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 Национального Банка Республики Казахстан от 30 июля 2018 года № 164. Зарегистрировано в Министерстве юстиции Республики Казахстан 9 августа 2018 года № 17289.

Примечание РЦПИ!

Настоящее постановление вводится в действие с 1 января 2019 года.

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

Сноска. Преамбула - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 29.08.2024 № 73 (вводится в действие по истечении шестидесяти календарных дней после дня его первого официального опубликования).

1. Утвердить прилагаемые 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.

2. Департаменту регулирования небанковских финансовых организаций (Кошербаева А.М.) в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом (Сарсенова Н.В.) государственную регистрацию настоящего постановления в Министерстве юстиции Республики Казахстан;

2) в течение десяти календарных дней со дня государственной регистрации настоящего постановления направление его копии в бумажном и электронном виде на казахском и русском языках в Республиканское государственное предприятие на праве хозяйственного ведения "Республиканский центр правовой информации" для официального опубликования и включения в Эталонный контрольный банк нормативных правовых актов Республики Казахстан;

3) размещение настоящего постановления на официальном интернет-ресурсе Национального Банка Республики Казахстан после его официального опубликования;

4) в течение десяти рабочих дней после государственной регистрации настоящего постановления представление в Юридический департамент сведений об исполнении

мероприятий, предусмотренных подпунктами 2), 3) настоящего пункта и пунктом 3 настоящего постановления.

3. Управлению по защите прав потребителей финансовых услуг и внешних коммуникаций (Терентьев А.Л.) обеспечить в течение десяти календарных дней после государственной регистрации настоящего постановления направление его копии на официальное опубликование в периодические печатные издания.

4. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Национального Банка Республики Казахстан Курманова Ж.Б.

5. Настоящее постановление вводится в действие с 1 января 2019 года и подлежит официальному опубликованию.

Председатель
Национального Банка *Д. Акишев*

Утверждены
постановлением Правления
Национального Банка
Республики Казахстан
от 30 июля 2018 года № 164

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

Глава 1. Общие положения

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.

Сноска. Пункт 1 - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 29.08.2024 № 73 (вводится в действие по истечении шестидесяти календарных дней после дня его первого официального опубликования).

2. В Требованиях используются следующие понятия:

1) информационный актив – совокупность информации и объекта информационной-коммуникационной инфраструктуры, используемого для хранения и (или) обработки информации;

2) объекты информационной-коммуникационной инфраструктуры – информационные системы страховой (перестраховочной) организации, технологические платформы, аппаратно-программные комплексы, сети телекоммуникаций, а также системы обеспечения бесперебойного функционирования технических средств и информационной безопасности;

3) информационно-коммуникационная инфраструктура (далее – информационная инфраструктура) – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

4) информационная безопасность – состояние защищенности электронных информационных ресурсов, информационных систем и информационной инфраструктуры от внешних и внутренних угроз;

5) угроза информационной безопасности - совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

6) обеспечение информационной безопасности – процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов страховой (перестраховочной) организации;

7) инцидент информационной безопасности – отдельно или серийно возникающие сбои в работе информационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов страховой (перестраховочной) организации;

8) центр обработки данных – специально выделенное помещение, в котором размещено серверное и коммуникационное оборудование информационной инфраструктуры страховой (перестраховочной) организации;

9) доступ – возможность использования информационных активов;

10) резервная копия – копия данных на носителе информации, предназначенная для восстановления данных в оригинальном или новом месте их расположения в случае необходимости;

11) информационная система страховой (перестраховочной) организации – информационная система, в которой хранятся и обрабатываются данные страховой (перестраховочной) организации и ее клиентов;

12) технологическая учетная запись – учетная запись в информационной системе, предназначенная для аутентификации между информационными системами;

13) уполномоченный орган – уполномоченный орган по регулированию, контролю и надзору финансового рынка и финансовых организаций;

14) атака – попытка уничтожения, раскрытия, изменения, ограничения доступа, кражи, получения несанкционированного доступа или несанкционированного использования информационного актива.

Глава 2. 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

3. Страховая (перестраховочная) организация организует безопасную работу, обеспечивающую сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой (перестраховочной) организации, а также кибербезопасность страховой (перестраховочной) организации путем создания системы управления информационной безопасностью (далее – система управления информационной безопасностью), являющейся частью общей системы управления страховой (перестраховочной) организацией, предназначенной для управления процессом обеспечения информационной безопасности.

4. Система управления информационной безопасностью обеспечивает защиту информационных активов страховой (перестраховочной) организации.

5. Страховая (перестраховочная) организация обеспечивает функционирование системы управления информационной безопасностью, ее развитие и улучшение.

6. Участниками системы управления информационной безопасностью страховой (перестраховочной) организации являются:

1) орган управления;

2) исполнительный орган;

3) подразделение по информационной безопасности;

4) подразделение по информационным технологиям;

5) подразделение по безопасности;

6) подразделение по работе с персоналом;

7) юридическое подразделение;

8) подразделение по комплаенс-контролю;

9) подразделение внутреннего аудита.

Допускается осуществление функций подразделений, указанных в подпунктах 3), 4) , 5), 6), 7), 8) и 9) настоящего пункта, ответственными лицами.

7. Страховая (перестраховочная) организация при создании и функционировании системы управления информационной безопасностью обеспечивает независимость подразделений по информационной безопасности и по информационным технологиям посредством их подчинения разным членам исполнительного органа страховой (перестраховочной) организации или напрямую руководителю исполнительного органа страховой (перестраховочной) организации.

8. Орган управления страховой (перестраховочной) организации утверждает политику информационной безопасности, которая определяет:

1) цели, задачи и основные принципы построения системы управления информационной безопасностью;

2) требования к организации доступа к создаваемой, хранимой и обрабатываемой информации в информационных системах страховой (перестраховочной) организации, мониторинга информации и доступа к ней;

3) требования к осуществлению сбора, консолидации и хранения информации об инцидентах информационной безопасности;

4) требования к осуществлению мониторинга деятельности по обеспечению информационной безопасности;

5) требования к проведению анализа информации об инцидентах информационной безопасности;

6) ответственность работников страховой (перестраховочной) организации за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей.

9. Орган управления страховой (перестраховочной) организации утверждает перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих тайну страхования, служебную, коммерческую или иную охраняемую законом тайну (далее – защищаемая информация), и порядок работы с защищаемой информацией.

10. Орган управления страховой (перестраховочной) организации осуществляет контроль за состоянием системы управления информационной безопасности страховой (перестраховочной) организации.

11. Исполнительный орган страховой (перестраховочной) организации утверждает внутренние документы страховой (перестраховочной) организации, регламентирующие процесс обеспечения информационной безопасности, порядок и периодичность пересмотра которых определяется внутренними документами страховой (перестраховочной) организации.

12. Подразделение по информационной безопасности в целях обеспечения конфиденциальности, целостности и доступности информации страховой (перестраховочной) организации осуществляет следующие функции:

1) организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности подразделений страховой (перестраховочной) организации по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

2) разрабатывает политику информационной безопасности страховой (перестраховочной) организации;

3) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности страховой (перестраховочной) организации;

4) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности страховой (перестраховочной) организации в рамках своих полномочий;

5) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;

6) осуществляет анализ информации об инцидентах информационной безопасности;

7) организует и проводит мероприятия по обеспечению осведомленности работников страховой (перестраховочной) организации в вопросах информационной безопасности;

8) осуществляет мониторинг состояния системы управления информационной безопасностью страховой (перестраховочной) организации;

9) осуществляет информирование руководства страховой (перестраховочной) организации о состоянии системы управления информационной безопасностью страховой (перестраховочной) организации.

13. Подразделение по информационным технологиям осуществляет следующие функции:

1) разрабатывает схемы информационной инфраструктуры страховой (перестраховочной) организации;

2) обеспечивает предоставление доступа работникам к информационным активам страховой (перестраховочной) организации;

3) обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности информационных систем страховой (перестраховочной) организации (включая резервирование и (или) архивирование) в соответствии с внутренними документами страховой (перестраховочной) организации;

4) обеспечивает соблюдение внутренних документов страховой (перестраховочной) организации, содержащих требования к информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем страховой (перестраховочной) организации.

14. Подразделение по безопасности осуществляет следующие функции:

1) реализует меры физической и технической безопасности в страховой (перестраховочной) организации, в том числе организует пропускной и внутриобъектовый режим;

2) проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз информационной безопасности при приеме на работу и увольнении работников страховой (перестраховочной) организации.

15. Подразделение по работе с персоналом осуществляет следующие функции:

1) обеспечивает подписание работниками страховой (перестраховочной) организации, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации;

2) участвует в организации процесса повышения осведомленности работников страховой (перестраховочной) организации в области информационной безопасности.

16. Юридическое подразделение осуществляет правовую экспертизу внутренних документов страховой (перестраховочной) организации по вопросам обеспечения информационной безопасности.

17. Подразделение по комплаенс-контролю совместно с юридическим подразделением страховой (перестраховочной) организации определяет виды информации, подлежащие включению в перечень защищаемой информации, предусмотренный пунктом 9 Требований.

18. Подразделение внутреннего аудита проводит оценку состояния системы управления информационной безопасностью в соответствии с внутренними документами страховой (перестраховочной) организации, регламентирующими организацию системы внутреннего аудита страховой (перестраховочной) организации.

19. Руководители подразделений страховой (перестраховочной) организации:

1) обеспечивают ознакомление работников с требованиями к информационной безопасности;

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

20. Работники подразделений страховой (перестраховочной) организации:

1) обеспечивают соблюдение требований к информационной безопасности, принятых в страховой (перестраховочной) организации;

2) извещают своего непосредственного руководителя и подразделение по информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными активами.

21. Предоставление физического доступа к информационным активам страховой (перестраховочной) организации осуществляется в соответствии с внутренними документами страховой (перестраховочной) организации.

22. Доступ к информации предоставляется работникам в объеме, необходимом для исполнения их функциональных обязанностей.

23. Доступ к информационным системам страховой (перестраховочной) организации осуществляется путем идентификации и аутентификации пользователей информационных систем страховой (перестраховочной) организации.

24. В информационных системах страховой (перестраховочной) организации используются только персонализированные учетные записи.

25. Использование технологических учетных записей допускается в соответствии с перечнем таких учетных записей для каждой информационной системы с указанием лиц, персонально ответственных за их использование и актуальность, утверждаемым руководителем подразделения по информационным технологиям по согласованию с руководителем подразделения по информационной безопасности.

26. В информационных системах страховой (перестраховочной) организации применяются функции или средства по управлению учетными записями и паролями, а также блокировке учетных записей, определяемые внутренними документами страховой (перестраховочной) организации.

27. Страховая (перестраховочная) организация осуществляет резервное хранение данных информационных систем страховой (перестраховочной) организации, их файлов и настроек, которое обеспечивает восстановление работоспособных копий информационных систем.

28. Порядок и периодичность резервного копирования, хранения, восстановления информации определяются внутренним документом страховой (перестраховочной) организации.

29. Страховая (перестраховочная) организация обеспечивает антивирусную защиту информационной инфраструктуры в соответствии с внутренними документами страховой (перестраховочной) организации.

30. В информационных системах страховой (перестраховочной) организации используется функция ведения аудиторского следа, которая отражает следующие события (успешные и неуспешные):

1) события установления соединений, идентификации и аутентификации в информационной системе страховой (перестраховочной) организации;

2) события модификации учетных записей и их полномочий;

3) события, отражающие установку обновлений и (или) изменений в информационной системе страховой (перестраховочной) организации;

4) события изменения параметров аудита;

5) события изменения системных параметров.

31. Срок хранения аудиторского следа составляет не менее 3 (трех) месяцев в информационных системах страховой (перестраховочной) организации и не менее 1 (одного) года в виде резервных копий аудиторского следа.

32. Подразделение по информационным технологиям отслеживает обновления информационных систем страховой (перестраховочной) организации и совместно с подразделением по информационной безопасности определяет порядок управления обновлениями информационных систем страховой (перестраховочной) организации.

33. Обновления информационных систем страховой (перестраховочной) организации до установки в промышленную среду проходят испытания в тестовой среде.

34. Порядок обеспечения физической безопасности центров обработки данных определяется внутренними документами страховой (перестраховочной) организации.

35. Страховой (перестраховочной) организацией определяется перечень программного обеспечения, разрешенного к использованию в страховой (перестраховочной) организации.

36. Центр обработки данных страховой (перестраховочной) организации оснащается следующими системами технической безопасности:

1) система контроля и управления доступом;

2) охранная сигнализация;

3) пожарная сигнализация;

4) система автоматического пожаротушения;

5) система поддержания заданных параметров микроклимата;

6) система видеонаблюдения;

7) система бесперебойного электропитания.

37. Доступ в центр обработки данных предоставляется лицам, перечень которых утверждается руководителем подразделения по информационным технологиям по согласованию с подразделением по информационной безопасности.

38. Запись событий ведется системой видеонаблюдения центра обработки данных непрерывно или с использованием детектора движения.

39. Архив системы видеонаблюдения центра обработки данных хранится не менее 3 (трех) месяцев.

40. Информация об инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности, подлежит консолидации, систематизации и хранению не менее 5 (пяти) лет.

41. Страховой (перестраховочной) организацией определяется порядок информирования о произошедшем инциденте информационной безопасности руководящих работников и подразделений страховой (перестраховочной) организации.

42. Страховой (перестраховочной) организацией определяется порядок принятия неотложных мер к устранению инцидента информационной безопасности, его причин и последствий.

43. В страховой (перестраховочной) организации ведется журнал учета инцидентов информационной безопасности на бумажном носителе либо в электронном виде, в который вносятся регистрационные данные заключения по результатам анализа инцидента информационной безопасности в соответствии с пунктом 46 Требования.

44. При сборе технических данных с программно-технических средств, вовлеченных в инцидент информационной безопасности, обеспечивается сохранность и неизменность собранных данных.

45. По результатам обработки инцидента информационной безопасности проводится анализ причин возникновения инцидента информационной безопасности, его механизма и последствий.

46. По результатам анализа инцидента информационной безопасности готовится заключение в произвольной форме, в котором отражаются вся информация об инциденте информационной безопасности, а также предложения по принятию корректирующих мер в целях снижения вероятности и возможного ущерба от повторного инцидента информационной безопасности.

47. В страховой (перестраховочной) организации внедряются организационные и технические меры, запрещающие работникам страховой (перестраховочной) организации самостоятельно проводить установку и настройку программного обеспечения.

48. В исключительных случаях отдельным группам пользователей предоставляется право самостоятельной установки и настройки программного обеспечения и оборудования. Этим группам пользователей предоставляются права локального администратора или аналогичные права.

49.Перечень пользователей, указанных в пункте 48 Требований, формируется, актуализируется и утверждается руководителем подразделения по информационным технологиям по согласованию с подразделением по информационной безопасности. В случае предоставления пользователям дополнительных прав в соответствии с пунктом 48 Требований подразделение по информационной безопасности осуществляет контроль их использования.

50. Страховая (перестраховочная) организация ежегодно, не позднее 10 января года, следующего за отчетным годом, представляет в уполномоченный орган информацию о состоянии системы управления информационной безопасностью.

51. Информация, указанная в пункте 50 Требований, включает сведения о:

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

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

3) наличии, материально-технической обеспеченности центров обработки данных;

4) проведенных мероприятиях по совершенствованию системы управления информационной безопасностью и информационных активов страховой (перестраховочной) организации либо их отсутствии.

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.

Сноска. Пункт 52 - в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 29.08.2024 № 73 (вводится в действие по истечении шестидесяти календарных дней после дня его первого официального опубликования).

53. Уполномоченный орган осуществляет проверку соответствия страховой (перестраховочной) организации Требованиям не реже одного раза в 3 (три) года.

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

Сноска. Требование дополнено главой 3 в соответствии с постановлением Правления Агентства РК по регулированию и развитию финансового рынка от 29.08.2024 № 73 (вводится в действие по истечении шестидесяти календарных дней после дня его первого официального опубликования).

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.