О внесении изменений и дополнений в постановление Правления Национального Банка Республики Казахстан от 27 сентября 2018 года № 228 "Об утверждении Требований к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов, являющихся банками, организациями, осуществляющими отдельные виды банковских операций, микрофинансовыми организациями и коллекторскими агентствами, а также Требований, предъявляемых кредитными бюро к поставщикам информации и получателям кредитных отчетов в соответствии с подпунктом 11) пункта 2 и подпунктом 9) пункта 3 статьи 27 Закона Республики Казахстан от 6 июля 2004 года "О кредитных бюро и формировании кредитных историй в Республике Казахстан"

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 16 августа 2024 года № 59. Зарегистрировано в Министерстве юстиции Республики Казахстан 19 августа 2024 года № 34948

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

1. Внести в постановление Правления Национального Банка Республики Казахстан от 27 сентября 2018 года № 228 "Об утверждении Требований к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов, являющихся банками, организациями, осуществляющими отдельные виды банковских операций, микрофинансовыми организациями и коллекторскими агентствами, а также Требований, предъявляемых кредитными бюро к поставщикам информации и получателям кредитных отчетов в соответствии с подпунктом 11) пункта 2 и подпунктом 9) пункта 3 статьи 27 Закона Республики Казахстан от 6 июля 2004 года "О кредитных бюро и формировании кредитных историй в Республике Казахстан" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 17702) (далее - постановление) следующие изменения и дополнения:

в постановлении:

заголовок изложить в следующей редакции: "Об утверждении Требований к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро,

поставщиков информации и получателей кредитных отчетов, а также Требований, предъявляемых кредитными бюро к поставщикам информации и получателям кредитных отчетов;

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 6) статьи 5 Закона Республики Казахстан "О кредитных бюро и формировании кредитных историй в Республике Казахстан" Правление Национального Банка Республики Казахстан **ПОСТАНОВЛЯЕТ:**";

пункт 1 изложить в следующей редакции:

"1. Утвердить:

1) Требования к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов согласно приложению 1 к настоящему постановлению;

2) Требования, предъявляемые кредитными бюро к поставщикам информации и получателям кредитных отчетов согласно приложению 2 к настоящему постановлению.
";

в приложении 1:

заголовок изложить в следующей редакции:

"Требования к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов";

пункт 1 изложить в следующей редакции:

"1. Настоящие Требования к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов разработаны в соответствии с подпунктом 6) статьи 5 Закона Республики Казахстан "О кредитных бюро и формировании кредитных историй в Республике Казахстан" и устанавливают требования к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, банков, организаций, осуществляющих отдельные виды банковских операций, организаций, осуществляющих микрофинансовую деятельность, коллекторских агентств и сервисных компаний, осуществляющих доверительное управление правами (требованиями) по договорам банковского займа и (или) договорам о предоставлении микрокредита в рамках договора доверительного управления правами (требованиями) по договорам банковского займа и (или) договорам о предоставлении микрокредита, заключенного с банком, организацией, осуществляющей отдельные виды банковских операций, организацией, осуществляющей микрофинансовую деятельность, коллекторским агентством, дочерней организацией банка, приобретающей

сомнительные и безнадежные активы родительского банка, организацией, специализирующейся на улучшении качества кредитных портфелей банков второго уровня, юридическим лицом – залогодержателем прав требования по договору о предоставлении микрокредита при выпуске микрофинансовой организацией обеспеченных облигаций или получении займов, специальной финансовой компанией, созданной в соответствии с законодательством Республики Казахстан о проектном финансировании и секьюритизации, при сделке секьюритизации, лицом, осуществляющим выкуп ипотечных займов физических лиц, не связанных с предпринимательской деятельностью, сто процентов акций которого принадлежат Национальному Банку Республики Казахстан, специальном фондом развития частного предпринимательства – по договору банковского займа, по договору о предоставлении микрокредита, заключенному в рамках сделки по финансированию субъектов частного предпринимательства путем обусловленного размещения средств в банках и организациях, осуществляющих отдельные виды банковских операций, микрофинансовых организациях, иным лицом – в отношении права (требования) по договору банковского займа, по договору о предоставлении микрокредита физического лица, связанного с осуществлением предпринимательской деятельности, или по договору банковского займа, по договору о предоставлении микрокредита юридического лица, по которому выявлены признаки обесценения в соответствии с международными стандартами финансовой отчетности, в том числе на момент приобретения или возникновения (создания) права (требования) по договору банковского займа, по договору о предоставлении микрокредита.";

пункт 37 изложить в следующей редакции:

"37. Руководители структурных подразделений кредитного бюро:

1) обеспечивают ознакомление работников с внутренними документами кредитного бюро, содержащими требования к информационной безопасности (далее – требования к информационной безопасности);

2) несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях;

3) обеспечивают заключение соглашений о неразглашении конфиденциальной информации и включение условий об обеспечении информационной безопасности в соглашения, договоры на оказание услуг/выполнение работ в случаях, когда подразделение кредитного бюро выступает инициатором заключения таких соглашений, договоров.";

дополнить пунктом 40-1 следующего содержания:

"40-1. Доступ к информационным активам кредитного бюро третьих лиц предоставляется на период и в объеме, определяемыми проводимыми работами на основании соглашения, договора, включающего условия о соблюдении требований к информационной безопасности, за исключением случаев, предусмотренных

законодательством Республики Казахстан. В соглашениях, договорах, заключаемых с поставщиком информации, получателем кредитных отчетов, третьими лицами, содержатся положения о конфиденциальности, условия о возмещении ущерба, возникшего вследствие нарушения информационной безопасности, а также сбоев в работе информационных систем и нарушения их безопасности, вызванных действием или бездействием кредитного бюро, поставщика информации, получателя кредитных отчетов, третьих лиц.";

заголовок параграфа 7 изложить в следующей редакции:

"Параграф 7. Требования к предоставлению информации о состоянии системы управления информационной безопасностью, событиях и инцидентах информационной безопасности кредитных бюро";

пункты 79, 80 и 81 изложить в следующей редакции:

"79. Кредитное бюро ежегодно, не позднее 20 января года, следующего за отчетным годом, представляет в уполномоченный орган информацию о состоянии системы управления информационной безопасностью и ее соответствии Требованиям.

80. Информация о состоянии системы управления информационной безопасностью включает сведения о (об):

1) сфере действия системы управления информационной безопасностью кредитного бюро и ее участниках с указанием соответствия их функционала Требованиям;

2) наличии документов, регламентирующих создание и функционирование системы управления информационной безопасностью;

3) наличии и количественном составе программно-технических средств, используемых для обеспечения информационной безопасности;

4) имеющихся в договорах о предоставлении услуг, заключенных с операторами связи, условиях и обязательствах по обеспечению информационной безопасности;

5) наличии, материально-технической обеспеченности и готовности резервных центров обработки данных;

6) проведенных мероприятиях по приведению системы управления информационной безопасностью и информационных активов кредитного бюро в соответствие с Требованиями.

81. Информация о состоянии системы управления информационной безопасностью, событиях и инцидентах информационной безопасности представляется в уполномоченный орган посредством автоматизированной системы обработки информации (далее – АСОИ), предназначенной для обработки информации о событиях и инцидентах информационной безопасности и интегрированной с системами информационной безопасности или системами кредитного бюро, осуществляющими в реальном времени сбор и анализ информации о событиях в информационной

инфраструктуре или в электронном формате с использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых данных.

Для кредитного бюро с государственным участием допускается представление информации о событиях и инцидентах информационной безопасности в уполномоченный орган посредством объектов информатизации Национального Банка Республики Казахстан, интегрированных с АСОИ.";

дополнить пунктами 81-1 и 81-2 следующего содержания:

"81-1. Кредитное бюро предоставляет в уполномоченный орган 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) иных инцидентах информационной безопасности, повлекших простои информационных систем более одного часа.

Информация об инцидентах информационной безопасности, указанных в настоящем пункте, предоставляется незамедлительно кредитным бюро посредством АСОИ или в электронном формате с использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых данных.

Для кредитного бюро с государственным участием допускается представление информации о событиях и инцидентах информационной безопасности в уполномоченный орган посредством объектов информатизации Национального Банка Республики Казахстан, интегрированных с АСОИ.

81-2. Информация о событиях информационной безопасности предоставляется в автоматизированном режиме путем передачи из систем информационной безопасности или систем кредитного бюро, осуществляющих в реальном времени сбор и анализ информации о событиях в информационной инфраструктуре кредитного бюро в АСОИ.

Для кредитного бюро с государственным участием допускается представление информации о событиях и инцидентах информационной безопасности в уполномоченный орган посредством объектов информатизации Национального Банка Республики Казахстан, интегрированных с АСОИ.";

главу 3 дополнить параграфом 8 следующего содержания:

"Параграф 8. Требования к обеспечению информационной безопасности программного обеспечения дистанционного оказания услуг кредитных бюро

81-3. Программное обеспечение дистанционного оказания услуг кредитного бюро включает:

1) программное обеспечение серверов веб-приложений (далее – веб-приложение);

2) программное обеспечение для мобильных устройств (далее – мобильное приложение);

3) программное обеспечение серверов программных интерфейсов (далее – серверное ППО).

81-4. Разработка и (или) доработка программного обеспечения дистанционного оказания услуг осуществляется кредитным бюро в соответствии с внутренними документами кредитного бюро, регламентирующими порядок разработки и (или) доработки программного обеспечения, этапы разработки и их участников.

81-5. В случае, если разработка и (или) доработка программного обеспечения дистанционного оказания услуг кредитного бюро передана сторонней организации и (или) третьему лицу, кредитное бюро обеспечивает исполнение сторонней организацией и (или) третьим лицом требований настоящей главы и внутренних документов, отвечает за состояние безопасности программного обеспечения дистанционного оказания услуг.

81-6. Хранение исходных кодов программного обеспечения дистанционного оказания услуг, разрабатываемых в кредитном бюро, осуществляется в специализированных системах управления репозиториями кода, размещаемых в периметре защиты кредитного бюро, с обеспечением резервного копирования.

81-7. Независимо от принятого в кредитном бюро подхода к разработке и (или) доработке программного обеспечения дистанционного оказания услуг, обязательным является тестирование безопасности, в ходе которого осуществляются, как минимум, следующие мероприятия:

1) статический анализ исходного кода;

2) анализ компонентов и (или) сторонних библиотек.

81-8. Статический анализ исходного кода программного обеспечения дистанционного оказания услуг кредитного бюро проводится с использованием сканера статического анализа исходных кодов, поддерживающего анализ всех используемых языков программирования в проверяемом программном обеспечении, в функции которого входит выявление следующих уязвимостей, но не ограничиваясь:

1) наличие механизмов, допускающих инъекции вредоносного кода;

2) использование уязвимых операторов и функций языков программирования;

3) использование слабых и уязвимых криптографических алгоритмов;

4) использование кода, вызывающего при определенных условиях отказ в обслуживании или существенное замедление работы программного обеспечения дистанционного оказания услуг кредитного бюро;

5) наличие механизмов обхода систем защиты программного обеспечения дистанционного оказания услуг кредитного бюро;

6) использование в коде секретов в открытом виде;

7) нарушение шаблонов и практик обеспечения безопасности приложения.

81-9. Анализ компонентов и (или) сторонних библиотек программного обеспечения дистанционного оказания услуг кредитного бюро проводится с целью выявления известных уязвимостей, присущих используемой версии компонента и (или) сторонней библиотеки, а также отслеживания зависимостей между компонентами и (или) сторонними библиотеками и их версиями.

81-10. Кредитное бюро обеспечивает реализацию корректирующих мер по устранению выявленных уязвимостей в порядке, определенном внутренним документом, утвержденным исполнительным органом. При этом критичные уязвимости устраняются до ввода в эксплуатацию программного обеспечения дистанционного оказания услуг и (или) его новых версий.

81-11. Кредитное бюро осуществляет ввод в эксплуатацию программного обеспечения дистанционного оказания услуг и (или) его новых версий после согласования с подразделением по информационной безопасности.

81-12. Кредитное бюро обеспечивает хранение и доступ в оперативном режиме ко всем версиям исходных кодов программного обеспечения дистанционного оказания услуг и результатов тестирования безопасности, которые были введены в эксплуатацию в течение последних 3 (трех) лет.

81-13. Обмен данными между клиентской и серверной сторонами программного обеспечения дистанционного оказания услуг шифруется с использованием версии протокола шифрования Transport Layer Security (Транспорт Лэйер Секьюрити) не ниже 1.2.

81-14. При первичной регистрации клиента в мобильном приложении кредитное бюро осуществляет биометрическую идентификацию клиента посредством Центра обмена идентификационными данными (далее - ЦОИД), либо с использованием биометрических данных, полученных посредством устройств кредитного бюро.

81-15. Изменение кода доступа (пароля) к мобильному приложению осуществляется с применением биометрической идентификации клиента с использованием биометрических данных, подтвержденных ЦОИД, либо с использованием биометрических данных, полученных посредством устройств кредитного бюро.

81-16. Идентификация и аутентификация клиента в программном обеспечении дистанционного оказания услуг осуществляется с применением способов

двухфакторной аутентификации (использованием двух из трех факторов: знания, владения, неотъемлемости) в соответствии с процедурами безопасности, установленными внутренними документами кредитного бюро.

81-17. Механизм кроссдоменной аутентификации программного обеспечения дистанционного оказания услуг согласовывается с подразделением по информационной безопасности.

81-18. Веб-приложение обеспечивает:

1) однозначность идентификации принадлежности веб-приложения кредитному бюро (доменное имя, логотипы, корпоративные цвета);

2) запрет на сохранение в памяти браузера авторизационных данных;

3) маскирование вводимых секретов;

4) информирование на странице авторизации клиента о мерах обеспечения кибергигиены, которым рекомендуется следовать при использовании веб-приложения;

5) обработку ошибок и исключений безопасным способом, не допуская отображение в интерфейсе клиента конфиденциальных данных, предоставляя минимально достаточную информацию об ошибке.

81-19. Мобильное приложение обеспечивает:

1) однозначность идентификации принадлежности мобильного приложения кредитному бюро (данные в официальном магазине приложений, логотипы, корпоративные цвета);

2) блокировку функционала по оказанию дистанционных услуг кредитного бюро в случае обнаружения признаков нарушения целостности и (или) обхода защитных механизмов операционной системы, обнаружения процессов удаленного управления;

3) уведомление клиента о наличии обновлений мобильного приложения;

4) возможность принудительной установки обновлений мобильного приложения или блокировки функционала мобильного приложения до их установки в случаях необходимости устранения критичных уязвимостей;

5) хранение конфиденциальных данных в защищенном контейнере мобильного приложения или хранилище системных учетных данных;

6) исключение кэширования конфиденциальных данных;

7) исключение из резервных копий мобильного приложения конфиденциальных данных в открытом виде;

8) информирование клиента о методах обеспечения кибергигиены, которым рекомендуется следовать при использовании мобильного приложения;

9) информирование клиента о событиях авторизации под его учетной записью, изменения и (или) восстановления пароля, изменения, зарегистрированного кредитным бюро номера мобильного телефона;

10) в ходе осуществления операций с денежными средствами - передачу в серверное ППО кредитного бюро геолокационных данных мобильного устройства при

наличии разрешения от клиента либо передачу информации об отсутствии такого разрешения.

81-20. Кредитное бюро обеспечивает на своей стороне:

1) обработку ошибок и исключений безопасным способом, не допуская в ответе раскрытия конфиденциальных данных, предоставляя минимально достаточную информацию для диагностики проблемы;

2) идентификацию и аутентификацию мобильных приложений и связанных с ними устройств;

3) проверку данных на валидность для предотвращения атак с подделкой запросов и инъекций вредоносного кода.";

в приложении 2:

заголовок изложить в следующей редакции:

"Требования, предъявляемые кредитными бюро к поставщикам информации и получателям кредитных отчетов";

пункт 1 изложить в следующей редакции:

"1. Настоящие Требования, предъявляемые кредитными бюро к поставщикам информации и получателям кредитных отчетов (далее - Требования), разработаны в соответствии с подпунктом 6) статьи 5 Закона Республики Казахстан "О кредитных бюро и формировании кредитных историй в Республике Казахстан" и определяют требования, предъявляемые кредитными бюро к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности поставщиков информации, являющихся индивидуальным предпринимателем или юридическим лицом, реализующим товары и услуги в кредит либо предоставляющим отсрочки платежей, систематизированные признаки которых определяются постановлением Правительства Республики Казахстан от 18 января 2005 года № 25 "Об утверждении систематизированных признаков индивидуальных предпринимателей или юридических лиц, реализующих товары и услуги в кредит либо предоставляющих отсрочки платежей" (далее – постановление № 25), субъектами естественной монополии, оказывающими коммунальные услуги, иными лицами на основании договоров о предоставлении информации (далее – поставщики информации), а также получателей кредитных отчетов, являющихся индивидуальным предпринимателем или юридическим лицом, реализующим товары и услуги в кредит либо предоставляющим отсрочки платежей, систематизированные признаки которых определяются постановлением № 25, иными лицами на основании договоров о предоставлении информации, представителем держателей облигаций в отношении кредитного отчета эмитента облигаций, с которым заключен договор о представлении интересов держателей облигаций (далее – получатели кредитных отчетов).".

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*