УТВЕРЖДЕНО
Решением Правления
ООО «НКО «ЭЛЕКСИР»
Протокол № __б/н_____
от «_19_» __мая____ 2025 г.

Методика

реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств

в Платежной Системе OLMAPAY

г. Москва, 2025 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 OLMAPAY (далее по тексту - Методика) устанавливает требования к организации процесса управления инцидентами защиты информации в Платежной Системе OLMAPAY (далее по тексту – Платежная Система).

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 технологический процесс, реализуемый в Платежной Системе;
- обеспечение оперативной реакции на восстановление объектов информационной инфраструктуры, обеспечивающих ведение технологического процесса в Платежной Системе.

1.4. Настоящая Методика подлежит пересмотру не реже 1 (Одного) раза в 3 (Три) года 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.

1.5. Ответственным за актуализацию настоящей Методики является Оператор Платежной Системы.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная банковская система (АБС) – это аппаратно-программный комплекс для обработки, накопления, анализа и передачи информации о денежных платежах, расчётах и других финансово-кредитных операциях.

Автоматизированное рабочее место (АРМ) - функционально полный набор аппаратных и программных средств на базе терминалов, персональных компьютеров, сетевых устройств, позволяющих осуществлять ввод, вывод, хранение, накопление и обработку информации автономно или при подключении к локально вычислительной сети.

Администратор – работник, обеспечивающий работу ИТ инфраструктуры.

ИБ – информационная безопасность.

ИТ – информационные технологии.

Объекты информационной инфраструктуры Оператора Платежной Системы, входящие в состав и обеспечивающие реализацию технологических процессов, осуществляемых в рамках Платежной Системы (объекты информационной инфраструктуры) - все, что имеет ценность для Платежной Системы и находится в распоряжении Оператора Платежной Системы, в том числе:

- финансовые (денежные) средства;
- аппаратные средства, программные средства, аппаратно-программные средства, прикладное программное обеспечение автоматизированных систем и приложений;
- телекоммуникационные средства и пр.;
- информационные активы (в том числе, платежная информация, персональные данные, управляющая информация платежных, информационных и телекоммуникационных систем

(информация, используемая для технической настройки программно-аппаратных комплексов обработки, хранения и передачи информации));
- технологические процессы;
- сервисы;
- работники (персонал),

а также все прочие объекты информационной инфраструктуры Оператора Платежной Системы, влияющие на доступность, целостность и конфиденциальность информационных активов, включая любые процессы или процедуры, посредством которых выполняется администрирование автоматизированных систем Оператора Платежной Системы или их сопровождение.

Информационный технологический процесс – часть технологического процесса, реализующая операции по изменению и (или) определению состояния информационных активов, необходимых для функционирования Платежной Системы и не являющихся платежной информацией.

Платежный технологический процесс – часть технологического процесса, реализующая операции над информационными активами Платежной Системы, связанные с обработкой платежной информации и (или) контролем данных операций.

Технологический процесс – набор взаимосвязанных операций с информацией и (или) объектами информатизации, используемых при функционировании и (или) необходимых для осуществления переводов денежных средств в рамках Платежной Системы.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Платежной Системы, находящаяся в распоряжении Оператора Платежной Системы и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме, в том числе, платежная информация, персональные данные, управляющая информация платежных, информационных и телекоммуникационных систем, а также **информация, используемая для технической настройки программно-аппаратных комплексов обработки, хранения и передачи информации.**

Оператор Платежной системы (Оператор Системы, Оператор ПС, Оператор) – организация, определяющая Правила Платежной системы, а также выполняющая иные обязанности, предусмотренные Законодательством.

Оператором Платежной системы OLMAPAY является Общество с ограниченной ответственностью «Небанковская кредитная организация «ЭЛЕКСИР (электронные системы и решения)», (ООО «НКО «ЭЛЕКСИР») (ИНН: 7729496647, ОГРН: 1167700053278, Лицензия Банка России № 3533-К от 19.08.2021 г.).

Информационная инфраструктура Платежной Системы – совокупность активов, включая информационные активы, Оператора Платежной Системы, операторов УПИ, иных участников Платежной Системы, обеспечивающих технологический процесс по осуществлению переводов денежных средств в рамках Платежной Системы.

Услуги платежной инфраструктуры (УПИ) – операционные услуги, услуги платежного клиринга, расчетные услуги.

Операторы УПИ – операционный центр, платежный клиринговый центр, расчетный центры 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, в результате которых приостанавливалось оказание услуг платежной инфраструктуры и/или нарушился регламент выполнения процедур (время начала, время окончания, продолжительность и последовательность процедур) выполняемых Оператором

УПИ при оказании операционных услуг, услуг платежного клиринга и расчетных услуг, предусмотренных временным регламентом функционирования Платежной Системы, установленным Правилами.

Объект доступа - объект информатизации, представляющий собой аппаратное средство, средство вычислительной техники и (или) сетевое оборудование, в том числе входящие в состав объектов информационной инфраструктуры.

Работник ИБ – работник Оператора Платежной Системы, ответственный за обеспечение информационной безопасности.

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

Событие защиты информации - идентифицированное появление определенного состояния объектов информационной инфраструктуры, указывающего на возможное нарушение политик ИБ, или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Система управления базами данных (СУБД) - комплекс программных и языковых средств, который отвечает за хранение и управление информацией в базах данных.

Субъекты Платежной Системы – вместе или по отдельности Оператор Платежной Системы, Операторы УПИ, иные участники Платежной системы.

Технология управления информацией и событиями безопасности (Security Information and Event Management- или SIEM) - комплексное решение для обеспечения информационной безопасности, которое объединяет управление информацией о защите информации и управление событиями защиты информации.

3. ОРГАНИЗАЦИЯ МОНИТОРИНГА ДАННЫХ РЕГИСТРАЦИИ О СОБЫТИЯХ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Для того чтобы эффективно противостоять угрозам информационной безопасности, Оператору Платежной Системы, Операторам УПИ и иным участникам Платежной Системы рекомендуется:

- обеспечить защиту объектов информационной инфраструктуры в соответствие со стандартным уровнем защиты информации, определенным в ГОСТ 57580.1 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер";
- работникам ИБ оператора Платежной Системы, необходимо доводить до участников Платежной Системы информацию об актуальных угрозах, реализация которых возможна в Платежной Системе OLMAPAY;
- для отслеживания и ведения статистики Инцидентов необходимо выбрать средство накопления и хранения экспертной информации и отчётов о произошедших ранее Инцидентах.

3.2. Организация мониторинга данных регистрации о событиях защиты информации, обеспечивается за счет использования встроенных возможностей технических средств в составе системы защиты информации Оператора Платежной Системы, Операторов УПИ и иных участников Платежной Системы.

3.3. Регистрация событий защиты информации должна настраивается на следующих объектах информатизации:

- сетевом оборудовании, в том числе активном сетевом оборудовании, маршрутизаторах, коммутаторах;

- сетевых приложениях и сервисах;
- операционных системах, СУБД;
- информационных системах и приложениях;
- средствах и системах защиты информации;
- гипервизорах и системах управления средой виртуализации;
- других объектах и ресурсах доступа.

3.4. Сбор данных регистрации о событиях защиты информации, формируемых объектами информатизации, определенными в пункте 3.3. настоящей Методики, может проводиться, с помощью системы класса SIEM или в ручном режиме для дальнейшего анализа и корреляции событий.

3.5. При регистрации событий на объектах информатизации должна обеспечиваться генерация временных меток для зарегистрированных событий защиты информации.

3.6. Для объектов информатизации, используемых для формирования, сбора и анализа данных в процессе регистрации, должна обеспечивается синхронизация системного времени. Вносить изменения в настройки времени на системных компонентах разрешается только администраторам защищаемых ресурсов, которые имеют привилегированный доступ к настройкам системы. Вносить изменения в настройки времени на назначенных серверах времени могут только уполномоченные администраторы серверов из числа работников подразделения ИТ. Изменения в схеме получения времени объектами информационной инфраструктуры Оператора Платежной Системы, Операторов УПИ и иных участников Платежной Системы, входящих в периметр Платежной Системы, должны согласовываться с работником ИБ Оператора Платежной Системы.

3.7. Администраторы, ответственные за работу объекта информатизации, должны контролировать формирование данных о регистрации событий защиты информации объектов информатизации, определенных в пункте 3.3. настоящей Методики.

3.8. Не реже 1 (Одного) раза в день ответственными администраторами объектов информационной инфраструктуры Оператора Платежной Системы, Операторов УПИ и иных участников Платежной Системы, должен проводиться контроль факта регистрации событий и состав зарегистрированных событий. Администраторы объектов информационной инфраструктуры Оператора Платежной Системы, Операторов УПИ и иных участников Платежной Системы, должны проводить анализ с целью подтверждения их штатного функционирования, выявления аномалий в работе, подозрений на возникновение Инцидентов.

3.9. Администраторы объектов информационной инфраструктуры Оператора Платежной Системы, Операторов УПИ и иных участников Платежной Системы на периодической основе должны анализировать достаточность объема памяти для хранения данных о регистрации событий защиты информации на протяжении 5 лет. В случае недостаточности объема памяти для хранения регистрируемых событий администраторами Оператора Платежной Системы, Операторов УПИ и иных участников Платежной Системы принимаются меры по обеспечению возможности сохранности всех зарегистрированных событий.

3.10. Оперативный доступ к зарегистрированным данным о событиях защиты информации должен обеспечиваться минимум за последний 3 (Три) месяца.

4. ТРЕБОВАНИЯ К РЕГИСТРАЦИИ СОБЫТИЙ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Обеспечивается возможность выполнения операции нормализации (приведения к единому формату), фильтрации, агрегации и классификации данных регистрации о событиях защиты информации, например, с помощью используемой системы класса SIEM.

4.2. Обеспечивается возможность выявления и анализа событий защиты информации,

потенциально связанных с Инцидентами, включая:

- действия и (или) операции по созданию, удалению, копированию ресурсов доступа;
- действия и (или) операции по созданию, удалению, блокированию, разблокированию учетных записей;
- действия и (или) операции по изменению (предоставлению) прав логического доступа;
- действия и (или) операции по подключению СВТ к вычислительным сетям Оператора Платежной Системы;
- действия и (или) операции по запуску программных процессов;
- действия и (или) операции при осуществлении логического доступа;
- факты выявления уязвимостей защиты информации;
- факты выявления вредоносного кода и (или) неконтролируемого запуска мобильного кода;
- факты выявления попыток осуществления вторжений и сетевых атак;
- факты выявления атак типа «отказ в обслуживании»;
- действия и (или) операции, направленные на изменение правил сегментации и межсетевого экранирования вычислительных сетей Оператора Платежной Системы;
- действия и (или) операции по изменению параметров настроек технических мер защиты информации, параметров настроек системного ПО, влияющих на обеспечение защиты информации;
- факты выявления нарушений и сбоев в работе технических мер защиты информации;
- факты выявление нарушений и сбоев в установлении (обновлении) ПО и параметров настроек технических мер защиты информации, их сигнатурных баз (в случае их использования);
- факты выявления нарушений и сбоев в установлении (обновлении) системного ПО и параметров его настроек, влияющих на обеспечение защиты информации;
- факты выявления смены и (или) компрометации аутентификационных данных, используемых для доступа к серверному и сетевому оборудованию;
- действия и (или) операции со средствами криптографической защиты информации и ключевой информацией;
- действия и (или) операции при осуществлении доступа к серверным компонентам виртуализации виртуальными машинами, логическими разделами или томами;
- факты выявления нарушений при доверенной загрузке виртуальных машин.

4.3. С целью определения состава действий и (или) операций конкретного Субъекта Платежной Системы регистрация включает для каждого события следующие параметры:

- идентификатор пользователя;
- тип события;
- дата и время;
- результат события (успешно или неуспешно);
- источник события;
- идентификатор или название данных, объекта информационной инфраструктуры или ресурса определенного Субъекта Платежной Системы, входящих в периметр Платежной Системы, затронутых событием.

4.4. Обеспечивается возможность определения состава действий и (или) операций Субъектов Платежной Системы имеющих доступ при осуществлении логического доступа к конкретному ресурсу доступа.

4.5. Обеспечивается регистрация нарушений и сбоев в формировании и сборе данных о событиях защиты информации.

4.6. Обеспечивается регистрация доступа к хранимым данным о событиях защиты информации.

4.7. Обеспечивается регистрация операций, связанных с изменением правил нормализации (приведения к единому формату), фильтрации, агрегации и классификации данных

регистрации о событиях защиты информации.

5. ЖИЗНЕННЫЙ ЦИКЛ ИНЦИДЕНТА

Жизненный цикл Инцидента состоит из следующих этапов:

- обнаружение и регистрация Инцидента;
- информирование;
- реагирование, в том числе проведение анализа, решение и устранение последствий Инцидента;
- закрытие Инцидента.

5.1. Обнаружение и регистрация Инцидента.

5.1.1. Обнаружение Инцидентов должно осуществляться Субъектами Платежной Системы в режиме 24/7.

5.1.2. Источниками информации о событиях защиты информации, потенциально связанных с Инцидентами, в том числе несанкционированным доступом (НСД), являются:

- работники Оператора Платежной Системы, или Операторов УПИ, или иных участников Платежной Системы;
- внешние по отношению к Субъектам Платежной Системы лица – клиенты и (или) контрагенты;
- Банк России, иные органы исполнительной власти, осуществляющие контроль или надзор за деятельностью Субъектов Платежной Системы;
- журналы регистрации событий защиты информации в рамках мониторинга и анализа событий защиты информации;
- результаты проведения проверок, действующего у Субъектов Платежной Системы порядка обеспечения информационной безопасности.

5.2. Информирование об Инциденте

5.2.1. Для установления и применения единых правил получения от работников, клиентов и (или) контрагентов Субъектов Платежной Системы информации, связанной с Инцидентами (в том числе потенциальными), каждым Субъектом Платежной Системы должен быть определен адрес электронной почты и номер телефона, иные каналы связи, по которым можно оставить соответствующую заявку. Координаты для обращений работников и внешних лиц могут быть размещены на корпоративных сайтах Оператора Платежной Системы, Операторов УПИ, и иных участников Платежной Системы.

5.2.2. Порядок информационного взаимодействия между Субъектами Платежной Системы при выявлении Инцидентов установлен в Правилах Платежной Системы.

5.3. Реагирование на Инцидент

5.3.1. Действия по реагированию на Инцидент производятся Субъектами Платежной Системы в соответствии с внутренними регламентами по управлению Инцидентами.

5.3.2. Оператором Платежной Системы и иными Субъектами Платежной Системы должны быть определены и назначены роли, связанные с реагированием на Инциденты - роли группы реагирования на Инциденты защиты информации (ГРИЗИ). Роли предполагают разделение обязанностей работников Субъектов Платёжной системы при реагировании на Инциденты.

5.3.3. В составе ГРИЗИ могут выделяться следующие основные роли:

Роль	Функции
Руководитель ГРИЗИ	- обеспечение оперативного руководства реагированием на Инциденты; - подготовка плана работ; - контроль выполнения работ, в том числе контроль сроков решения Инцидентов, не позднее максимально отведенного срока (установлены Приложением № 1 к настоящей - Методике);
Оператор-диспетчер ГРИЗИ	- обеспечение сбора и регистрации информации об Инцидентах; - информирование Субъектов Платежной Системы об Инциденте; - фиксирование информации о ходе решения Инцидентов; - 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 Субъектов Платежной Системы;
Аналитик ГРИЗИ	- знание специфики технологического процесса, реализуемого в Платежной Системе со стороны Субъекта Платежной Системы на экспертном уровне; - выполнение непосредственных действий по реагированию на Инцидент: • анализ Инцидента, в том числе определение типа и критичности Инцидента; • определение источников и причин возникновения Инцидента; • оценка последствий Инцидента на реализацию технологических процессов Платежной Системы; • принятие мер по устранению последствий Инцидента; • решение проблемных ситуаций, возникающих в рамках решения Инцидентов; • планирование и принятие мер по предотвращению повторного возникновения Инцидента;
Секретарь ГРИЗИ	- Документирование результатов реагирования на Инциденты; - Формирование аналитических отчетов и материалов.

5.3.4. Допускается назначение нескольких ролей ГРИЗИ одному работнику, общее количество членов ГРИЗИ не должны быть меньше двух.

5.3.5. При возникновении Инцидентов должно обеспечиваться своевременное (оперативное) оповещение членов ГРИЗИ о выявленных Инцидентах.

5.3.6. При возникновении Инцидентов обеспечивается предоставление членам ГРИЗИ прав логического и физического доступа и административных полномочий, необходимых для реагирования.

5.3.7. В случае необходимости к процессу реагирования на Инциденты могут быть привлечены внешние эксперты. В случае привлечения внешних экспертов такое решение должно быть обосновано, согласовано руководителем Субъекта Платежной Системы, подписано соглашение о конфиденциальности между Субъектом Платежной Системы и привлекаемыми внешними экспертами.

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

5.3.9. Для каждого Инцидента должна быть определена его критичность с учетом степени влияния на реализацию каждым Субъектом технологических процессов Платежной Системы. Категории критичности, ожидаемые сроки реакции/решения Инцидента и сроки устранения последствий приведены в Приложении № 1 к настоящей Методике.

5.3.10. Перечень типов Инцидентов и первичная критичность приведены в Приложении № 2 к настоящей Методике. Первичная критичность Инцидента может быть пересмотрена в ходе реагирования на Инцидент.

5.3.11. Каждая заявка об Инциденте или подозрении на Инцидент должна быть зарегистрирована Субъектом Платежной Системы в соответствии с внутренним порядком.

5.3.12. Для установления и применения единых правил регистрации и классификации Инцидентов в части состава и содержания атрибутов, описывающих Инцидент, и их возможных значений в Приложении № 3 к настоящей Методике содержится рекомендуемый шаблон карточки Инцидента.

5.3.13. Восстановление объектов информационной инфраструктуры после Инцидентов, приведших к их неработоспособности, осуществляется в соответствии с планом ОНиВД Субъекта Платежной Системы.

5.3.14. Все процессы реагирования на Инциденты фиксируются в карточке Инцидента.

5.4. Закрытие Инцидента.

5.4.1. Решение о закрытии Инцидента принимается на основании результатов решения Инцидентов и подтверждения пользователями объектов информационной инфраструктуры.

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

5.4.3. После закрытия Инцидента 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 технологический процесс, ведение которого осуществляется в Платежной Системе;
- хронологическое описание этапов решения Инцидента.

6. ЗАЩИТА ИНФОРМАЦИИ ОБ ИНЦИДЕНТАХ

6.1. В целях защиты информации об Инцидентах Субъектами Платежной Системы должны проводиться следующие мероприятия:

- обеспечивается реализация защиты информации об Инцидентах от НСД, обеспечение целостности и доступности указанной информации;
- обеспечивается разграничение доступа членов ГРИЗИ к информации об Инцидентах в соответствии с определенным распределением ролей, связанных с реагированием на Инциденты;
- сохранность зарегистрированных данных об Инцидентах обеспечивается в течение 5 (пяти) лет;
- обеспечивается регистрация доступа к информации об Инцидентах.

7. ОТВЕТСТВЕННОСТЬ

7.1. Оператор Платежной Системы несет ответственность за:

- организацию работы по мониторингу данных регистрации событий защиты информации и управлению Инцидентами;
- организацию взаимодействия с Субъектами Платежной Системы по информированию об Инцидентах;
- методическое руководство порядка мониторинга событий защиты информации и управления Инцидентами;
- предоставление результатов и отчетных материалов руководству.

7.2. Субъект Платежной Системы несет ответственность за:

- контроль выполнения требований мониторинга событий защиты информации и управления Инцидентами;
- определение состава объектов информационной инфраструктуры Субъекта Платежной Системы, на которых производится настройка регистрации событий защиты информации;
- определение состава регистрируемых событий защиты информации;
- осуществление обнаружения, регистрации, управления Инцидентами;
- предоставление результатов и отчетных материалов по управлению Инцидентами Оператору Платежной Системы.

7.3. Подразделение ИТ каждого Субъекта Платежной Системы несет ответственность за:

- настройку и контроль регистрации событий защиты информации;
- настройку и контроль синхронизации времени объектов информационной инфраструктуры Субъекта Платежной Системы;
- контроль на постоянной основе регистрации событий безопасности информации;
- участие в реагировании на Инциденты;
- своевременное предоставление работнику ИБ Субъекта Платежной Системы информации, необходимой для контроля и совершенствования процесса мониторинга событий защиты информации и управления Инцидентами.

Приложение № 1

к Методике анализа и реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе OLMAPAY

Метрики приоритетов инцидентов

Критичность Инцидента	**Степень влияния на реализацию Оператором Платежной Системы технологического процесса, проводимого в Платежной Системе**	**Ожидаемый срок реакции/решения Инцидента, час**	**Ожидаемый срок устранения последствий Инцидента, час**
Высокая	Инцидент может существенно негативно повлиять на ведение технологического процесса платежной системы, привести к значительным финансовым или репутационным рискам	Незамедлительно/6	24
Средняя	Инцидент может незначительно негативно повлиять на ведение технологического процесса Платежной Системы	1/24	72
Низкая	Инцидент не может привести к негативным последствиям для технологического процесса Платежной системы	4/48	120

Приложение № 2

к Методике анализа и реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе OLMAPAY

Перечень типов инцидентов

№	Название	Первичная критичность
1	2	3
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 № 3

к Методике анализа и реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе OLMAPAY

Карточка инцидента

Характеристика	Значение
1	2
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 инцидента	
Оценка необходимости реализации мер по совершенствованию процессов информационной безопасности	

Всего прошито, пронумеровано и скреплено печатью

14 листа (ов)

Должность Председатель Правления

Подпись _____ /С.П. Синицын /

_____ 20 25 г. М.П.