О внесении изменений и дополнения в постановление Правления Национального Банка Республики Казахстан от 30 июля 2018 года № 164 "Об утверждении Требований к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой (перестраховочной) организации, а также кибербезопасности страховой (перестраховочной) организации"

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 29 августа 2024 года № 73. Зарегистрировано в Министерстве юстиции Республики Казахстан 3 сентября 2024 года № 35024

Примечание ИЗПИ!

Порядок введения в действие см. п. 4.

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

1. Внести в постановление Правления Национального Банка Республики Казахстан от 30 июля 2018 года № 164 "Об утверждении Требований к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой (перестраховочной) организации, а также кибербезопасности страховой (перестраховочной) организации" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 17289) следующие изменения и дополнение:

преамбулу изложить в следующей редакции:

"В соответствии с Законом Республики Казахстан "О страховой деятельности" Правление Национального Банка Республики Казахстан **ПОСТАНОВЛЯЕТ:**";

в Требованиях к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой (перестраховочной) организации, а также кибербезопасности страховой (перестраховочной) организации, утвержденных указанным постановлением:

пункт 1 изложить в следующей редакции:

"1. Настоящие Требования к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой (перестраховочной) организации, а также кибербезопасности страховой (перестраховочной) организации (далее – Требования) разработаны в соответствии с Законом Республики Казахстан "О страховой деятельности" и устанавливают требования к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным,

хранящимся в страховой (перестраховочной) организации, а также кибербезопасности страховой (перестраховочной) организации.";

пункт 52 изложить в следующей редакции:

"52. Информация, указанная в пункте 50 Требований, представляется в уполномоченный орган посредством автоматизированной системы обработки информации, предназначенной для обработки информации о событиях и инцидентах информационной безопасности, или в электронном формате с использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых данных.";

дополнить главой 3 следующего содержания:

"Глава 3. Требования к обеспечению информационной безопасности программного обеспечения дистанционного оказания услуг страховой (перестраховочной) организации

54. Программное обеспечение дистанционного оказания услуг страховой (перестраховочной) организации 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).

55. Разработка и (или) доработка программного обеспечения дистанционного оказания услуг осуществляется страховой (перестраховочной) организации в соответствии с внутренними документами страховой (перестраховочной) организации, регламентирующими порядок разработки и (или) доработки программного обеспечения , этапы разработки и их участников.

56. Если разработка и (или) доработка программного обеспечения дистанционного оказания услуг страховой (перестраховочной) организации передана сторонней организации и (или) третьему лицу, страховая (перестраховочная) организации обеспечивает исполнение сторонней организацией и (или) третьим лицом требований настоящей главы и внутренних документов, отвечает за состояние безопасности программного обеспечения дистанционного оказания услуг.

57. Хранение исходных кодов программного обеспечения дистанционного оказания услуг, разрабатываемых в страховой (перестраховочной) организации, осуществляется в специализированных системах управления репозиториями кода, размещаемых в периметре защиты страховой (перестраховочной) организации, с обеспечением резервного копирования.

58. Независимо от принятого в страховой (перестраховочной) организации подхода к разработке и (или) доработке программного обеспечения дистанционного оказания

услуг, обязательным является тестирование основных функций системы, таких как регистрация пользователей, обмен сообщениями и другие ключевые операции, проверка безопасности системы для защиты от угроз, таких как несанкционированный доступ, фишинг, взлом и утечка данных.

59. Страховая (перестраховочная) организация 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.

60. Страховая (перестраховочная) организация осуществляет ввод в эксплуатацию программного обеспечения дистанционного оказания услуг и (или) его новых версий, после согласования с ответственным лицом по информационной безопасности.

61. Страховая (перестраховочная) организация 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.

62. 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.

63. При первичной регистрации клиента в мобильном приложении страховая (перестраховочная) организация осуществляет биометрическую идентификацию клиента посредством Центра обмена идентификационными данными (далее - ЦОИД) и одноразового персонального идентификатора (пароля) полученного в SMS-сообщении.

64. Изменение кода доступа (пароля) к мобильному приложению осуществляется с применением биометрической идентификации клиента с использованием биометрических данных, подтвержденных ЦОИД и одноразового персонального идентификатора (пароля) полученного в SMS-сообщении.

65. 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 страховой (перестраховочной) организации.

66. Механизм кроссдоменной аутентификации программного обеспечения дистанционного оказания услуг согласовывается с подразделением по информационной безопасности.

67. Веб-приложение обеспечивает:

1) однозначность идентификации принадлежности веб-приложения страховой (перестраховочной) организации (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.

68. Мобильное приложение обеспечивает:

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

2) блокировку функционала по оказанию дистанционных услуг страховой (перестраховочной) организации 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 страховой организацией номера мобильного телефона;

10) в ходе осуществления операций с денежными средствами - передачу в серверное ППО страховой (перестраховочной) организации геолокационных данных мобильного устройства при наличии разрешения от клиента либо передачу информации об отсутствии такого разрешения.

69. Страховая (перестраховочная) организация 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.".

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 шестидесяти календарных дней после дня его первого официального опубликования.

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