О внесении изменений и дополнений в постановление Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 221 "Об утверждении Правил ведения реестра платежных систем"

Постановление Правления Национального Банка Республики Казахстан от 28 апреля 2022 года № 35. Зарегистрировано в Министерстве юстиции Республики Казахстан 12 мая 2022 года № 27998

Примечание ИЗПИ!

Порядок введения в действие см. п. 5.

В соответствии с подпунктом 52-7) части второй статьи 15 Закона Республики Казахстан "О Национальном Банке Республики Казахстан" и подпунктом 22) 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 № 221 "Об утверждении Правил ведения реестра платежных систем" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 14297) следующие изменения и дополнения:

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 52-7) части второй статьи 15 Закона Республики Казахстан "О Национальном Банке Республики Казахстан" и подпунктом 22) пункта 1 статьи 4 Закона Республики Казахстан "О платежах и платежных системах" **ПОСТАНОВЛЯЕТ**:";

в Правилах ведения реестра платежных систем, утвержденных указанным постановлением:

пункт 3 изложить в следующей редакции:

"3. В Правилах используются понятия, предусмотренные Законом о платежах и платежных системах и Правилами организации деятельности платежных организаций, утвержденными постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 215 "Об утверждении Правил организации деятельности платежных организаций", зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 14347.";

дополнить пунктами 4-1 и 4-2 следующего содержания:

"4-1. Порядок соблюдения мер информационной безопасности в платежной системе в соответствии с требованиями подпунктов 7) и 9) пункта 2 статьи 5 Закона о платежах и платежных системах оператора платежной системы включает:

1) сведения по инфраструктуре платежной системы (программное обеспечение и его характеристики, мощности, применяемое оборудование, методы восстановления и защиты резервирования);

2) сведения по методам совершенствования применяемых технологий в инфраструктуре платежной системы;

3) сведения по соответствию инфраструктуры платежной системы международным стандартам;

4) меры по соблюдению информационной безопасности в инфраструктуре платежной системы, обеспечивающие:

организацию системы управления информационной безопасностью, осуществление координации и контроля деятельности по обеспечению информационной безопасности инфраструктуры платежной системы и мероприятия по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности инфраструктуры платежной системы;

методологическую поддержку процесса обеспечения информационной безопасности инфраструктуры платежной системы;

выбор, внедрение и применение методов, средств и механизмов управления, обеспечение и контроль информационной безопасности инфраструктуры платежной системы;

сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности в инфраструктуре платежной системы;

анализ информации об инцидентах информационной безопасности в инфраструктуре платежной системы;

внедрение, надлежащего функционирования программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности инфраструктуры платежной системы, а также предоставление доступа к ним;

определение ограничения по использованию привилегированных учетных записей в инфраструктуре платежной системы;

организацию и проведение мероприятия по обеспечению осведомленности работников оператора платежной системы в вопросах информационной безопасности;

мониторинг состояния системы управления информационной безопасностью оператора платежной системы;

периодическое (но не реже одного раза в год) информирование руководства оператора платежной системы о состоянии системы управления информационной безопасностью;

хранение информации об инцидентах информационной безопасности в инфраструктуре платежной системы не менее пяти лет;

информирование Национального Банка о следующих выявленных инцидентах информационной безопасности в инфраструктуре платежной системы, реализованных по операциям в Республике Казахстан:

эксплуатация уязвимостей в прикладном и системном программном обеспечении инфраструктуры платежной системы;

несанкционированный доступ в информационную систему инфраструктуры платежной системы;

атака "отказ в обслуживании" на информационную систему или сеть передачи данных инфраструктуры платежной системы;

заражение сервера инфраструктуры платежной системы вредоносной программой или кодом (инцидентом);

повлекшие за собой совершение несанкционированного перевода денег вследствие нарушения контролей безопасности информационных систем и программного обеспечения инфраструктуры платежной системы.

Информация об инцидентах информационной безопасности в инфраструктуре платежной системы, указанных в настоящем пункте, предоставляется оператором платежной системы в возможно короткий срок, но не позднее сорока восьми часов с момента выявления такого инцидента оператором платежной системы по факту выявления инцидента информационной безопасности в виде карты инцидента информационной безопасности по форме согласно приложению 1-1 к Правилам и в соответствии с объемом доступной информации об инциденте на момент ее предоставления.

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

4-2. Сведения по информационным системам инфраструктуры платежной системы, содержащие информацию по применяемым в платежной системе технологиям оператора платежной системы включают описание программных модулей, обеспечивающих:

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

4) 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.";

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

2. Операторам платежных систем, за исключением Национального Банка, функционирующим на территории Республики Казахстан до введения в действие настоящего постановления, в течение двадцати рабочих дней со дня введения в действие настоящего постановления представить в Национальный Банк Республики Казахстан на бумажном носителе либо в электронном виде сведения и документы, предусмотренные частью 2 пункта 4 Правил ведения реестра платежных систем, утвержденных постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 221 "Об утверждении Правил ведения реестра платежных систем", зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 14297.

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 по истечении шестидесяти календарных дней после дня его первого официального опубликования.

Председатель
Национального Банка
Республики Казахстан *Г. Пирматов*

Приложение
к постановлению
от 28 апреля 2022 года № 35
Приложение 1-1
к Правилам ведения
реестра платежных систем
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	
7	Основные события (эксплуатация уязвимостей в прикладном и 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; иные 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 и иное)	
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)	

Ответственный работник по информационной безопасности

_____ _____

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

Дата "____" _____ 20 ___ года