О внесении изменений и дополнений в постановления Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 202 "Об утверждении Правил выпуска , использования и погашения электронных денег, а также требований к эмитентам электронных денег и системам электронных денег на территории Республики Казахстан" и от 31 августа 2016 года № 215 "Об утверждении Правил организации деятельности платежных организаций"

Постановление Правления Национального Банка Республики Казахстан от 20 декабря 2021 года № 116. Зарегистрировано в Министерстве юстиции Республики Казахстан 10 января 2022 года № 26413

Примечание ИЗПИ!

Порядок введения в действие см. п. 5.

В соответствии с подпунктами 42) и 52-1) части второй статьи 15 Закона Республики Казахстан "О Национальном Банке Республики Казахстан" и подпунктами 1) и 12) пункта 1 статьи 4 Закона Республики Казахстан "О платежах и платежных системах" Правление Национального Банка Республики Казахстан ПОСТАНОВЛЯЕТ:

1. Внести в постановление Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 202 "Об утверждении Правил выпуска, использования и погашения электронных денег, а также требований к эмитентам электронных денег и системам электронных денег на территории Республики Казахстан" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 14298) следующие изменения и дополнения:

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 42) части второй статьи 15 Закона Республики Казахстан "О Национальном Банке Республики Казахстан" и подпунктом 12) пункта 1 статьи 4 Закона Республики Казахстан "О платежах и платежных системах" Правление Национального Банка Республики Казахстан **ПОСТАНОВЛЯЕТ**:";

в Правилах выпуска, использования и погашения электронных денег, а также требованиях к эмитентам электронных денег и системам электронных денег на территории Республики Казахстан, утвержденных указанным постановлением:

часть первую пункта 1 изложить в следующей редакции:

"1. Настоящие Правила выпуска, использования и погашения электронных денег, а также требования к эмитентам электронных денег и системам электронных денег на территории Республики Казахстан (далее – Правила) разработаны в соответствии с подпунктом 42) части второй статьи 15 Закона Республики Казахстан "О Национальном Банке Республики Казахстан" и подпунктом 12) пункта 1 статьи 4

Закона Республики Казахстан "О платежах и платежных системах" (далее – Закон о платежах и платежных системах) и определяют порядок выпуска, использования и погашения электронных денег на территории Республики Казахстан, а также требования к эмитентам электронных денег (далее – эмитент) и системам электронных денег на территории Республики Казахстан.";

пункт 2 изложить в следующей редакции:

"2. В Правилах используются понятия, предусмотренные статьей 1 Закона о платежах и платежных системах, а также следующие понятия:

1) инцидент информационной безопасности, включая нарушения, сбои в информационных системах (далее – инцидент информационной безопасности) – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов оператора системы электронных денег;

2) информация об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах – информация об отдельно или серийно возникающих сбоях в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающих угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов оператора системы электронных денег;

3) периметр защиты информационно-коммуникационной инфраструктуры – совокупность программно-аппаратных средств, отделяющих информационно-коммуникационную инфраструктуру оператора системы электронных денег от внешних информационных сетей и обеспечивающих защиту от угроз информационной безопасности;

4) информационная безопасность – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

5) угроза информационной безопасности – совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

6) обеспечение информационной безопасности – процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов оператора системы электронных денег;

7) процедура безопасности – комплекс организационных мер и программно-технических средств защиты информации, предназначенных для удостоверения прав владельца электронных денег на использование электронных денег и обнаружения ошибок и (или) изменений в содержании передаваемых и получаемых

электронным способом сообщений (далее - электронное сообщение) при использовании электронных денег;

8) информационный актив оператора системы электронных денег – совокупность информации и объекта информационно-коммуникационной инфраструктуры, используемого для ее хранения и (или) обработки;

9) информационно-коммуникационная инфраструктура оператора системы электронных денег (далее – информационная инфраструктура) – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

10) внутренние правила системы электронных денег – правила, в соответствии с которыми производятся выпуск, реализация, приобретение, погашение электронных денег, а также осуществляются операции с их использованием в системе электронных денег;

11) личный кабинет владельца электронных денег – персональный раздел владельца электронных денег на интернет-ресурсе системы электронных денег, посредством которого владелец электронных денег имеет доступ к своему электронному кошельку для получения необходимой информации об остатке электронных денег, операциях, проведенных по нему, осуществления платежей и иных операций с использованием электронных денег в порядке, предусмотренном внутренними правилами системы электронных денег и договорами, заключенными между оператором системы электронных денег (далее – оператор) или эмитентом и владельцем электронных денег. Перечень предоставляемых услуг посредством личного кабинета владельца электронных денег устанавливается оператором;

12) обменные операции с электронными деньгами – операции по обмену электронных денег, выпущенных одним эмитентом, на электронные деньги другого эмитента, являющегося участником другой системы электронных денег;

13) принудительное погашение электронных денег – операция по погашению электронных денег, предусматривающая перечисление равной номинальной их стоимости на банковский счет владельца электронных денег либо на консолидированный счет эмитента до их востребования физическим лицом;

14) прекращение выпуска электронных денег – прекращение деятельности эмитента по оказанию платежной услуги, предусматривающей выдачу электронных денег физическому лицу или агенту системы электронных денег (далее – агент) путем обмена на равную по их номинальной стоимости сумму денег;

15) блокирование электронного кошелька – полный или частичный запрет на использование электронных денег, хранящихся в электронном кошельке владельца электронных денег.";

абзац первый пункта 4 изложить в следующей редакции:

"4. Эмитент в течение десяти календарных дней с даты начала осуществления деятельности по выпуску электронных денег уведомляет об этом Национальный Банк Республики Казахстан по форме согласно приложению 1 к Правилам и представляет следующие документы и сведения:";

пункт 38 изложить в следующей редакции:

"38. Эмитент за тридцать календарных дней до момента прекращения выпуска электронных денег уведомляет об этом Национальный Банк Республики Казахстан по форме согласно приложению 1 к Правилам.";

пункт 50 изложить в следующей редакции:

"50. Удаленная идентификация владельца электронных денег - физического лица осуществляется эмитентом и (или) оператором на основании сведений из доступных источников, полученных от операционного центра межбанковской системы переводов денег, в порядке и по основаниям, предусмотренным Правилами оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденными постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 212 (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 14337).";

дополнить главой 7 следующего содержания:

"Глава 7. Требования к программно-техническим средствам и системам управления информационной безопасностью операторов систем электронных денег, являющихся платежными организациями

55. Программное обеспечение обеспечивает:

1) надежное хранение информации, защиту от несанкционированного доступа, целостность баз данных и полную сохранность информации в электронных архивах и базах данных при полном или частичном отключении электропитания в любое время на любом участке оборудования;

2) многоуровневый доступ к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении, предусматривающим как минимум, два уровня доступа: администратор и пользователь;

3) контроль полноты вводимых данных полей обязательных к заполнению, необходимых для проведения и регистрации операций (при выполнении функций или операций без полного заполнения всех полей программа обеспечивает выдачу соответствующего уведомления);

4) поиск информации по критериям и параметрам, определенным для данной информационной системы, с сохранением запроса, а также сортировку информации по любым параметрам (определенным для данной информационной системы) и возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в информационной системе;

5) обработку информации и ее хранение по дате и времени;

6) автоматизированное формирование форм отчетов, представляемых операторами систем электронных денег в Национальный Банк Республики Казахстан, а также отчетов о проведенных операциях;

7) ведение и автоматизированное формирование журналов системы внутреннего учета. Программное обеспечение формирует журнал полностью, а также частично (на указанный диапазон дат, определенную дату);

8) возможность резервирования и восстановления данных, хранящихся в учетных системах;

9) возможность вывода выходных документов на экран, принтер или в файл;

10) возможность обмена электронными документами;

11) регистрацию и идентификацию происходящих в информационной системе событий с сохранением следующих атрибутов: дата и время начала события, наименование события, пользователь, производивший действие, идентификатор записи , дата и время окончания события, результат выполнения события.

56. Операторы систем электронных денег обеспечивают создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления операторов систем электронных денег, предназначенной для управления процессом обеспечения информационной безопасности.

57. Система управления информационной безопасностью обеспечивает защиту информационных активов операторов систем электронных денег, допускающую минимальный уровень потенциального ущерба для бизнес-процессов операторов систем электронных денег.

58. Оператор системы электронных денег обеспечивает надлежащий уровень системы управления информационной безопасностью, ее развитие и улучшение.

59. Оператор системы электронных денег в целях обеспечения конфиденциальности , целостности и доступности информации осуществляет следующие функции:

1) организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

2) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности;

3) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности в рамках своих полномочий;

4) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;

5) осуществляет анализ информации об инцидентах информационной безопасности;

6) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности, а также предоставление доступа к ним;

7) определяет ограничения по использованию привилегированных учетных записей;

8) организует и проводит мероприятия по обеспечению осведомленности работников оператора систем электронных денег в вопросах информационной безопасности;

9) осуществляет мониторинг состояния системы управления информационной безопасностью оператора систем электронных денег;

10) периодически (но не реже одного раза в год) осуществляет информирование руководства оператора системы электронных денег о состоянии системы управления информационной безопасностью.

60. Оператор системы электронных денег управляет рисками информационной безопасности с указанием критериев приемлемого уровня по отношению к информационным активам.

При реализации рисков информационной безопасности разрабатывается план мероприятий, направленный на минимизацию возникновения подобных рисков.

61. Информация об инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности, подлежит консолидации, систематизации и хранению.

62. Срок хранения информации об инцидентах информационной безопасности составляет не менее 5 (пяти) лет.

63. Оператором системы электронных денег определяется порядок принятия неотложных мер к устранению инцидента информационной безопасности, его причин и последствий.

64. Оператор систем электронных денег ведет журнал учета инцидентов информационной безопасности с отражением всей информации об инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах.

65. Оператор системы электронных денег предоставляет в Национальный Банк информацию о следующих выявленных инцидентах информационной безопасности:

1) эксплуатация уязвимостей в прикладном и системном программном обеспечении ;

2) несанкционированный доступ в информационную систему;

3) атака "отказ в обслуживании" на информационную систему или сеть передачи данных;

4) заражение сервера вредоносной программой или кодом;

5) совершение несанкционированного перевода электронных денег вследствие нарушения контролей информационной безопасности;

6) инцидентах информационной безопасности, несущих угрозу стабильности деятельности оператора системы электронных денег.

Информация об инцидентах информационной безопасности, указанных в настоящем пункте, предоставляется оператором системы электронных денег в возможно короткий срок, но не позднее 48 часов с момента выявления, в виде карты инцидента информационной безопасности по форме согласно приложению 2 к Правилам.

Информация по обработанным инцидентам информационной безопасности представляется в электронном формате с использованием платформы Национального Банка для обмена событиями и инцидентами информационной безопасности.

На каждый инцидент информационной безопасности заполняется отдельная карта инцидента информационной безопасности.";

в приложении текст в правом верхнем углу изложить в следующей редакции:

"Приложение 1
к Правилам выпуска,
использования и погашения
электронных денег,
а также требованиям
к эмитентам электронных денег
и системам электронных денег
на территории Республики Казахстан";

дополнить приложением 2 в редакции согласно приложению 1 к настоящему постановлению.

2. Внести в постановление Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 215 "Об утверждении Правил организации деятельности платежных организаций" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 14347) следующие изменения и дополнения:

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 52-1) части второй статьи 15 Закона Республики Казахстан "О Национальном Банке Республики Казахстан", законами Республики Казахстан "О государственных услугах", "О разрешениях и уведомлениях", и подпунктом 1) пункта 1 статьи 4 Закона Республики Казахстан "О платежах и платежных системах" Правление Национального Банка Республики Казахстан ПОСТАНОВЛЯЕТ:";

в Правилах организации деятельности платежных организаций, утвержденных указанным постановлением:

пункты 1 и 2 изложить в следующей редакции:

"1. Настоящие Правила организации деятельности платежных организаций (далее – Правила) разработаны в соответствии с подпунктом 52-1) части второй статьи 15

Закона Республики Казахстан "О Национальном Банке Республики Казахстан", законами Республики Казахстан "О государственных услугах", "О разрешениях и уведомлениях", подпунктом 1) пункта 1 статьи 4 Закона Республики Казахстан "О платежах и платежных системах" (далее – Закон о платежах и платежных системах) и определяют порядок организации деятельности платежных организаций.

Порядок организации деятельности платежных организаций включает учетную регистрацию платежных организаций в Национальном Банке Республики Казахстан (далее – Национальный Банк), ведение Национальным Банком реестра платежных организаций (далее – реестр), оказание платежных услуг платежными организациями, уведомление платежными организациями об открытии филиалов, требования к программно-техническим средствам платежных организаций и системе управления информационной безопасности.

2. В Правилах используются понятия, предусмотренные Законом о платежах и платежных системах, и следующие понятия:

1) информация об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах – информация об отдельно или серийно возникающих сбоях в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающих угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов платежной организации;

2) инцидент информационной безопасности, включая нарушения, сбои в информационных системах (далее – инцидент информационной безопасности) – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов платежной организации;

3) информационная безопасность – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

4) угроза информационной безопасности – совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

5) обеспечение информационной безопасности – процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов платежной организации;

6) периметр защиты информационно-коммуникационной инфраструктуры – совокупность программно-аппаратных средств, отделяющих информационно-коммуникационную инфраструктуру платежной организации от

внешних информационных сетей и обеспечивающих защиту от угроз информационной безопасности;

7) информационно-коммуникационная инфраструктура платежной организации (далее – информационная инфраструктура) – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним.";

8) информационный актив платежной организации – совокупность информации и объекта информационно-коммуникационной инфраструктуры, используемого для ее хранения и (или) обработки.";

пункт 7 изложить в следующей редакции:

"7. Правила осуществления деятельности платежной организации содержат следующие обязательные условия:

1) описание платежных услуг, оказываемых платежной организацией;

2) порядок и сроки оказания платежных услуг клиентам платежной организации;

3) стоимость платежных услуг (тарифы), оказываемых платежной организацией;

4) порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых платежной организацией;

5) сведения о системе управления рисками, используемой платежной организацией;

6) порядок урегулирования спорных ситуаций и разрешения споров с клиентами;

7) порядок соблюдения мер информационной безопасности;

8) описание программно-технических средств и оборудования, необходимого для осуществления платежных услуг.";

дополнить главой 6 следующего содержания:

"Глава 6. Требования к программно-техническим средствам платежных организаций и системе управления информационной безопасностью

34. Программное обеспечение обеспечивает:

1) надежное хранение информации, защиту от несанкционированного доступа, целостность баз данных и полную сохранность информации в электронных архивах и базах данных при полном или частичном отключении электропитания в любое время на любом участке оборудования;

2) многоуровневый доступ к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении, предусматривающим как минимум, два уровня доступа: администратор и пользователь;

3) контроль полноты вводимых данных полей обязательных к заполнению, необходимых для проведения и регистрации операций (при выполнении функций или операций без полного заполнения всех полей программа обеспечивает выдачу соответствующего уведомления);

4) поиск информации по критериям и параметрам, определенным для данной информационной системы, с сохранением запроса, а также сортировку информации по любым параметрам (определенным для данной информационной системы) и возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в информационной системе;

5) обработку информации и ее хранение по дате и времени;

6) автоматизированное формирование форм отчетов, представляемых платежными организациями в Национальный Банк, а также отчетов о проведенных операциях;

7) ведение и автоматизированное формирование журналов системы внутреннего учета. Программное обеспечение формирует журнал полностью, а также частично (на указанный диапазон дат, определенную дату);

8) возможность резервирования и восстановления данных, хранящихся в учетных системах;

9) возможность вывода выходных документов на экран, принтер или в файл;

10) возможность обмена электронными документами;

11) регистрацию и идентификацию происходящих в информационной системе событий с сохранением следующих атрибутов: дата и время начала события, наименование события, пользователь, производивший действие, идентификатор записи , дата и время окончания события, результат выполнения события.

35. Платежные организации обеспечивают создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления платежной организации, предназначенной для управления процессом обеспечения информационной безопасности.

36. Система управления информационной безопасностью обеспечивает защиту информационных активов платежной организации, допускающую минимальный уровень потенциального ущерба для бизнес-процессов платежной организации.

37. Платежная организация обеспечивает надлежащий уровень системы управления информационной безопасностью, ее развитие и улучшение.

38. Платежная организация в целях обеспечения конфиденциальности, целостности и доступности информации платежной организации осуществляет следующие функции :

1) организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

2) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности;

3) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности в рамках своих полномочий;

4) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;

5) осуществляет анализ информации об инцидентах информационной безопасности;

6) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности, а также предоставление доступа к ним;

7) определяет ограничения по использованию привилегированных учетных записей;

8) организует и проводит мероприятия по обеспечению осведомленности работников платежной организации в вопросах информационной безопасности;

9) осуществляет мониторинг состояния системы управления информационной безопасностью платежной организации;

10) периодически (но не реже одного раза в год) осуществляет информирование руководства платежной организации о состоянии системы управления информационной безопасностью платежной организации.

39. Платежная организация управляет рисками информационной безопасности с указанием критериев приемлемого уровня по отношению к информационным активам.

При реализации рисков информационной безопасности разрабатывается план мероприятий, направленный на минимизацию возникновения подобных рисков.

40. Информация об инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности, подлежит консолидации, систематизации и хранению.

41. Срок хранения информации об инцидентах информационной безопасности составляет не менее 5 (пяти) лет.

42. Платежной организацией определяется порядок принятия неотложных мер к устранению инцидента информационной безопасности, его причин и последствий.

43. В платежной организации ведется журнал учета инцидентов информационной безопасности с отражением всей информации об инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах.

44. Платежная организация предоставляет в Национальный Банк информацию о следующих выявленных инцидентах информационной безопасности:

1) эксплуатация уязвимостей в прикладном и системном программном обеспечении ;

2) несанкционированный доступ в информационную систему;

3) атака "отказ в обслуживании" на информационную систему или сеть передачи данных;

4) заражение сервера вредоносной программой или кодом;

5) совершение несанкционированного перевода денежных средств вследствие нарушения контролей информационной безопасности;

6) инцидентах информационной безопасности, несущих угрозу стабильности деятельности платежной организации.

Информация об инцидентах информационной безопасности, указанных в настоящем пункте, предоставляется платежной организацией в возможно короткий срок, но не позднее 48 часов с момента выявления, в виде карты инцидента информационной безопасности по форме согласно приложению 7 к Правилам.

Информация по обработанным инцидентам информационной безопасности представляется в электронном формате с использованием платформы Национального Банка для обмена событиями и инцидентами информационной безопасности.

На каждый инцидент информационной безопасности заполняется отдельная карта инцидента информационной безопасности.";

дополнить приложением 7 в редакции согласно приложению 2 к настоящему постановлению.

3. Департаменту платежных систем (Ашыкбеков Е.Т.) в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом (Касенов А.С.) государственную регистрацию настоящего постановления в Министерстве юстиции Республики Казахстан;

2) размещение настоящего постановления на официальном интернет-ресурсе Национального Банка Республики Казахстан после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего постановления представление в Юридический департамент сведений об исполнении мероприятия, предусмотренного подпунктом 2) настоящего пункта.

4. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Национального Банка Республики Казахстан Шолпанкулова Б.Ш.

5. Настоящее постановление вводится в действие с 1 апреля 2022 года.

Председатель
Национального Банка *Е. Досаев*
Республики Казахстан

СОГЛАСОВАНО
Министерство национальной экономики
Республики Казахстан

СОГЛАСОВАНО
Министерство цифрового развития,
инноваций и аэрокосмической промышленности
Республики Казахстан

Приложение 1
к постановлению Правления

Национального Банка
Республики Казахстан
от 20 декабря 2021 года № 116
Приложение 2
к Правилам выпуска,
использования и погашения
электронных денег,
а также требованиям к эмитентам
электронных денег и системам
электронных денег
на территории
Республики Казахстан
Форма

Карта инцидента информационной безопасности

№	Общие сведения	
	Характеристики инцидента информационной безопасности	Информация об инциденте информационной безопасности
1	Наименование инцидента информационной безопасности	
2	Дата и время выявления (дд.мм.гггг и чч:мм с указанием часового пояса UTC+X)	
3	Место выявления (организация, филиал, сегмент информационной инфраструктуры)	
4	Источник информации об инциденте информационной безопасности (пользователь, администратор, администратор информационной безопасности, работник подразделения информационной безопасности или техническое средство)	
5	Использованные методы при реализации инцидента информационной безопасности (социальная инженерия, внедрение вредоносного кода)	
Содержание инцидента информационной безопасности		
6	Симптомы, признаки инцидента информационной безопасности	
	Основные события (эксплуатация уязвимостей в прикладном и системном программном обеспечении; несанкционированный доступ в информационную систему;	

7	атака "отказ в обслуживании" на информационную систему или сеть передачи данных; заражение сервера вредоносной программой или кодом; совершение несанкционированного перевода денежных средств; инциденты информационной безопасности, несущие угрозу стабильности деятельности оператора системы электронных денег)	
8	Пораженные активы (физический уровень информационной инфраструктуры, уровень сетевого оборудования, уровень сетевых приложений и сервисов, уровень операционных систем, уровень технологических процессов и приложений и уровень бизнес-процессов оператора системы электронных денег)	
9	Статус инцидента информационной безопасности (свершившийся инцидент информационной безопасности, попытка осуществления инцидента информационной безопасности, подозрение на инцидент информационной безопасности)	
10	Ущерб	
11	Источник угрозы (выявленные идентификаторы)	
12	Преднамеренность (намеренный, ошибочный)	
Предпринятые меры по инциденту информационной безопасности		
13	Предпринятые действия (идентификация уязвимости, блокирование, восстановление)	
14	Запланированные действия, направленные на минимизацию возникновения рисков информационной безопасности	
15	Оповещенные лица (фамилия, имя , отчество (при его наличии)	

	должностных лиц, наименование государственных органов, организаций)	
16	Привлеченные специалисты (фамилия, имя, отчество (при его наличии) место работы, должность, номер телефона)	

Ответственный работник по информационной безопасности

_____ _____

(фамилия, имя, отчество (при его наличии) (подпись)

Дата "____" _____ 20 ___ года

Приложение 2
к постановлению
Приложение 7
к Правилам организации деятельности
платежных организаций
Форма

Карта инцидента информационной безопасности

№	Общие сведения	
	Характеристики инцидента информационной безопасности	Информация об инциденте информационной безопасности
1	Наименование инцидента информационной безопасности	
2	Дата и время выявления (дд.мм.гггг и чч:мм с указанием часового пояса UTC+X)	
3	Место выявления (организация, филиал, сегмент информационной инфраструктуры)	
4	Источник информации об инциденте информационной безопасности (пользователь, администратор, администратор информационной безопасности, работник подразделения информационной безопасности или техническое средство)	
5	Использованные методы при реализации инцидента информационной безопасности (социальная инженерия, внедрение вредоносного кода)	
Содержание инцидента информационной безопасности		
6	Симптомы, признаки инцидента информационной безопасности	
	Основные события (эксплуатация уязвимостей в прикладном и	

7	системном программном обеспечении; несанкционированный доступ в информационную систему; атака "отказ в обслуживании" на информационную систему или сеть передачи данных; заражение сервера вредоносной программой или кодом; совершение несанкционированного перевода денежных средств; инциденты информационной безопасности, несущие угрозу стабильности деятельности платежной организации)	
8	Пораженные активы (физический уровень информационной инфраструктуры, уровень сетевого оборудования, уровень сетевых приложений и сервисов, уровень операционных систем, уровень технологических процессов и приложений и уровень бизнес-процессов платежной организации)	
9	Статус инцидента информационной безопасности (свершившийся инцидент информационной безопасности, попытка осуществления инцидента информационной безопасности, подозрение на инцидент информационной безопасности)	
10	Ущерб	
11	Источник угрозы (выявленные идентификаторы)	
12	Преднамеренность (намеренный, ошибочный)	
Предпринятые меры по инциденту информационной безопасности		
13	Предпринятые действия (идентификация уязвимости, блокирование, восстановление)	
14	Запланированные действия, направленные на минимизацию возникновения рисков информационной безопасности	
	Оповещенные лица (фамилия, имя , отчество (при его наличии)	

15	должностных лиц, наименование государственных органов, организаций)	
16	Привлеченные специалисты (фамилия, имя, отчество (при его наличии) место работы, должность, номер телефона)	

Ответственный работник по информационной безопасности

_____ _____

(фамилия, имя, отчество (при его наличии) (подпись)

Дата "____" _____ 20 ___ года