществлении переводов денежных средств;
- проведение обучения персонала Субъекта платежной системы.

Приложение № 1

к Методике реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе «КП Ритейл»

Перечень типов Инцидентов защиты информации

№	Тип	Первичная критичность
1.	DDoS-атака	
2.	Вирусное заражение	
3.	Несанкционированное изменение Объектов информационной инфраструктуры Субъекта платежной системы	
4.	Подбор пароля	
5.	Несанкционированное создание учетной записи/получение доступа к Объекту информационной инфраструктуры	
6.	Подозрение на компрометацию учетных данных пользователя	
7.	Компрометация ключей шифрования	
8.	Компрометация ключей к электронной подписи	
9.	Обнаружение вредоносного кода	
10.	Утечка конфиденциальных данных	

Приложение № 2

к Методике реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе «КП Ритейл»

Метрики приоритетов Инцидентов защиты информации

Критичность инцидента	**Степень влияния на реализацию Субъектом платежной системы Бизнес-процесса, реализуемого в платежной системе**	**Ожидаемый срок реакции/решения инцидента, астр. час**	**Ожидаемый срок устранения последствий инцидента, астр. час**
Высокая	Инцидент может существенно негативно повлиять на ведение Бизнес-процессов в платежной системе, привести к значительным финансовым или репутационным рискам	Незамедлительно/6	24
Средняя	Инцидент может незначительно негативно повлиять на ведение Бизнес-процессов в платежной системе	1/24	72
Низкая	Инцидент не может привести к негативным последствиям для Бизнес-процессов в платежной системе	4/48	120

Приложение № 3

к Методике реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе «КП Ритейл»

Карточка Инцидента защиты информации

Характеристика	Значение
Идентификатор инцидента	
Тип инцидента	
Первичная критичность	
Дата и время обнаружения	
Источник информации	
Наименование технического средства, с использованием которого обнаружен инцидент	
Описание инцидента	
Затронутые Объекты информационной инфраструктуры Субъекта платежной системы	
Уровень инцидента	
Степень тяжести последствий инцидента	
Действия по реагированию на инцидент (каким образом проводилось сдерживание, удаление и восстановление)	
Дата и время закрытия инцидент	
Оценка необходимости реализации мер по совершенствованию процессов информационной безопасности	