О внесении изменений в постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 21 сентября 2020 года № 90 "Об утверждении Требований к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности"

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 27 ноября 2023 года № 86. Зарегистрировано в Министерстве юстиции Республики Казахстан 4 декабря 2023 года № 33717

Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка ПОСТАНОВЛЯЕТ:

1. Внести в постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 21 сентября 2020 года № 90 "Об утверждении Требований к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 21274) следующие изменения:

в Требованиях к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности, утвержденных указанным постановлением:

пункт 2 изложить в следующей редакции:

"2. В Требованиях используются понятия, предусмотренные Законом Республики Казахстан "Об информатизации", постановлением Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 "Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах", зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 16772, а также следующие понятия:

1) ретроспективный анализ событий информационной безопасности – анализ совокупности данных, полученных в ходе мониторинга событий информационной безопасности, за промежуток времени не менее трех месяцев на основе обновленных индикаторов компрометации и иных сведений о релевантных угрозах информационной безопасности с целью выявления необнаруженных ранее инцидентов информационной безопасности и (или) связанных с ними угроз информационной безопасности;

2) внутреннее расследование инцидента информационной безопасности – процесс, осуществляемый работниками банка, организации и третьими лицами в целях установления причин и предпосылок возникновения инцидента информационной безопасности, порядка реализации инцидента информационной безопасности, оценки масштаба воздействия и ущерба от реализации инцидента информационной безопасности, анализа эффективности принятых мер реагирования на инциденты информационной безопасности;

3) стандартная процедура реагирования – порядок применения неотложных мер по локализации инцидента информационной безопасности, вероятность возникновения которого высока без возможности снижения риска возникновения инцидента информационной безопасности в короткие сроки;

4) индикатор компрометации – уникальная характеристика объекта, наблюдаемого в энергозависимой памяти, на электронных носителях или в сетевом трафике, которая с большой долей вероятности указывает на компрометацию устройства;

5) уязвимость – недостаток информационной системы или ее отдельных элементов, эксплуатация которого способна привести к нарушению целостности и (или) конфиденциальности и (или) доступности информационной системы.";

пункты 8 и 9 изложить в следующей редакции:

"8. На этапе реагирования на инциденты информационной безопасности служба реагирования применяет стандартные процедуры реагирования, а в случаях низкой эффективности применения стандартных процедур реагирования, принимает оперативные меры реагирования на инциденты информационной безопасности, включающие следующие меры, но не ограничиваясь ими:

1) информирование и привлечение к процессу реагирования работников банка, организации, а также третьих лиц в целях обеспечения процесса эффективного противодействия инциденту информационной безопасности;

2) по согласованию с владельцами бизнес-процесса применение дополнительных мер контроля по частичной или полной остановке бизнес-процесса в банке, организации;

3) сбор данных с программно-технических средств, вовлеченных в инцидент информационной безопасности;

4) анализ инцидента информационной безопасности, его сдерживание и устранение его последствий;

5) ретроспективный анализ событий информационной безопасности;

6) определение индикаторов компрометации и уязвимостей, выявленных в ходе реагирования на инциденты информационной безопасности, и реализация корректирующих мер, направленных на недопущение аналогичного инцидента информационной безопасности в дальнейшем;

7) принятие решения о необходимости проведения внутреннего расследования инцидента информационной безопасности.

9. Служба реагирования обеспечивает консолидацию, систематизацию, хранение, целостность и сохранность информации об инцидентах информационной безопасности в журнале учета инцидентов информационной безопасности на бумажном носителе либо в электронном виде с отражением информации об инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах с вводом указанной информации в автоматизированную систему обработки информации по событиям и инцидентам информационной безопасности уполномоченного органа в соответствии с пунктом 12 Правил подключения и использования финансовыми организациями объекта информатизации по сбору, обработке и обмену информацией по событиям и инцидентам информационной безопасности, используемого отраслевым центром информационной безопасности финансового рынка и финансовых организаций, утвержденных постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 12 сентября 2022 года № 67, зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 29639.".

2. Департаменту информационной и кибербезопасности в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом государственную регистрацию настоящего постановления в Министерстве юстиции Республики Казахстан;

2) размещение настоящего постановления на официальном интернет-ресурсе Агентства Республики Казахстан по регулированию и развитию финансового рынка 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.

3. Контроль за исполнением настоящего постановления возложить на курирующего заместителя Председателя Агентства Республики Казахстан по регулированию и развитию финансового рынка.

4. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Председатель Агентства
Республики Казахстан
по регулированию и развитию
финансового рынка *М. Абылкасымова*