

**Об утверждении Правил оценки уровня защищенности от угроз информационной безопасности**

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 23 ноября 2020 года № 110. Зарегистрировано в Министерстве юстиции Республики Казахстан 27 ноября 2020 года № 21685.

      Настоящее постановление вводится в действие с 1 января 2021 года.

      В соответствии с подпунктом 1) 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 Правила оценки уровня защищенности от угроз 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 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 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 23 ноября 2020 года № 110 |

**Правила оценки уровня защищенности от угроз информационной безопасности**

**Глава 1. Общие положения**

      1. Настоящие Правила оценки уровня защищенности от угроз информационной безопасности (далее – Правила) разработаны в соответствии с Законом Республики Казахстан от 4 июля 2003 года "О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций" и определяют порядок оценки уровня защищенности от угроз информационной безопасности финансовых организаций и филиалов банков-нерезидентов Республики Казахстан, филиалов страховых (перестраховочных) организаций-нерезидентов Республики Казахстан, филиалов страховых брокеров-нерезидентов Республики Казахстан (далее – финансовые организации).

      2. В Правилах используются следующие понятия:

      1) ключевые информационные системы финансовой организации – информационные системы финансовой организации, необходимые для функционирования бизнес-процессов, реализующих основные направления деятельности финансовой организации;

      2) уполномоченный орган – государственный орган, осуществляющий государственное регулирование, контроль и надзор финансового рынка и финансовых организаций.

**Глава 2. Порядок оценки уровня защищенности от угроз**

      3. Оценка уровня защищенности от угроз информационной безопасности осуществляется финансовыми организациями по запросу уполномоченного органа.

      4. Оценка уровня защищенности от угроз информационной безопасности осуществляется финансовой организацией в соответствии с параметрами оценки уровня защищенности от угроз информационной безопасности согласно приложению к Правилам.

      По каждому параметру, указанному в столбце 2 приложения к Правилам, финансовая организация определяет один из указанных в столбцах 3, 4, 5 приложения к Правилам уровней защищенности.

      5. Оценка уровня защищенности от угроз информационной безопасности оформляется финансовой организацией в виде таблицы с указанием параметров оценки уровня защищенности от угроз информационной безопасности, перечисленных в столбце 2 приложения к Правилам, уровня защищенности и краткого описания их исполнения.

      6. Результат оценки уровня защищенности от угроз информационной безопасности утверждается руководителем финансовой организации и предоставляется финансовой организацией сопроводительным письмом в уполномоченный орган в срок, не превышающий трех месяцев со дня получения запроса уполномоченного органа на проведение такой оценки.

      7. К результатам оценки уровня защищенности от угроз информационной безопасности финансовой организацией прилагаются документы, подтверждающие уровни защищенности 2 и 3 согласно приложению к Правилам.

      8. Уполномоченный орган проверяет предоставленные финансовой организацией результаты оценки уровня защищенности от угроз информационной безопасности на соответствие приложенным документам и определяет итоговый уровень защищенности финансовой организации по каждому из параметров оценки уровня защищенности от угроз информационной безопасности согласно приложению к Правилам.

      9. Итоговые результаты оценки уровня защищенности финансовой организации от угроз информационной безопасности доводятся уполномоченным органом до сведения финансовой организации.

|  |  |
| --- | --- |
|  | Приложение  к Правилам оценки уровня  защищенности от угроз  информационной безопасности |

**Параметры оценки уровня защищенности от угроз информационной безопасности**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Параметр оценки уровня защищенности от угроз информационной безопасности | Уровень защищенности 1 | Уровень защищенности 2 | Уровень защищенности 3 |
| 1 | 2 | 3 | 4 | 5 |
| 1. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации, а также сторонних организаций документ, содержащий описание политики информационной безопасности. | Отсутствует документ, содержащий описание политики информационной безопасности. | В наличии утвержденный документ, содержащий описание политики информационной безопасности. | В наличии утвержденный документ, содержащий описание политики информационной безопасности, и доведенный до сведения всех работников, а также сторонних организаций. |
| 2. | Финансовой организацией осуществляется анализ и пересмотр документа, содержащего описание политики информационной безопасности, через заданные промежутки времени или при возникновении существенных изменений. | Периодичность пересмотра документа, содержащего описание политики информационной безопасности, не утверждена. | Периодичность пересмотра документа, содержащего описание политики информационной безопасности, утверждена, нет документальных свидетельств пересмотра в утвержденный срок. | Периодичность пересмотра документа, содержащего описание политики информационной безопасности, утверждена, есть документальные свидетельства пересмотра в утвержденный срок. |
| 3. | Финансовой организацией утвержден документ, определяющий обязанности работников и руководства финансовой организации по обеспечению информационной безопасности. | Отсутствует документ, определяющий обязанности руководителей и работников по обеспечению информационной безопасности. | В наличии утвержденный документ, определяющий обязанности работников по обеспечению информационной безопасности. | В наличии утвержденный документ, определяющий обязанности руководителей и работников по обеспечению информационной безопасности. |
| 4. | Финансовой организацией утверждено соглашение о неразглашении информации, которое подписано всеми работниками финансовой организации, имеющими доступ к конфиденциальной информации. | Отсутствует соглашение о неразглашении информации. | В наличии утвержденное соглашение о неразглашении информации, но оно не подписано всеми работниками, имеющими доступ к конфиденциальной информации. | В наличии утвержденное соглашение о неразглашении информации, которое подписано всеми работниками, имеющими доступ к конфиденциальной информации. |
| 5. | Финансовой организацией утверждены процедуры, определяющие перечень лиц и порядок их взаимодействия с компетентными органами (например, правоохранительными органами, пожарными службами, уполномоченным органом). | Отсутствуют процедуры, определяющие взаимодействие работников с компетентными органами. | - | В наличии задокументированные и утвержденные процедуры, определяющие взаимодействие работников с компетентными органами. |
| 6. | Финансовой организацией поддерживается взаимодействие ее работников по информационной безопасности с профессиональными группами, ассоциациями и принятие ими участия в конференциях (форумах) по информационной безопасности. | Отсутствует взаимодействие работников по информационной безопасности финансовой организации с профессиональными группами, ассоциациями и принятие участия в конференциях (форумах) по информационной безопасности. | Отсутствует утвержденный документ, определяющий порядок взаимодействия работников по информационной безопасности финансовой организации с профессиональными группами, ассоциациями и принятие участия в конференциях (форумах) по информационной безопасности, работники по информационной безопасности осуществляют взаимодействие по собственной инициативе. | В наличии утвержденный документ, определяющий порядок взаимодействия работников по информационной безопасности финансовой организации с профессиональными группами, ассоциациями и принятие участия в конференциях (форумах) по информационной безопасности, работники по информационной безопасности состоят в профессиональных группах, ассоциациях и ежегодно принимают участие в конференциях (форумах) по информационной безопасности. |
| 7. | Финансовая организация подвергает внешнему аудиту процессы обеспечения информационной безопасности ключевых информационных систем через определенные промежутки времени. | Внешний аудит информационной безопасности ключевых информационных систем не проводился в течение последних трех лет. | В течение последних трех лет проводился внешний аудит обеспечения информационной безопасности более половины из всех ключевых информационных систем. | В течение последних трех лет проводился внешний аудит обеспечения информационной безопасности всех ключевых информационных систем. |
| 8. | Финансовой организацией результаты внешнего аудита обеспечения информационной безопасности ключевых информационных систем используются для улучшения обеспечения информационной безопасности. | Внешний аудит информационной безопасности ключевых информационных систем не проводится. | - | По результатам последнего внешнего аудита обеспечения информационной безопасности ключевых информационных систем реализованы мероприятия по улучшению обеспечения информационной безопасности. |
| 9. | Финансовая организация контролирует доступ третьих лиц к своим средствам обработки информации. | Доступ третьих лиц к средствам обработки информации финансовой организации не контролируется. | В наличии утвержденный документ, определяющий обеспечение информационной безопасности при предоставлении доступа третьим лицам к средствам обработки информации. | При предоставлении доступа третьим лицам к средствам обработки информации осуществляется анализ рисков информационной безопасности и разрабатываются мероприятия по снижению выявленных рисков. |
| 10. | Финансовой организацией определены меры информационной безопасности при предоставлении клиентам доступа к информационным системам финансовой организации. | Меры информационной безопасности при предоставлении клиентам доступа к информационным системам финансовой организации не определены. | В наличии утвержденный документ, определяющий меры информационной безопасности при предоставлении клиентам доступа к информационным системам финансовой организации. | - |
| 11. | Соглашения финансовой организации со сторонними организациями, имеющими доступ к информации или информационным активам финансовой организации, содержат требования по информационной безопасности. | Соглашения со сторонними организациями, имеющими доступ к информации или информационным активам финансовой организации, не содержат требования по информационной безопасности. | Отдельные соглашения со сторонними организациями, имеющими доступ к информации или информационным активам финансовой организации, содержат требования по информационной безопасности. | Все действующие соглашения со сторонними организациями, имеющими доступ к информации или информационным активам финансовой организации, содержат стандартизированные требования по информационной безопасности, определенные внутренним документом. |
| 12. | Финансовой организацией утвержден документ, содержащий перечень ключевых информационных систем финансовой организации с указанием владельцев. | Отсутствует документ, содержащий перечень ключевых информационных систем финансовой организации. | - | В наличии утвержденный или актуализированный в течение последнего года документ, включающий перечень ключевых информационных систем финансовой организации с указанием владельцев. |
| 13. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации документ, содержащий правила использования электронной почты. | Отсутствует документ, содержащий правила использования электронной почты. | - | В наличии утвержденный документ, содержащий правила использования электронной почты, доведенный до сведения всех работников финансовой организации. |
| 14. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации документ, содержащий правила использования сети Интернет. | Отсутствует документ, содержащий правила использования сети Интернет. | - | В наличии утвержденный документ, содержащий правила использования сети Интернет, доведенный до сведения всех работников финансовой организации. |
| 15. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации документ, содержащий перечень защищаемой информации. | Отсутствует документ, содержащий перечень защищаемой информации. | - | В наличии утвержденный документ, содержащий перечень защищаемой информации, доведенный до сведения всех работников финансовой организации. |
| 16. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации документ, содержащий перечень персональных данных. | Отсутствует документ, содержащий перечень персональных данных. | - | В наличии утвержденный документ, содержащий перечень персональных данных, доведенный до сведения всех работников финансовой организации. |
| 17. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации документ, содержащий правила классификации информации с указанием перечня классов информации, принципов отнесения информации к определенному классу, определением ответственности работников по классификации информации. | Отсутствует документ, содержащий правила классификации информации. | - | В наличии утвержденный документ, содержащий правила классификации информации, доведенный до сведения всех работников финансовой организации. |
| 18. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации документ, содержащий правила маркировки носителей информации. | Отсутствует документ, содержащий правила маркировки носителей информации. | - | В наличии утвержденный документ, содержащий правила маркировки носителей информации, доведенный до сведения всех работников финансовой организации. |
| 19. | Финансовой организацией утвержден документ, определяющий роли и функции подразделений или работников финансовой организации в процессах обеспечения информационной безопасности. | Отсутствует документ, определяющий роли и функции подразделений или работников финансовой организации в процессах обеспечения информационной безопасности. | В наличии утвержденный документ, определяющий функции подразделения по информационной безопасности или работника по информационной безопасности финансовой организации. | В наличии утвержденный документ, определяющий роли и функции в процессах обеспечения информационной безопасности подразделения по информационной безопасности и других подразделений или работников финансовой организации. |
| 20. | Финансовой организацией в трудовых договорах с работниками предусмотрена ответственность работников за несоблюдение требований информационной безопасности, включая ответственность после увольнения из финансовой организации. | В трудовых договорах с работниками ответственность работников за несоблюдение требований информационной безопасности не предусмотрена. | - | В трудовых договорах с работниками предусмотрена ответственность работников за несоблюдение требований информационной безопасности. |
| 21. | Работники финансовой организации проходят обучение или переподготовку в целях регулярного получения информации о требованиях правил и процедур по информационной безопасности в финансовой организации. | Обучение работников о требованиях правил и процедур по информационной безопасности не проводится. | Обучение работников о требованиях правил и процедур по информационной безопасности проводится нерегулярно (менее чем 1 раз в полгода за последние 3 года). | Обучение работников о требованиях правил и процедур по информационной безопасности проводится регулярно (не менее чем 1 раз в полгода за последние 3 года). |
| 22. | Финансовой организацией утвержден документ, определяющий дисциплинарную ответственность за нарушение правил и процедур по информационной безопасности. | Отсутствует документ, определяющий дисциплинарную ответственность за нарушение правил и процедур по информационной безопасности. | В наличии утвержденный документ, в котором определена дисциплинарная ответственность за нарушение правил и процедур по информационной безопасности. | - |
| 23. | Финансовой организацией обеспечивается контроль возврата работниками при увольнении активов финансовой организации, находящихся в их пользовании. | Процесс контроля возврата активов финансовой организации при увольнении работников отсутствует. | Процесс контроля возврата активов финансовой организации при увольнении работников осуществляется в ручном режиме. | Процесс контроля возврата активов финансовой организации при увольнении работников частично или полностью автоматизирован. |
| 24. | Финансовой организацией обеспечивается аннулирование доступа работников к средствам обработки информации при увольнении. | Процесс аннулирования доступа работников к средствам обработки информации при увольнении отсутствует. | Процесс аннулирования доступа работников к средствам обработки информации при увольнении осуществляется в ручном режиме. | Процесс аннулирования доступа работников к средствам обработки информации при увольнении частично или полностью автоматизирован. |
| 25. | В финансовой организации физический доступ к средствам обработки информации предоставляется только авторизованным работникам. | Процесс ограничения физического доступа к средствам обработки информации отсутствует. | Процесс ограничения физического доступа к средствам обработки информации осуществляется в ручном режиме. | Процесс ограничения физического доступа к средствам обработки информации частично или полностью автоматизирован. |
| 26. | В финансовой организации серверное оборудование располагается в выделенных помещениях с обеспечением микроклимата, рекомендованного производителем оборудования. | Серверное оборудование располагается в рабочих кабинетах работников. | Серверное оборудование располагается в отдельных помещениях, где поддерживается микроклимат. Мониторинг микроклимата не осуществляется. | Серверное оборудование располагается в отдельных помещениях, где поддерживается микроклимат. Осуществляется мониторинг микроклимата с оповещением ответственных работников. |
| 27. | В финансовой организации серверное оборудование обеспечивается бесперебойным, защищенным от помех питанием. | Отсутствует защита от помех и резервное питание серверного оборудования. | В наличии имеется защита от помех и резервное питание до 1-го часа для серверного оборудования. | В наличии имеется защита от помех и резервное питание более 1-го часа для серверного оборудования. |
| 28. | Финансовой организацией осуществляется защита каналов связи, выходящих за пределы физического периметра безопасности. | Защита каналов связи не осуществляется. | Осуществляется шифрование каналов связи между стационарными офисами и устройствами финансовой организации. | Осуществляется шифрование каналов связи между стационарными офисами и устройствами финансовой организации, а также каналов связи с мобильными устройствами финансовой организации. |
| 29. | Финансовой организацией осуществляется уничтожение информации с носителей перед повторным их использованием. | Уничтожение информации с носителей не регламентировано и не осуществляется. | Уничтожение информации с носителей регламентировано и осуществляется штатными средствами операционных систем. | Уничтожение информации с носителей регламентировано и осуществляется специализированными средствами гарантированного уничтожения информации. |
| 30. | Финансовой организацией осуществляется контроль перемещения оборудования через границу физического периметра безопасности. | Контроль перемещения оборудования через границу физического периметра безопасности не регламентирован и не осуществляется. | Контроль перемещения оборудования через границу физического периметра безопасности регламентирован и осуществляется в ручном режиме. | Контроль перемещения оборудования через границу физического периметра безопасности регламентирован и автоматизирован частично или полностью. |
| 31. | Финансовой организацией определены правила управления изменениями в ключевых информационных системах. | Правила управления изменениями в ключевых информационных системах не определены. | Правила управления изменениями в ключевых информационных системах определены, процесс управления изменениями осуществляется в ручном режиме. | Правила управления изменениями в ключевых информационных системах определены, процесс управления изменениями частично или полностью автоматизирован. |
| 32. | Финансовой организацией используются раздельные среды для разработки, тестирования и промышленной эксплуатации ключевых информационных систем. | Среды разработки, тестирования и промышленной эксплуатации ключевых информационных систем не разделены. | Разделены среды тестирования и промышленной эксплуатации ключевых информационных систем. | Разделены среды разработки, тестирования и промышленной эксплуатации ключевых информационных систем. |
| 33. | В финансовой организации работники, осуществляющие разработку изменений для ключевых информационных систем, не осуществляют их внедрение в промышленную среду. | Работники совмещают обязанности по разработке и внедрению изменений в ключевые информационные системы. | Обязанности по разработке и внедрению изменений в ключевые информационные системы разделены между работниками, доступ разработчиков к промышленной среде не ограничен. | Обязанности по разработке и внедрению изменений в ключевые информационные системы разделены между работниками, доступ разработчиков к промышленной среде закрыт. |
| 34. | Финансовой организацией осуществляется установка и регулярное обновление программного обеспечения, выявляющего вредоносный программный код, а также проверка компьютеров и носителей информации на наличие вредоносного программного кода. | Выявляющее вредоносный программный код программное обеспечение не установлено на всех компьютерах. | Выявляющее вредоносный программный код программное обеспечение установлено на всех компьютерах, не осуществляется регулярное обновление или сканирование на наличие вредоносного программного кода компьютеров и носителей информации. | Выявляющее вредоносный программный код программное обеспечение установлено на всех компьютерах, осуществляется регулярное обновление и сканирование на наличие вредоносного программного кода компьютеров и носителей информации. |
| 35. | Финансовой организацией регламентированы и осуществляются процессы по созданию, проверке и тестированию на регулярной основе резервных копий информации и программного обеспечения ключевых информационных систем. | Резервные копии информации и программного обеспечения ключевых информационных систем не создаются. | Создание резервных копий информации и программного обеспечения ключевых информационных систем регламентировано и осуществляется в соответствии с утвержденным регламентом. Тестирование резервных копий не осуществляется. | Создание и тестирование резервных копий информации и программного обеспечения ключевых информационных систем регламентировано и осуществляется в соответствии с утвержденным регламентом. |
| 36. | Финансовой организацией осуществляется ведение и хранение журналов аудита ключевых информационных систем, регистрирующих действия пользователей, нештатные ситуации и события информационной безопасности, для использования в будущих расследованиях и проведении мониторинга контроля доступа. | Ведение журналов аудита ключевых информационных систем не регламентировано, журналы аудита ведутся с настройками "по умолчанию" или не ведутся. | - | Ведение, настройки и хранение журналов аудита ключевых информационных систем описаны во внутренних утвержденных документах, журналы аудита настроены, ведутся и хранятся в соответствии с утвержденными документами. |
| 37. | Финансовой организацией обеспечивается регистрация и регулярный анализ действий привилегированных пользователей в ключевых информационных системах. | Действия привилегированных пользователей в ключевых информационных системах не регистрируются. | Действия привилегированных пользователей в ключевых информационных системах регистрируются, но не анализируются на периодической основе. | Действия привилегированных пользователей в ключевых информационных системах регистрируются и анализируются на периодической основе. |
| 38. | Финансовой организацией синхронизируется с помощью единого источника точного времени системное время ключевых информационных систем. | Системное время ключевых информационных систем в пределах финансовой организации не синхронизируется. | - | Системное время ключевых информационных систем в пределах финансовой организации синхронизируется с помощью единого источника точного времени. |
| 39. | В финансовой организации доступ пользователей в ключевые информационные системы осуществляется по уникальным персональным идентификаторам. | Для доступа в одну или более ключевые информационные системы не требуется уникального персонального идентификатора. | - | Доступ во все ключевые информационные системы осуществляется по уникальным персональным идентификаторам. |
| 40. | Финансовой организацией используется функционал разграничения уровней доступа пользователей в ключевых информационных системах. | Разграничение уровней доступа пользователей используется не во всех ключевых информационных системах. | - | Разграничение уровней доступа пользователей используется во всех ключевых информационных системах. |
| 41. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации документ, содержащий правила управления паролями пользователей в ключевых информационных системах. | Отсутствует документ, содержащий правила управления паролями пользователей в ключевых информационных системах. | - | В наличии утвержденный документ, содержащий правила управления паролями пользователей в ключевых информационных системах, доведенный до всех работников финансовой организации. |
| 42. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации документ, содержащий правила периодического пересмотра действующих прав доступа пользователей в ключевые информационные системы. | Отсутствует документ, содержащий правила периодического пересмотра действующих прав доступа пользователей в ключевых информационных системах. | - | В наличии утвержденный документ, содержащий правила периодического пересмотра действующих прав доступа пользователей в ключевых информационных системах. |
| 43. | Финансовой организацией используется двух- или многофакторная аутентификация для подключения пользователей извне физического периметра безопасности. | Для подключения пользователей извне физического периметра безопасности используется один фактор для аутентификации. | - | Для подключения пользователей извне физического периметра безопасности используется двух- или многофакторная аутентификация. |
| 44. | Информационная сеть финансовой организации разграничена на группы (VLAN). | Разграничение информационной сети финансовой организации на группы не предусмотрено. | Информационная сеть финансовой организации разграничена на группы по функциональному признаку средств обработки информации. | Информационная сеть финансовой организации разграничена на группы на основе классификации обрабатываемой информации. |
| 45. | Финансовой организацией используется функционал автоматизированного управления паролями в ключевых информационных системах. | Функционал автоматизированного управления паролями в ключевых информационных системах не используется. | В ключевых информационных системах используется функционал самостоятельной смены паролей пользователями, контроля периодической смены пароля. | В ключевых информационных системах используется функционал самостоятельной смены паролей пользователями, контроля периодической смены пароля, контроля сложности пароля, контроля повторения предыдущих паролей. |
| 46. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации документ, содержащий правила работы в дистанционном режиме. | Отсутствует документ, содержащий правила работы в дистанционном режиме. | - | В наличии утвержденный документ, содержащий правила работы в дистанционном режиме, доведенный до сведения всех работников финансовой организации. |
| 47. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации документ, содержащий правила использования средств криптографической защиты информации. | Отсутствует документ, содержащий правила использования средств криптографической защиты информации. | - | В наличии утвержденный документ, содержащий правила использования средств криптографической защиты информации, доведенный до сведения всех работников финансовой организации, имеющих доступ к средствам криптографической защиты информации. |
| 48. | Финансовой организацией утвержден и доведен до сведения всех работников финансовой организации документ, содержащий правила управления криптографическими ключами. | Отсутствует документ, содержащий правила управления криптографическими ключами. | - | В наличии утвержденный документ, содержащий правила управления криптографическими ключами. |
| 49. | Финансовой организацией обеспечивается контроль доступа к исходным кодам ключевых информационных систем. | Доступ к исходным кодам ключевых информационных систем не ограничен. | Доступ к исходным кодам ключевых информационных систем предоставлен только разработчикам. | Доступ к исходным кодам ключевых информационных систем предоставлен только разработчикам, информация обо всех изменениях в исходных кодах автоматически записывается в журнал. |
| 50. | Финансовой организацией осуществляется анализ информации о технических уязвимостях ключевых информационных систем, оценка опасности таких уязвимостей и принятие мер по их устранению. | Анализ информации о технических уязвимостях ключевых информационных систем не осуществляется. | - | Осуществляется периодический анализ информации о технических уязвимостях ключевых информационных систем, оценка опасности таких уязвимостей и принимаются меры по их устранению. |
| 51. | Работники финансовой организации оповещены о необходимости незамедлительного уведомления о любых замеченных или предполагаемых нарушениях информационной безопасности. | Отсутствует процесс оповещения работников о необходимости уведомлять о нарушениях информационной безопасности. | Работники периодически оповещаются о необходимости уведомлять о нарушениях информационной безопасности. | Работники периодически оповещаются о необходимости уведомлять о нарушениях информационной безопасности, проводятся периодические проверки действий работников при обнаружении нарушений информационной безопасности. |
| 52. | Финансовой организацией утвержден документ, содержащий процедуры реагирования на инциденты информационной безопасности. | Отсутствует документ, содержащий процедуры реагирования на инциденты информационной безопасности. | - | В наличии утвержденный документ, содержащий процедуры реагирования на инциденты информационной безопасности. |
| 53. | Финансовой организацией ведется регистрация инцидентов информационной безопасности и их последующий анализ. | Регистрация инцидентов информационной безопасности не ведется. | Ведется регистрация инцидентов информационной безопасности, анализ в течение прошедшего года не осуществлялся. | Ведется регистрация инцидентов информационной безопасности, результаты анализа за прошедший год зафиксированы документально. |
| 54. | Финансовой организацией обеспечивается регулярное тестирование на проникновение информационной инфраструктуры. | Тестирование на проникновение информационной инфраструктуры финансовой организации не осуществляется. | Тестирование на проникновение информационной инфраструктуры финансовой организации осуществляется менее одного раза в год. | Тестирование на проникновение информационной инфраструктуры финансовой организации осуществляется не менее одного раза в год. |
| 55. | Финансовой организацией регулярно осуществляется анализ на уязвимости исходных кодов ключевых информационных системы при наличии доступа к таким исходным кодам. | Анализ исходных кодов ключевых информационных систем на уязвимости не осуществляется. | Анализ исходных кодов ключевых информационных систем на уязвимости осуществляется выборочно, не по каждому изменению в промышленной среде. | Анализ исходных кодов ключевых информационных систем на уязвимости осуществляется перед каждым изменением в промышленной среде. |

© 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан» Министерства юстиции Республики Казахстан