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 21 сентября 2020 года № 90. Зарегистрировано в Министерстве юстиции Республики Казахстан 25 сентября 2020 года № 21274.

Сноска. Вводится в действие с 01.01.2021 в соответствии с пунктом 4 настоящего постановления.

В соответствии с подпунктом 4) части первой статьи 13-6 Закона Республики Казахстан от 4 июля 2003 года "О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций" Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые Требования к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности.

2. Управлению 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 мероприятий, предусмотренных 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 с 1 января 2021 года и подлежит официальному опубликованию.

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

Утверждены
постановлением
Правления Агентства

Республики Казахстан
по регулированию и
развитию финансового рынка
от 21 сентября 2020 года № 90

Требования к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности

Глава 1. Общие положения

1. Настоящие Требования к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности (далее – Требования) разработаны в соответствии с Законом Республики Казахстан от 4 июля 2003 года "О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций" и устанавливают требования к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности банков второго уровня и филиалов банков-нерезидентов Республики Казахстан (далее – банк), организаций, осуществляющих отдельные виды банковских операций, (далее – организация).

Сноска. Пункт 1 - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 17.02.2021 № 34 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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.

Сноска. Пункт 2 - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 27.11.2023 № 86 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

3. Банк, организация обеспечивает создание структурного подразделения по реагированию на инциденты информационной безопасности – службу реагирования на инциденты информационной безопасности (далее – служба реагирования).

4. В целях надлежащего функционирования службы реагирования банк, организация обеспечивает:

1) внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процессы мониторинга событий информационной безопасности и реагирования на инциденты информационной безопасности;

2) определение перечня событий и (или) совокупностей событий информационной безопасности, требующих обязательного незамедлительного реагирования на них службой реагирования, с фиксацией предпринятых мер (далее – перечень событий информационной безопасности), источников событий информационной безопасности, периодичности, порядка и методов мониторинга событий информационной безопасности;

3) определение порядка отнесения событий информационной безопасности к инцидентам информационной безопасности, их классификации и приоритизации;

4) разработку, поддержание в актуальном состоянии стандартных процедур реагирования и обучение работников службы реагирования по вопросам применения стандартных процедур реагирования;

5) определение порядка информирования руководящих работников банка, организации, подразделений банка, организации и уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организаций (далее – уполномоченный орган), в том числе для принятия решения о проведении внутреннего расследования инцидента информационной безопасности;

6) определение порядка учета, хранения, обеспечения целостности и сохранности информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах, информации о результатах внутренних расследований инцидентов информационной безопасности и материалов этих расследований;

7) определение ответственных работников и (или) подразделений банка, организации, вовлеченных в процесс реагирования на инциденты информационной безопасности;

8) определение порядка принятия неотложных мер по устранению инцидентов информационной безопасности, установления причин возникновения инцидентов информационной безопасности и их последствий;

9) наделение службы реагирования полномочиями по введению дополнительных мер контроля по частичной или полной остановке бизнес-процесса в банке, организации в случае выявления инцидента информационной безопасности;

10) не реже одного раза в год пересмотр перечня событий информационной безопасности, источников событий информационной безопасности, периодичности, порядка и методов мониторинга событий информационной безопасности;

11) не реже одного раза в год анализ выявленных инцидентов информационной безопасности и нанесенного ими ущерба для рассмотрения коллегиальным органом банка, организации с целью оценки рисков информационной безопасности, корректировки методов и средств обеспечения информационной безопасности, изменения бизнес-процессов банка, организации;

12) наличие документов, сведений и фактов, подтверждающих реализацию порядка реагирования на инциденты информационной безопасности;

13) режим работы службы реагирования, обеспечивающий непрерывность реагирования на инциденты информационной безопасности, возникающие в критических информационных системах банка, организации;

14) в случаях нанесения материального ущерба банку, организации и (или) клиентам банка, организации вследствие реализации инцидента информационной безопасности, проведение внутреннего расследования инцидента информационной безопасности, с уведомлением уполномоченного органа о начале, сроках и результатах проведения расследования.

Сноска. Пункт 4 – в редакции постановления Постановление Правления Агентства РК по регулированию и развитию финансового рынка от 23.11.2022 № 95 (вводится в

действие по истечении десяти календарных дней после дня его первого официального опубликования).

5. Порядок реагирования на инциденты информационной безопасности службой реагирования устанавливается внутренними документами банка, организации и состоит из следующих этапов, включая, но не ограничиваясь ими:

1) мониторинг событий информационной безопасности и выявление инцидентов информационной безопасности (далее – этап мониторинга и выявления);

2) локализация и противодействие инциденту информационной безопасности (далее – этап реагирования);

3) внутреннее расследование инцидента информационной безопасности (далее – этап внутреннего расследования).

6. В случае передачи отдельных функций службы реагирования сторонней организации-юридическому лицу банк, организация обеспечивает исполнение Требований, в том числе путем включения соответствующих норм Требований в договоры оказания услуг, заключаемых с третьими лицами.

Глава 2. Требования к службам реагирования

7. На этапе мониторинга и выявления служба реагирования осуществляет:

1) мониторинг и анализ событий информационной безопасности;

2) отнесение событий информационной безопасности к инциденту информационной безопасности в соответствии с разработанным порядком отнесения событий информационной безопасности к инцидентам информационной безопасности;

3) классификацию и приоритизацию инцидентов информационной безопасности;

4) передачу информации об инциденте информационной безопасности на этап реагирования.

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.

Сноска. Пункт 8 - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 27.11.2023 № 86 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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.

Сноска. Пункт 9 - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 27.11.2023 № 86 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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

Глава 3. Требования к проведению внутренних расследований инцидентов информационной безопасности

11. На этапе внутреннего расследования инцидента информационной безопасности банком, организацией обеспечивается:

1) привлечение к внутреннему расследованию инцидента информационной безопасности ответственных работников и (или) подразделений банка, организации, вовлеченных в процесс реагирования на инциденты информационной безопасности, а также третьих лиц;

2) сбор и анализ материалов, необходимых для проведения внутреннего расследования инцидента информационной безопасности;

3) установление причин возникновения инцидента информационной безопасности и порядка реализации инцидента информационной безопасности;

4) оценка масштаба воздействия и ущерба от реализации инцидента информационной безопасности;

5) анализ эффективности принятых мер реагирования на расследуемый инцидент информационной безопасности;

6) подготовка заключения о результатах расследования инцидента информационной безопасности, в котором отражается информация об инциденте информационной безопасности, а также рекомендации по принятию корректирующих мер в целях снижения вероятности и возможного ущерба от повторной реализации инцидента информационной безопасности.

12. Банк, организация в соответствии с внутренними документами банка, организации информирует о результатах расследования инцидента информационной безопасности руководящих работников банка, организации, уполномоченный орган и, при необходимости, представителей других подразделений банка, организации.

13. Банк, организация обеспечивает консолидацию, систематизацию, целостность и сохранность информации о результатах внутреннего расследования инцидента информационной безопасности и материалов расследования на бумажном носителе и (или) в электронном виде.

14. Срок хранения информации о результатах внутреннего расследования инцидента информационной безопасности и материалов расследования составляет не менее 5 (пяти) лет.