Об утверждении Правил обеспечения информационной безопасности электронной торговой площадки по продаже банковских и микрофинансовых активов

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 16 августа 2024 года № 57. Зарегистрировано в Министерстве юстиции Республики Казахстан 19 августа 2024 года № 34951

Примечание ИЗПИ!

Вводится в действие с 20.08.2024

В соответствии с частью второй пункта 4 статьи 15-18 Закона Республики Казахстан "О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций" Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка ПОСТАНОВЛЯЕТ:

1. Утвердить Правила обеспечения информационной безопасности электронной торговой площадки по продаже банковских и микрофинансовых активов согласно приложению к настоящему постановлению.

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 с 20 августа 2024 года и подлежит официальному опубликованию.

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

Приложение к постановлению
Правления Агентства
Республики Казахстан
по регулированию и развитию

финансового рынка
от 16 августа 2024 года № 57

Правила обеспечения информационной безопасности электронной торговой площадки по продаже банковских и микрофинансовых активов

Глава 1. Общие положения

1. Настоящие Правила обеспечения информационной безопасности электронной торговой площадки по продаже банковских и микрофинансовых активов (далее – Правила) разработаны в соответствии с частью второй пункта 4 статьи 15-18 Закона Республики Казахстан "О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций" (далее – Закон о государственном регулировании) и определяют порядок обеспечения уполномоченным органом по регулированию, контролю и надзору финансового рынка и финансовых организаций (далее – уполномоченный орган) информационной безопасности электронной торговой площадки по продаже банковских и микрофинансовых активов (далее – электронная торговая площадка).

2. В Правилах используются понятия, предусмотренные законами Республики Казахстан "Об информатизации", "Об электронном документе и электронной цифровой подписи" и Законом о государственном регулировании.

Глава 2. Обеспечение информационной безопасности электронной торговой площадки

3. Информационная безопасность электронной торговой площадки обеспечивается оператором электронной торговой площадки (далее – оператор) путем:

1) организации доступа к электронной торговой площадке работникам оператора и участникам торгов, проводимых на электронной торговой площадке (далее – участники);

2) защиты информации, находящейся в электронной торговой площадке, при ее обработке, хранении и передаче;

3) резервирования и обеспечения доступности информации, находящейся в электронной торговой площадке;

4) процедур восстановления информационной системы электронной торговой площадки после сбоев и отказов оборудования и программного обеспечения;

5) обеспечения шифрования передаваемой информации на электронной торговой площадке между оператором и участником.

4. Оператор обеспечивает доступ к электронной торговой площадке работникам оператора и участникам путем идентификации и аутентификации работников оператора и участников.

5. Доступ к электронной торговой площадке предоставляется работникам оператора в объеме, определяемом их функциональными обязанностями.

6. На электронной торговой площадке используются персонализированные учетные записи работников оператора.

7. На электронной торговой площадке применяются функции по управлению учетными записями, защите паролей, а также блокировке и разблокировке учетных записей работников оператора в информационной системе электронной торговой площадки.

8. Идентификация и аутентификация работников оператора в информационной системе электронной торговой площадки осуществляется с применением двухфакторной аутентификации (использованием двух из трех факторов: знания, владения, неотъемлемости) в соответствии с процедурами безопасности.

9. Первичная регистрация участника на электронной торговой площадке осуществляется с помощью электронной цифровой подписи, предоставленной аккредитованным удостоверяющим центром Республики Казахстан, или с применением услуги биометрической идентификации участника посредством Центра обмена идентификационными данными (далее – ЦОИД) или с использованием биометрических данных, полученных посредством устройств электронной торговой площадки.

10. Идентификация и аутентификация участника осуществляется с применением двухфакторной аутентификации (использованием двух из трех факторов: знания, владения, неотъемлемости) с обязательным применением как минимум одного из следующих способов:

1) электронная цифровая подпись, предоставленная аккредитованным удостоверяющим центром Республики Казахстан;

2) биометрическая идентификация посредством использования услуг ЦОИД или с использованием биометрических данных, полученных посредством устройств электронной торговой площадки.

11. Изменение кода доступа (пароля) к электронной торговой площадке осуществляется с применением биометрической идентификации участника с использованием биометрических данных, подтвержденных ЦОИД, или полученных посредством устройств электронной торговой площадки.

12. Оператор обеспечивает антивирусную защиту всех компонентов информационной системы электронной торговой площадки.

13. Обновления безопасности компонентов информационной системы электронной торговой площадки, устраняющие критичные уязвимости, устанавливаются не позднее одного месяца со дня их публикации и распространения производителем.

14. Обновления программных и аппаратных компонентов информационной системы электронной торговой площадки до установки в промышленную среду проходят испытания в тестовой среде.

15. Оператор обеспечивает резервное хранение данных, файлов и конфигураций всех компонентов информационной системы электронной торговой площадки в целях восстановления ее работоспособной копии.

16. Порядок и периодичность резервного копирования, хранения, восстановления информации, периодичность тестирования восстановления работоспособности информационной системы электронной торговой площадки из ее резервных копий определяются оператором.

17. Оператор обеспечивает неизменность документов, подтверждающих выполнение процессов и процедур, записей в журналах событий, снимков экрана, результатов аудио-, фото- и видеофиксации, в информационной системе электронной торговой площадки как на организационном, так и на техническом уровне.

Срок хранения данных, предусмотренных частью первой настоящего пункта, составляет не менее 3 (трех) месяцев в оперативном доступе и не менее 5 (пяти) лет в архивном доступе.

18. Программное обеспечение информационной системы электронной торговой площадки включает:

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

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

3) программное обеспечение серверов программных интерфейсов.

19. Разработка и (или) доработка программного обеспечения информационной системы электронной торговой площадки осуществляется в соответствии с порядком разработки и (или) доработки программного обеспечения, этапов разработки и их участников оператора.

Если разработка и (или) доработка программного обеспечения информационной системы электронной торговой площадки передана сторонней организации и (или) третьему лицу, оператор предоставляет доступ к информационной системе электронной площадки сторонней организации и (или) третьему лицу на период и в объеме, определяемыми проводимыми работами, на основании договора, содержащего условия об обеспечении информационной безопасности электронной торговой площадки. В договорах, заключаемых со сторонней организацией и (или) третьим лицом, содержатся положения о конфиденциальности, условия о возмещении ущерба, возникшего вследствие нарушения информационной безопасности, а также сбоев в работе информационной системы электронной торговой площадки, вызванных действием или бездействием сторонней организации и (или) третьего лица.

20. Хранение исходных кодов программного обеспечения информационной системы электронной торговой площадки осуществляется в специализированных системах управления репозиториями кода, размещаемыми в периметре защиты оператора с обеспечением резервного копирования.

21. Независимо от принятого у оператора подхода к разработке и (или) доработке программного обеспечения информационной системы электронной торговой площадки обязательным этапом является тестирование информационной безопасности электронной торговой площадки, в ходе которого осуществляются, как минимум, следующие мероприятия:

1) статический анализ исходного кода;

2) анализ компонентов и сторонних библиотек.

22. Статический анализ исходного кода программного обеспечения информационной системы электронной торговой площадки 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 функций языков программирования;

3) использование слабых и уязвимых криптографических алгоритмов;

4) использование кода, вызывающего отказ в обслуживании или существенное замедление работы программного обеспечения информационной системы электронной торговой площадки;

5) наличие механизмов обхода систем защиты программного обеспечения информационной системы электронной торговой площадки;

6) использование в коде секретов в открытом виде;

7) нарушение шаблонов и практик обеспечения безопасности программного обеспечения информационной системы электронной торговой площадки.

23. Анализ компонентов и (или) сторонних библиотек программного обеспечения информационной системы электронной торговой площадки проводится с целью выявления уязвимостей, присущих используемой версии компонента и (или) сторонней библиотеки, а также отслеживания зависимостей между компонентами и (или) сторонними библиотеками и их версиями.

24. Оператор обеспечивает хранение и доступ в оперативном режиме ко всем версиям исходных кодов программного обеспечения информационной системы электронной торговой площадки и результатов тестирования информационной безопасности, которые были введены в эксплуатацию в течение последних 3 (трех) лет.

25. Обмен данными между клиентской и серверной сторонами программного обеспечения информационной системы электронной торговой площадки шифруется с

использованием версии протокола шифрования Transport Layer Security (Транспорт Лэйер Секьюрити) не ниже 1.2.

26. Веб-приложение обеспечивает:

1) однозначность идентификации принадлежности веб-приложения оператору (доменное имя, логотипы, корпоративные цвета, публичная контактная информация);

2) запрет на сохранение в памяти браузера авторизационных данных;

3) маскирование вводимых секретов;

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

5) обработку ошибок и исключений безопасным способом, не допуская отображение в интерфейсе участника конфиденциальных данных, предоставляя минимально достаточную информацию для диагностики проблемы.

27. Мобильное приложение обеспечивает:

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

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

3) уведомление участника 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) обмен данными только с авторизованным серверным программным обеспечением серверов программных интерфейсов электронной торговой площадки;

7) исключение кэширования конфиденциальных данных;

8) исключение из резервных копий мобильного приложения конфиденциальных данных;

9) информирование участника о действенных методах обеспечения кибербезопасности, которым рекомендуется следовать при использовании мобильного приложения;

10) информирование клиента о событиях авторизации под его учетной записью, изменении и (или) восстановлении пароля, изменении, номера мобильного телефона, зарегистрированного электронной торговой площадкой;

11) передачу в серверное программное обеспечение серверов программных интерфейсов электронной торговой площадки геолокационных данных мобильного устройства при наличии разрешения от клиента либо передачу информации об отсутствии такого разрешения.

28. Серверное программное обеспечение серверов программных интерфейсов электронной торговой площадки обеспечивает:

1) контроль скорости приема запросов со стороны мобильных и веб-приложений участника;

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

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

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