e.zan
Қазақстан Республикасының электронды нысандағы нормативтік құқықтық актілердің эталонды бақылау банкі
Эталонный контрольный банк нормативных правовых актов Республики Казахстан в электронном виде

Редакциялау күні 17.10.2023
Сақтау күні 29.03.2024
Дата редакции 17.10.2023
Дата скачивания 29.03.2024

Қазақстан Республикасының Ұлттық Банкі

Постановление Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48. Зарегистрировано в Министерстве юстиции Республики Казахстан 18 апреля 2018 года № 16772

Национальный Банк Республики Казахстан

Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах

Сноска. Заголовок в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 17.02.2021 № 34 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

В соответствии с пунктом 7 статьи 61-5 Закона Республики Казахстан от 31 августа 1995 года «О банках и банковской деятельности в Республике Казахстан» Правление Национального Банка Республики Казахстан **ПОСТАНОВЛЯЕТ**:

Сноска. Преамбула в редакции постановления Правления Национального Банка РК от 19.11.2019 № 203 (вводится в действие с 01.01.2020).

1. Утвердить:

1) Требования к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, согласно приложению 1 к настоящему постановлению;

QR-код содержит данные ЭЦП должностного лица РГП на ПХВ «ИЗПИ»

QR-код содержит ссылку на данный документ в ЭКБ НПА РК

2) Правила и сроки предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах, согласно приложению 2 к настоящему постановлению.

Сноска. Пункт 1 с изменением, внесенным постановлением Правления Агентства РК по регулированию и развитию финансового рынка от 17.02.2021 № 34 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

2. Признать утратившим силу постановление Правления Национального Банка Республики Казахстан от 31 марта 2001 года № 80 «Об утверждении Правил по обеспечению безопасности информационных систем банков второго уровня и организаций, осуществляющих отдельные виды банковских операций (зарегистрированное в Реестре государственной регистрации нормативных правовых актов под № 1517).

3. Управлению информационных угроз и киберзащиты (Перминов Р.В.) 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 4 настоящего постановления.

4. 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.

5. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Национального Банка Республики Казахстан Смолякова О.А.

6. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования, за исключением подпункта 1) пункта 1 и пункта 2 настоящего постановления, которые вводятся в действие с 1 декабря 2018 года.

Председатель Национального Банка **Д. Акишев**

e.zan
Қазақстан Республикасының электронды нысандағы нормативтік құқықтық актілердің эталонды бақылау банкі
Эталонный контрольный банк нормативных правовых актов Республики Казахстан в электронном виде
Редакциялау күні 17.10.2023
Сақтау күні 29.03.2024
Дата редакции 17.10.2023
Дата скачивания 29.03.2024

Приложение 1
к постановлению Правления
Национального Банка
Республики Казахстан
от 27 марта 2018 года
№ 48

Требования к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций

Сноска. Требования в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 29.04.2022 № 30 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Глава 1. Общие положения

1. Настоящие Требования к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковский операций (далее – Требования), разработаны в соответствии с пунктом 7 статьи 61-5 Закона Республики Казахстан «О банках и банковской деятельности в Республике Казахстан» и устанавливают требования к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан (далее – банк) и организаций, осуществляющих отдельные виды банковских операций (далее – организация).

2. В Требованиях используются понятия, предусмотренные Законом Республики Казахстан «Об информатизации», а также следующие понятия:

1) информационная безопасность в сфере информатизации (далее – информационная безопасность) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

2) штатный носитель информации – носитель информации, являющийся составной частью объекта информационно-коммуникационной инфраструктуры и подключенный к нему на постоянной основе;

3) информационный актив – совокупность информации и объекта информационно-коммуникационной инфраструктуры, используемого для ее хранения и (или) обработки;

4) ИТ-менеджер информационной системы/актива – работник или подразделение (работники или подразделения) банка, организации ответственные за поддержание информационной системы/актива в состоянии, соответствующем требованиям бизнес-владельца информационной системы/актива;

5) бизнес-владелец информационной системы или подсистемы – подразделение (работник) банка, организации, являющееся (являющийся) владельцем основного бизнес-процесса, который автоматизирует информационная система или подсистема;

6) 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;

7) периметр защиты информационно-коммуникационной инфраструктуры – совокупность программно-аппаратных средств, отделяющих информационно-коммуникационную инфраструктуру банка, организации от внешних информационных сетей и реализующих защиту от угроз информационной безопасности;

8) угроза информационной безопасности – совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

9) риск информационной безопасности — вероятное возникновение ущерба вследствие нарушения конфиденциальности, преднамеренного нарушения целостности или доступности информационных активов банка, организации;

10) обеспечение информационной безопасности – процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов банка, организации;

11) информация об инцидентах информационной безопасности – информация об отдельно или серийно возникающих сбоях в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающих угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;

12) инцидент информационной безопасности – отдельно или серийно возникающие сбои в работе информационно-коммуникационной 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;

13) предустановленные учетные записи – учетные записи информационных систем, установленные их производителями;

14) привилегированная учетная запись – учетная запись в информационной системе, обладающая привилегиями создания, удаления и изменения прав доступа учетных записей;

15) консоль администрирования и мониторинга – рабочая станция, позволяющая осуществлять удаленное управление информационной системой;

16) бизнес-процесс – совокупность взаимосвязанных мероприятий или задач, направленных на создание определенного продукта или услуги для внешнего или внутреннего потребителя;

17) владелец бизнес-процесса – подразделение (работник) банка, организации, отвечающее (отвечающий) за жизненный цикл бизнес-процесса и координацию деятельности подразделений банка, организации, вовлеченных в бизнес-процесс;

18) виртуальная среда – вычислительные ресурсы или их логическое объединение, абстрагированное от аппаратной реализации, и обеспечивающее при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе;

19) гипервизор – программное или аппаратно-программное обеспечение, позволяющее создавать и запускать одновременно несколько операционных систем на одном и том же сервере или компьютере;

20) протокол передачи данных – набор правил и действий, позволяющий осуществлять соединение и обмен данными между двумя и более включенными в сеть устройствами;

21) центр обработки данных – специально выделенное помещение, в котором размещены серверы, обеспечивающие работу информационных систем банка, организации;

22) межсетевой экран – элемент информационной инфраструктуры, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами;

23) рабочая станция – стационарный персональный компьютер пользователя информационного актива банка, организации;

24) доступ – возможность использования информационных активов банка, организации;

25) групповые политики безопасности – реализованные средствами информационных систем типовые наборы правил информационной безопасности;

26) приложение – прикладное программное обеспечение пользователя информационной системы;

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

28) сигнатуры – набор данных, идентифицирующих программный код;

29) обеспечение технической безопасности – процесс обеспечения безопасности банка, организации с использованием технических средств (системы охранной и пожарной сигнализации, контроля и управления доступом,

видеонаблюдения, пожаротушения, контроля температурного режима и влажности в центре обработки данных);

30) технологическая учетная запись – учетная запись в информационной системе, предназначенная для аутентификации при взаимодействии информационных систем;

31) корректирующая мера – набор организационных и технических мероприятий, направленных на исправление существующей проблемы в процессе обеспечения информационной безопасности либо последствий ее нарушения;

32) уполномоченный орган – уполномоченный орган по регулированию, контролю и надзору финансового рынка и финансовых организаций.

3. К обеспечению информационной безопасности банков, организаций предъявляются следующие требования:

1) требования к организации системы управления информационной безопасностью;

2) требования к категорированию информационных активов банка, организации;

3) требования к организации доступа к информационным активам банка, организации;

4) требования к обеспечению безопасности информационной инфраструктуры;

5) требования к средствам криптографической защиты информации;

6) требования к обеспечению информационной безопасности при доступе третьих лиц к информационным активам банка, организации;

7) требования к проведению внутренних проверок состояния информационной безопасности;

8) требования к процессам системы управления информационной безопасностью.

Глава 2. Требования к организации системы управления информационной безопасностью

4. Первый руководитель банка, организации обеспечивает создание, функционирование и улучшение системы управления информационной безопасностью, являющейся частью общей системы управления банка, организации, предназначенной для управления процессом обеспечения информационной безопасности.

5. Система управления информационной безопасностью обеспечивает защиту информационных активов банка, организации, предусматривающую минимальный уровень потенциального ущерба для бизнес-процессов банка, организации.

6. Банк, организация обеспечивают надлежащий уровень системы управления информационной безопасностью, ее развитие и улучшение.

7. Участниками системы управления информационной безопасностью банка, организации являются:

1) орган управления;

2) исполнительный орган;

3) коллегиальный орган, уполномоченный принимать решения по задачам обеспечения информационной безопасности (далее – коллегиальный орган);

4) подразделение по информационной безопасности;

5) подразделение по информационным технологиям;

6) подразделение по безопасности;

7) подразделение по работе с персоналом;

8) юридическое подразделение;

9) подразделение по комплаенс-контролю;

10) подразделение внутреннего аудита;

11) подразделение по управлению рисками информационной безопасности.

Функции подразделений, указанные в подпунктах 4), 5), 6), 7), 8), 9), 10) и 11) части первой настоящего пункта, в организации осуществляются подразделениями, указанными в части первой настоящего пункта, либо ответственными работниками организации.

8. Банк, организация при создании и функционировании системы управления информационной безопасностью обеспечивают независимость подразделения по информационной безопасности и подразделения по информационным технологиям посредством их подчинения разным членам исполнительного органа банка, организации или напрямую руководителю исполнительного органа банка, организации.

9. Орган управления банка, организации утверждает политику информационной безопасности, которая определяет:

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

2) область действия системы управления информационной безопасностью;

3) требования к управлению доступом к создаваемой, хранимой и обрабатываемой информации в информационных активах банка, организации;

4) требования к осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

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

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

7) ответственность работников банка, организации за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей.

10. Орган управления банка, организации при формировании бюджета учитывает потребности в ресурсах для обеспечения информационной безопасности банка, организации.

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

12. Исполнительный орган банка, организации утверждает внутренние документы, регламентирующие процесс управления информационной безопасностью, порядок и периодичность пересмотра которых определяется внутренними документами банка, организации.

13. Банк, организация создают коллегиальный орган, в состав которого входят представители подразделения по информационной безопасности, подразделения по управлению рисками информационной безопасности, подразделения по информационным технологиям, а также по решению руководителя коллегиального органа банка, организации представители иных подразделений банка, организации или возлагают на исполнительный орган функции коллегиального органа при соответствии исполнительного органа требованиям к составу коллегиального органа, указанным в настоящем пункте.

В случае создания в банке, организации коллегиального органа руководителем коллегиального органа банка, организации назначается руководитель исполнительного органа банка, организации либо член исполнительного органа банка, организации, курирующий деятельность подразделения по информационной безопасности.

14. Подразделение по информационной безопасности в целях обеспечения конфиденциальности, целостности и доступности информации банка, организации осуществляет следующие функции:

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

2) разрабатывает политику информационной безопасности банка, организации;

3) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности банка, организации;

4) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности банка, 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) подготавливает предложения для принятия коллегиальным органом решений по вопросам информационной безопасности;

8) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности банка, организации, а также предоставление доступа к ним;

9) определяет требования информационной безопасности по использованию привилегированных учетных записей;

10) обеспечивает проведение мероприятий по повышению осведомленности работников банка, организации в области информационной безопасности;

11) осуществляет мониторинг состояния системы управления информационной безопасностью банка, организации;

12) осуществляет информирование руководства банка, организации о состоянии системы управления информационной безопасностью банка, организации.

15. Банк, организация определяют возможность возложения на подразделение по информационной безопасности функций по обеспечению технической безопасности. Подразделение по информационной безопасности не осуществляет функции, влекущие конфликт интересов с их основными функциями.

16. Подразделение по информационным технологиям осуществляет следующие функции:

1) разрабатывает и поддерживает актуальность схемы информационной инфраструктуры банка, организации;

2) обеспечивает предоставление доступа работникам банка, организации, использующим информационные активы банка, организации (далее – пользователь) к информационным активам банка, организации, за исключением специализированных информационных активов, доступ к которым

предоставляется ИТ-менеджерами информационных систем, не относящимися к подразделению по информационным технологиям;

3) обеспечивает формирование типовых настроек и конфигурирование системного и прикладного программного обеспечения банка, организации с учетом требований информационной безопасности;

4) обеспечивает исполнение требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности данных информационных систем банка, организации (включая резервирование и (или) архивирование и резервное копирование информации) в соответствии с внутренними документами банка, организации;

5) обеспечивает соблюдение требований информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем.

17. Банк, организация определяют возможность делегирования подразделениям банка, организации отдельных функций, указанных в пунктах 14 и 16 Требований.

18. Подразделение по безопасности осуществляет следующие функции:

1) реализует меры физической и технической безопасности в банке, 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 банка, организации.

19. Подразделение по работе с персоналом осуществляет следующие функции:

1) обеспечивает подписание работниками банка, 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 банка, организации в области информационной безопасности.

3) уведомляет уполномоченный орган о назначении и увольнении работников подразделения по информационной безопасности.

20. Юридическое подразделение осуществляет правовую экспертизу внутренних документов банка, организации по вопросам обеспечения информационной безопасности.

21. Подразделение по комплаенс-контролю совместно с юридическим подразделением банка, организации определяет виды информации, подлежащие включению в перечень защищаемой информации, предусмотренный пунктом 11 Требований.

22. Подразделение внутреннего аудита проводит оценку состояния системы управления информационной безопасностью банка, организации в соответствии с внутренними документами банка, организации, регламентирующими организацию системы внутреннего аудита банка, организации.

23. Подразделение по управлению рисками информационной безопасности банка осуществляет функции, предусмотренные Правилами формирования системы управления рисками и внутреннего контроля для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан, утвержденными постановлением Правления Национального Банка Республики Казахстан от 12 ноября 2019 года № 188, зарегистрированными в Реестре государственной регистрации нормативных правовых актов под № 19632.

Подразделение по управлению рисками информационной безопасности организации осуществляет функции в соответствии с внутренними документами организации.

24. Руководители структурных подразделений банка, организации:

1) обеспечивают ознакомление работников с внутренними документами банка, организации, 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 банка, организации выступает инициатором заключения таких соглашений, договоров.

25. Бизнес-владельцы информационных систем или подсистемы:

1) отвечают за соблюдение требований к информационной безопасности при создании, внедрении, модификации, эксплуатации информационных систем и предоставлении продуктов и услуг клиентам и подразделениям банка, организации, а также при интеграции информационных систем с внешними информационными системами, включая информационные системы государственных органов;

2) формируют и поддерживают актуальность матриц доступа к информационным системам.

26. Работники структурных подразделений банка, организации:

1) отвечают за соблюдение требований к информационной безопасности, принятых в банке, организации;

2) контролируют исполнение требований к информационной безопасности третьими лицами, с которыми они взаимодействуют в рамках своих функциональных обязанностей, в том числе путем включения указанных требований в соглашения, договоры с третьими лицами;

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

27. В случае, если отдельные функции обеспечения информационной безопасности банка, организации переданы сторонним организациям, член исполнительного органа, курирующий вопросы информационной безопасности, является ответственным за обеспечение информационной безопасности банка, организации.

28. Банк, организация ежегодно, не позднее 10 января года, следующего за отчетным годом, представляют в уполномоченный орган информацию о состоянии системы управления информационной безопасностью и ее соответствии Требованиям (далее – информация о СУИБ).

29. Информация о СУИБ составляется в произвольной форме и представляется в уполномоченный орган в электронном формате с

использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых данных или на бумажном носителе.

30. Информация о СУИБ включает сведения о (об):

1) области действия системы управления информационной безопасностью банка, организации 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, условий и обязательств 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 банка, организации в соответствие с Требованиями.

31. Уполномоченный орган осуществляет оценку соответствия банка, организации Требованиям не реже одного раза в 3 (три) года.

Глава 3. Требования к категорированию информационных активов

32. Банк, организация осуществляют категорирование информационных активов путем разделения их на критичные и некритичные на основании уровня убытков от нарушения их конфиденциальности, целостности, доступности.

33. Банк, организация формируют перечень критичных информационных активов с указанием их владельцев.

34. Банк, организация обеспечивают информационную безопасность информационных активов банка, организации, отнесенных к категории

критичных, а также информационных систем, включающих эти активы, в соответствии с Требованиями.

35. Методы и средства защиты информационных активов, отнесенных к категории некритичных, а также информационных систем, полностью состоящих из этих активов, определяются банком, организацией самостоятельно.

Глава 4. Требования к организации доступа к информационным активам

36. Доступ к информации предоставляется работникам банка, организации в объеме, определяемом их функциональными обязанностями.

37. Предоставление доступа к информационным системам банка, организации производится путем формирования и внедрения ролей для обеспечения соответствия прав доступа пользователей информационных систем их функциональным обязанностям. Совокупность таких ролей представляет собой матрицы доступа к информационной системе, которая формируется банком, организацией в электронной форме или на бумажном носителе.

38. Процесс создания и использования матриц доступа в информационные системы банка, организации определяется банком, организацией в соответствии с главой 9 Требований.

39. Доступ к информационным системам банка, организации осуществляется путем идентификации и аутентификации пользователей информационных систем.

Идентификация и аутентификация пользователей информационных систем банка, организации производится одним из следующих способов:

1) посредством ввода пары «учетная запись (идентификатор) – пароль» или с применением способов двухфакторной аутентификации (использованием двух из трех факторов: знания, владения, неотъемлемости);

2) с использованием способов биометрической и (или) криптографической и (или) аппаратной аутентификации.

40. В информационных системах банка, организации используются только персонализированные пользовательские учетные записи.

41. Технологические учетные записи используются 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.

42. В информационных системах банка, организации применяются функции по управлению учетными записями и паролями, а также блокировке учетных записей пользователей, определяемые банком, организацией в соответствии с главой 9 Требований.

Глава 5. Требования к обеспечению безопасности информационной инфраструктуры

43. Подразделение по информационным технологиям банка, организации разрабатывает следующие процессы и обеспечивает их реализацию:

1) процесс формирования и утверждения общей схемы информационной инфраструктуры с указанием физического расположения ее элементов;

2) процесс назначения ответственных работников банка, организации, наделенных правами конфигурирования информационного актива или группы информационных активов (далее – администраторов);

3) процесс документирования и утверждения типовых настроек:

операционных систем;

систем управления базами данных;

телекоммуникационных устройств;

информационных систем;

узлов и конечных точек информационной инфраструктуры, рабочих станций, персональных компьютеров, исполненных в форме, удобной для переноски и использования в том числе, за пределами периметра защиты (далее –

ноутбук) и электронных устройств индивидуального пользования, функционирующих на основе мобильной версии операционной системы (далее – мобильное устройство).

44. Подразделение по информационной безопасности обеспечивает организацию системы контроля изменения настроек безопасности и целостности системных и конфигурационных файлов, а также журналов аудиторского следа в информационных активах банка, организации.

45. Банком, организацией проводятся организационные мероприятия и (или) устанавливаются программно-технические средства, снижающие риск доступа к информационной инфраструктуре неавторизованных устройств либо устройств, настройки которых не соответствует установленному внутренним документом банка, организации порядку обеспечения информационной безопасности.

46. Для каждого информационного актива банка, организации определяются, как минимум, бизнес-владелец информационной системы или подсистемы, а также ИТ-менеджер и (или) администратор.

47. При разработке технических заданий на создание (модернизацию) объектов информационной инфраструктуры бизнес-владелец информационной системы или подсистемы учитывает требования к информационной безопасности.

48. Банк, организация обеспечивают резервное хранение данных информационных систем, их файлов и настроек, которое обеспечивает восстановление работоспособной копии информационной системы.

Порядок и периодичность резервного копирования, хранения, восстановления информации, периодичность тестирования восстановления работоспособности информационных систем из резервных копий определяется банком, организацией.

49. Банк, организация обеспечивают антивирусную защиту информационной инфраструктуры в порядке, определяемом банком, организацией в соответствии с главой 9 Требований.

50. Порядок обеспечения физической безопасности центров обработки данных банка, организации определяется банком, организацией в соответствии с главой 9 Требований.

51. На рабочие станции, ноутбуки и корпоративные мобильные устройства работников банка, организации устанавливается программное обеспечение в соответствии с их функциональными обязанностями.

52. Подразделение по информационным технологиям формирует и актуализирует перечень программного обеспечения, разрешенного к использованию в банке, организации. Программное обеспечение включается в перечень после проведения проверки подразделением по информационной безопасности.

53. Организационные и технические меры, обеспечивающие защиту рабочих станций, ноутбуков и мобильных устройств банка, организации, а также носителей информации и сетевой инфраструктуры определяются банком, организацией в соответствии с главой 9 Требований.

Глава 6. Требования к средствам криптографической защиты информации

54. Процесс внедрения и поддержки средств криптографической защиты информации согласовывается бизнес-владельцем информационной системы с подразделением по информационной безопасности.

55. Порядок использования средств криптографической защиты информации определяется банком, организацией в соответствии с главой 9 Требований. Перечень применяемых средств криптографической защиты информации с указанием их назначения, реализованных в них криптографических алгоритмов, наименования информационной системы, владельца информационной системы, использующей средства криптографической защиты информации определяет банк, организация.

Глава 7. Требования к обеспечению информационной безопасности при доступе третьих лиц к информационным активам банка, организации

56. Банк, организация обеспечивает информационную безопасность при доступе к информационным активам банка, организации лиц, не являющихся работниками или клиентами банка, организации (далее – третьи лица).

57. Доступ к информационным активам банка, организации 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 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 третьих лиц.

58. При осуществлении проверки деятельности банка, организации либо при запросе информации уполномоченным органом до предоставления соответствующего доступа или информации проверяются полномочия представителей уполномоченного органа.

59. В целях обеспечения контроля деятельности третьих лиц предусматриваются, как минимум, одна из следующих организационных и (или) программно-технических мер:

1) проверка результата деятельности третьих лиц;

2) осуществление деятельности третьих лиц только в присутствии работников банка, организации;

3) ведение аудиторского следа по действиям третьих лиц;

4) запись сессии доступа к информационным активам банка, организации.

60. В случае передачи третьим лицам информационных активов банка, организации (размещение серверных мощностей в сторонних центрах обработки данных, использование внешних сервисов обработки и/или хранения данных) предпринимаются следующие меры обеспечения информационной безопасности:

1) отражение в соответствующем соглашении, договоре с третьим лицом требований по защите информационных активов банка, организации и права проверки банком, организацией исполнения таких требований, а также условий о

возмещении ущерба, возникшего вследствие нарушения информационной безопасности и работоспособности информационных систем;

2) исключение возможности доступа третьих лиц к информации, передача которой третьим лицам не допускается в соответствии с гражданским, банковским законодательством Республики Казахстан, законодательством Республики Казахстан о персональных данных и их защите. При использовании облачных сервисов для этих целей применяется метод хранения информации в зашифрованном виде с раскрытием информации на стороне банка, организации. При этом ключ шифрования хранится в банке, организации.

Глава 8. Требования к проведению внутренних проверок состояния информационной безопасности

61. Состояние информационной безопасности оценивается путем проведения проверок:

1) подразделением по информационной безопасности – в соответствии с планом, утверждаемым членом исполнительного органа, курирующим подразделение по информационной безопасности, а также по отдельному распоряжению руководителя исполнительного органа или руководителя органа управления банка, организации;

2) подразделением внутреннего аудита – в рамках годового плана аудиторских проверок в соответствии с внутренними документами банка, организации, регламентирующими организацию системы внутреннего аудита банка, организации.

62. По результатам проверки подразделением по информационной безопасности составляется отчет с приложением материалов проверки, который доводится до сведения проверяемого подразделения банка, организации.

Глава 9. Требования к процессам системы управления информационной безопасностью

Параграф 1. Требования к процессу организации доступа к информационным системам

63. Процесс создания матрицы доступа к информационной системе осуществляется в порядке, определяемом банком, организацией, и состоит из следующих этапов:

1) бизнес-владелец информационной системы обеспечивает формирование и актуальность матрицы доступа к информационной системе банка, организации;

2) владелец бизнес-процесса совместно с ИТ-менеджером информационной системы обеспечивают формирование и актуальность ролей в информационной системе в объеме, определяемом функциональными обязанностями работников;

3) сформированные роли согласовываются с бизнес-владельцем информационной системы;

4) банк, организация обеспечивает исключение в ролях конфликтующих прав доступа, позволяющих обойти существующие автоматизированные контроли;

5) ИТ-менеджер информационной системы реализует роли в информационной системе;

6) бизнес-владелец информационной системы или подсистемы и владелец бизнес-процесса тестируют созданные роли;

7) ИТ-менеджер информационной системы внедряет роли в информационной системе.

64. Внесение изменений и дополнений в матрицу доступа к информационной системе осуществляется в порядке, установленном пунктом 63 Требований.

65. Механизм управления доступом информационной системы банка, организации обеспечивает:

1) возможность регистрации нового пользователя на уровне приложения;

2) назначение пользователям прав на доступ к информационным системам только через роли;

3) предоставление пользователям отдельных прав в дополнение к имеющейся роли в информационной системе по согласованию с бизнес-владельцем информационной системы или подсистемы и с уведомлением подразделения по информационной безопасности;

4) сопровождение ролей пользователей (создание, изменение, удаление);

5) возможность блокирования одновременного доступа под одними учетными данными с различных аппаратных средств (компьютеров) для транзакционных систем;

6) ведение аудиторского следа.

66. Механизм управления доступом к данным информационной системы банка, организации включает:

1) обеспечение доступа к данным информационной системы через приложение;

2) предоставление доступа к данным информационной системы напрямую, минуя приложение, осуществляется по согласованию с подразделением по информационной безопасности;

3) формирование и актуализацию подразделением по информационным технологиям перечня пользователей, которым предоставлен доступ к данным напрямую, минуя приложение.

67. При изменении функциональных обязанностей работника отключаются все имеющиеся права доступа и присваиваются новые права доступа, соответствующие его новым функциональным обязанностям. При увольнении работника не более, чем через сутки с даты увольнения отключаются все его учетные записи.

68. Подразделением по информационной безопасности производится проверка корректности прав доступа к информационным системам в соответствии с матрицей доступа, а также контроль отключения прав доступа уволенным работникам.

69. Пересмотр ролей и прав доступа к информационным системам производится не реже одного раза в год бизнес-владельцами информационных систем или подсистем с привлечением заинтересованных подразделений банка, организации.

70. При отсутствии технической возможности реализации одного или нескольких требований настоящего параграфа в банке, организации применяются компенсирующие меры в виде дополнительных технических и организационных мер по частичному или полному исключению влияния рисков информационной безопасности.

Параграф 2. Требования к процессу управления паролями и блокировками учетных записей пользователей в информационных системах

71. В информационных системах банка, организации применяются следующие параметры функции по управлению паролями и блокировками учетных записей пользователей:

1) минимальная длина пароля – значение данного параметра составляет не менее 8 символов. Проверка пароля на соответствие данному параметру производится при каждой смене пароля, в случае несоответствия – выдается уведомление пользователю;

2) сложность пароля – возможность проверки наличия в пароле как минимум трех групп символов: строчных букв, заглавных букв, цифровых значений, специальных символов. Проверка пароля на соответствие данному параметру производится при каждой смене пароля, в случае несоответствия – выдается уведомление пользователю;

3) история пароля –- новый пароль не повторяет как минимум семь предыдущих паролей. Проверка пароля на соответствие данному параметру производится при каждой смене пароля, в случае несоответствия выдается уведомление пользователю;

4) минимальный срок действия пароля – 1 (один) рабочий день;

5) максимальный срок действия пароля – не более 60 (шестидесяти) календарных дней. Проверка пароля на соответствие данному параметру

производится при каждом входе в информационную систему и смене пароля. В случае, если до истечения максимального срока действия остается 7 (семь) и менее календарных дней, пользователю выдается соответствующее уведомление. По истечении максимального срока действия пароля информационная система блокирует доступ и требует обязательную смену пароля;

6) при первом входе в информационную систему либо после смены пароля администратором информационная система запрашивает у пользователя смену пароля с невозможностью отклонить данную процедуру. Данное правило превалирует над правилом о сроке действия пароля;

7) в случае отсутствия активности пользователя в информационной системе более 30 (тридцати) календарных дней его учетная запись автоматически блокируется;

8) при последовательном пятикратном вводе неправильного пароля учетная запись пользователя временно блокируется;

9) при неактивности пользователя более 30 (тридцати) минут информационная система автоматически завершает сеанс работы пользователя либо блокирует рабочую станцию или ноутбук с возможностью разблокировки только при вводе аутентификационных данных пользователя.

72. Требования пункта 71 Требований не применяются в случаях, когда:

1) информационная система интегрирована в части аутентификации с информационной системой, соответствующей требованиям пункта 71 Требований;

2) функции одной информационной системы минимизируют риск неавторизованного доступа в другой информационной системе.

73. Процесс управления паролями и учетными записями определяется банком, организацией и включает:

1) управление администраторами информационных систем учетными записями пользователей информационных систем и сменой их паролей;

2) подачу и рассмотрение заявок на создание учетных записей, а также изменения пароля при возникновении нештатной ситуации;

3) подачу заявок на изменение или удаление учетных записей;

4) идентификацию лиц, подающих заявки на создание, изменение или удаление учетных записей, а также изменение пароля;

5) недопущение неправомерной передачи паролей третьим лицам, а также администраторам информационных систем и иным работникам банка, организации;

6) недопущение работы в информационных системах под чужими учетными записями, за исключением предоставления доступа к чужой учетной записи в целях обеспечения непрерывности деятельности по согласованию с подразделением по информационной безопасности в указанный промежуток времени при обеспечении точной идентификации пользователя.

Параграф 3. Требования к процессу обеспечения безопасности информации

74. Процесс защиты информации при использовании Интернета и электронной почты определяется банком, организацией и включает любой из следующих методов, но не ограничиваясь ими:

1) организационный: обеспечение осведомленности персонала, ограничение количества работников, имеющих доступ к Интернету, службам мгновенных сообщений, облачным сервисам, IP-телефонии и внешней электронной почте;

2) программно-технический: ограничение количества пользователей и их доступа к интернет-ресурсам, контроль информации, передаваемой в Интернет, в том числе по службам мгновенных сообщений, IP-телефонии и внешней электронной почте, предоставление доступа в Интернет через терминальный сервер, разделение сегментов сети, ведение архива внешней электронной почты (срок хранения определяется банком, организацией, ограничение доступа на изменение или удаление информации в данном архиве), использование систем противодействия атакам, направленным на периметр защиты информационной инфраструктуры банка, организации, шифрование передаваемой информации.

75. Для защиты информации при использовании внешних носителей электронной информации применяются любой из следующих методов, включая, но не ограничиваясь ими:

1) организационный: обеспечение осведомленности персонала, ограничение количества работников, имеющих доступ к записи на внешние носители информации;

2) программно-технический: использование программно-технических средств, обеспечивающих ограничение, контроль и шифрование записи информации на внешние носители, отключение неиспользуемых портов ввода-вывода и устройств записи внешних носителей на рабочих станциях персонала банка, организации и серверах.

76. Для защиты информации при использовании бумажных носителей применяются любой из следующих методов, включая, но не ограничиваясь ими:

1) организационный: ограничения, определяемые банком, организацией, обеспечение осведомленности персонала, ограничение количества работников, имеющих доступ к работе с документами, содержащими защищаемую информацию;

2) программно-технический: использование программно-технических средств, обеспечивающих контроль вывода информации на бумажные носители.

77. Для защиты информации в случае утраты штатных носителей информации применяются любой из следующих методов, включая, но не ограничиваясь ими:

1) организационный: ограничения, определяемые банком, организацией, обеспечение физической безопасности периметра банка, организации, обеспечение осведомленности персонала, нормы утилизации носителей информации;

2) программно-технический: использование средств, контролирующих вскрытие системных блоков, шифрование информации на рабочих станциях, серверах, шифрование или токенизация (замена оригинальных данных на суррогат с использованием набора случайных данных (токена) информации в системах управления базами данных.

78. Уничтожение защищаемой информации производится методами, исключающими ее восстановление, с использованием любого из следующих методов уничтожения информации в зависимости от типа носителя:

1) физическое уничтожение носителя информации;

2) электромагнитное воздействие на носитель информации (для магнитных носителей);

3) программное уничтожение электронной информации специализированными программными средствами.

Параграф 4. Требования к процессу обеспечения безопасности периметра защиты информационной инфраструктуры

79. Банком, организацией определяются периметр защиты информационно-коммуникационной инфраструктуры (далее – периметр защиты). Подразделением по информационным технологиям утверждаются и поддерживаются в актуальном состоянии схема периметра защиты и перечень администраторов средств обеспечения безопасности периметра защиты.

80. Телекоммуникационные соединения, за исключением соединений с городской телефонной сетью, выходящие за периметр защиты банка, организации, подлежат шифрованию.

81. Шифрование телекоммуникационных соединений производится методами, согласованными с подразделением по информационной безопасности.

82. Наравне с шифрованием телекоммуникационных соединений, указанных в пунктах 80 и 81 Требований, используется шифрование передаваемой информации.

83. Для ограничения доступа к информационной инфраструктуре на периметре защиты устанавливаются межсетевые экраны.

84. Правила доступа, установленные на межсетевых экранах, настраиваются на блокирование соединений, неиспользуемых для функционирования информационных активов банка, организации. Указанные правила согласовываются с подразделением по информационной безопасности. Для выявления и отражения атак на периметр защиты используются средства обнаружения и предотвращения вторжений.

85. Банк, организация обеспечивают применение мер предотвращения атак типа «отказ в обслуживании». При реализации указанных мер используются штатные механизмы систем обеспечения безопасности периметра защиты и (или) дополнительные способы обеспечения безопасности периметра защиты.

86. Доступ пользователей к информационным активам банка, организации, находящимся внутри периметра защиты, из-за пределов периметра защиты предоставляется только по зашифрованному каналу с аутентификацией пользователя на периметре защиты. Доступ пользователей к информационным системам из-за пределов периметра защиты предоставляется только с использованием методов двухфакторной аутентификации (использованием двух из трех факторов: «что я знаю», «что я имею», «что я есть сам»).

87. Для обеспечения безопасности доступа пользователей к ресурсам Интернета, а также использования внешней электронной почты устанавливаются соответствующие шлюзы, обеспечивающие:

1) очистку трафика от вредоносного кода;

2) блокировку ресурсов Интернета, содержащих деструктивные функции;

3) очистку почтового трафика от спама;

4) аутентификацию доменного имени отправителя входящей электронной почты и возможность аутентификации доменного имени исходящей электронной почты с использованием криптографических алгоритмов.

88. Конфигурация средств обеспечения безопасности периметра защиты выполняется с учетом рекомендаций производителей и пересматривается с периодичностью, определяемой банком, организацией. В обязательном порядке изменяются пароли на предустановленные учетные записи. Неиспользуемые предустановленные учетные записи блокируются или удаляются.

89. С периодичностью, определяемой банком, организацией, проводится тестирование на проникновение в информационную инфраструктуру независимыми внешними экспертами в данной области. В рамках данного тестирования, кроме поиска и попыток эксплуатации уязвимостей системного и прикладного программного обеспечения, проводятся нагрузочные тесты, включая имитацию атак «отказ в обслуживании», а также тесты по социальной инженерии.

Параграф 5. Требования к процессу обеспечения защиты информационной инфраструктуры

90. ИТ-менеджер информационной системы обеспечивает синхронизацию системного времени информационного актива с централизованным источником эталонного времени.

91. Подразделение по информационным технологиям обеспечивает разделение внутренней сетевой инфраструктуры как минимум на следующие сегменты:

1) клиентский (пользовательский);

2) серверный (инфраструктурный);

3) разработки (при наличии);

4) тестовый.

92. Между сегментами сетевой инфраструктуры настраиваются правила доступа на блокирование соединений, неиспользуемых для функционирования информационных активов банка, организации.

93. Банк, организация в целях защиты информационной инфраструктуры используют методы или системы, позволяющие выявлять непредвиденную (аномальную) активность в информационной инфраструктуре банка, организации.

94. Банком, организацией используются организационные и (или) технические меры по созданию и применению групповых политик безопасности с использованием возможностей операционных систем, сетевой архитектуры или программного обеспечения, позволяющие устанавливать на конечных устройствах информационной инфраструктуры настройки безопасности.

Исключение конечных устройств информационной инфраструктуры из групповых политик безопасности согласуется с подразделением по информационной безопасности.

95. При размещении на одном сервере или гипервизоре нескольких информационных активов банка, организации, обеспечивается защита на уровне, соответствующем максимально критичному информационному активу, размещенному на данном сервере или гипервизоре.

Параграф 6. Требования к процессу обеспечения защиты информационных систем

96. Разработка и доработка информационных систем не осуществляется в среде промышленной эксплуатации.

97. Среды разработки, тестирования и промышленной эксплуатации отделяются друг от друга таким образом, чтобы изменения, внесенные в любую из этих сред, не оказывали влияния на информационную систему, расположенную в другой среде.

98. В случае использования в среде разработки и тестирования защищаемой информации, предпринимаются соответствующие меры по их защите.

99. Работники подразделения по информационным технологиям банка, организации и сторонних организаций, осуществляющие разработку, не имеют полномочий на перенос изменений информационной системы в промышленную среду, а также административный доступ к информационным системам в промышленной среде.

100. Перед вводом в промышленную эксплуатацию информационной системы в ней изменяются настройки безопасности, установленные по умолчанию, на настройки, соответствующие требованиям к информационной безопасности, установленным в банке, организации. Указанные настройки включают замену паролей, используемых при тестировании, а также удаление всех тестовых учетных записей.

101. Контроль использования привилегированных учетных записей обеспечивается путем:

1) составления и утверждения перечня администраторов информационных систем (операционная система, система управления базами данных, приложение);

2) введения двойного контроля при исполнении функций администрирования информационных систем и (или) внедрения специальных комплексов контроля использования привилегированных учетных записей.

102. Информационные системы банка, организации обеспечиваются технической поддержкой, в состав которой входят услуги по предоставлению обновлений соответствующей информационной системы, в том числе обновлений безопасности.

Параграф 7. Требования к процессу работы с персоналом

103. При приеме на работу новый работник банка, организации подписывает обязательство о неразглашении защищаемой информации. Обязательство приобщается к личному делу работника.

104. При приеме на работу нового работника, не позднее 5 (пяти) рабочих дней с момента приема на работу, он ознакамливается под подпись с основными требованиями к обеспечению информационной безопасности (вводный инструктаж). Результат ознакомления фиксируется в соответствующем журнале инструктажа или ином документе, подтверждающем прохождение инструктажа. Отдельный документ, подтверждающий прохождение инструктажа, приобщается к личному делу работника.

105. До ознакомления работника с требованиями к информационной безопасности ему предоставляется доступ только к некритичным информационным активам.

106. Трудовой договор, заключаемый с работником банка, организации, содержит обязательство о соблюдении требований по обеспечению информационной безопасности.

107. Банком, организацией разрабатывается программа повышения осведомленности работников в вопросах обеспечения информационной безопасности. При этом применяются следующие методы повышения осведомленности работников:

1) ознакомление с внутренними документами банка, организации, а также с внесенными в них изменениями и дополнениями;

2) проведение тестирования работников на знание требований внутренних документов банка, организации по информационной безопасности в соответствии с планом проведения тестирования работников банка, организации, утверждаемым исполнительным органом банка, организации;

3) методы, определенные банком, организацией.

108. При инструктаже, а также и при дальнейших мероприятиях по повышению осведомленности освещаются:

1) методы противодействия «социальной инженерии»;

2) запрет на распространение информации, запрещенной банковским законодательством Республики Казахстан;

3) положения о полномочиях банка, организации осуществлять мониторинг любой информации, создаваемой, хранимой и обрабатываемой в информационных системах банка, организации;

4) условия об ответственности, предусмотренной за нарушение внутренних документов банка, организации, устанавливающих требования к обеспечению информационной безопасности.

109. Банк, организация обеспечивают повышение квалификации работников подразделений по информационной безопасности, по управлению рисками информационной безопасности и внутреннего аудита путем проведения:

1) внутренних мероприятий (лекции, семинары);

2) внешнего обучения (посещение курсов, семинаров – не реже одного раза в три года для каждого работника).

110. При увольнении работника в целях обеспечения информационной безопасности осуществляются мероприятия по:

1) приему - передаче документов и информационных активов банка, организации;

2) сдаче удостоверений, пропусков и разрешительных документов;

3) проведению инструктажа с увольняющимся работником по неразглашению конфиденциальной информации;

4) блокировке или удалению учетных записей в информационных системах.

Параграф 8. Требования к процессу ведения аудиторского следа в информационных системах

111. ИТ-менеджер информационной системы обеспечивает ведение и неизменность аудиторского следа, как на организационном, так и на техническом уровне.

112. В информационных активах банка, организации используется функция ведения аудиторского следа, которая отражает следующее:

1) события установления соединений, идентификации, аутентификации и авторизации в информационном активе (успешные и неуспешные);

2) события модификации настроек безопасности;

3) события модификации групп пользователей и их полномочий;

4) события модификации учетных записей пользователей и их полномочий;

5) события, отражающие установку обновлений и (или) изменений в информационной системе;

6) события изменения параметров аудита;

7) события изменений системных параметров.

113. Формат аудиторского следа включает следующую информацию:

1) идентификатор (логин) пользователя, совершившего действие;

2) дата и время совершения действия;

3) наименование рабочей станции пользователя и (или) IP адрес, с которого совершено действие;

4) название объектов, с которыми проводилось действие;

5) тип или название совершенного действия;

6) результат действия (успешно или не успешно).

114. Срок хранения аудиторского следа составляет не менее 3 (трех) месяцев в оперативном доступе и не менее 1 (одного) года в архивном доступе либо не менее 1 (одного) года в оперативном доступе.

Параграф 9. Требования к процессу обеспечения антивирусной защиты

115. Банк, организация используют лицензионное антивирусное программное обеспечение или системы, обеспечивающие целостность и неизменность программной среды, как на рабочих станциях, ноутбуках, мобильных устройствах, так и на серверах, банкоматах и банковских киосках.

116. Используемое банком, организацией антивирусное программное обеспечение соответствует следующим требованиям:

1) обнаружение вирусов на основе известных сигнатур;

2) обнаружение вирусов на основе эвристического анализа (поиска характерных для вирусов команд и поведенческого анализа);

3) сканирование сменных носителей при подключении;

4) запуск сканирования и обновления антивирусной базы по расписанию;

5) наличие централизованной консоли администрирования и мониторинга;

6) блокирование для пользователя возможности прерывания функционирования антивирусного программного обеспечения, а также процессов обновления антивирусного программного обеспечения и плановой проверки на отсутствие вирусов;

7) для виртуальной среды – использование антивирусным программным обеспечением встроенных функций безопасности виртуальных сред, при отсутствии таких возможностей – подтверждение производителя о тестировании антивирусного программного обеспечения в виртуальных средах, используемых банком, организацией;

8) для мобильных устройств и иных устройств, используемых вне периметра защиты банка, организации, использование антивирусного программного обеспечения со встроенной функцией межсетевого экранирования.

117. При использовании систем, обеспечивающих целостность и неизменность программной среды, минимальными требованиями являются:

1) наличие лицензионного программного обеспечения, предусматривающего обновление и техническую поддержку;

2) наличие централизованной консоли администрирования и мониторинга;

3) наличие возможности блокирования для конечного пользователя возможности прерывания функционирования данной системы;

4) наличие возможности проверки образа программной среды антивирусным программным обеспечением перед установкой на конечные устройства;

5) наличие межсетевого экрана для мобильных устройств и иных устройств, используемых вне периметра защиты.

118. Выбор антивирусного программного обеспечения проводится подразделением по информационным технологиям при обязательном участии подразделения по информационной безопасности.

119. Антивирусное программное обеспечение максимально исключает прерывание пользователем всех служебных процессов. Обновление антивирусного программного обеспечения производится не реже одного раза в сутки, полное сканирование компьютера – не реже одного раза в неделю.

Параграф 10. Требования к процессу управления обновлениями и уязвимостями информационных активов

120. ИТ-менеджер информационной системы обеспечивает своевременную установку обновлений безопасности информационных активов банка, организации.

121. Обновления безопасности информационных активов, устраняющие критичные уязвимости, устанавливаются не позднее одного месяца со дня их публикации и распространения производителем, за исключением случаев, согласованных с подразделением по информационной безопасности.

122. Обновления информационных активов до установки в промышленную среду проходят испытания в тестовой среде.

123. В случае невозможности установки обновлений по согласованию с подразделением по информационной безопасности, ИТ-менеджер информационной системы реализует корректирующие меры.

124. Подразделение по информационной безопасности обеспечивает сканирование (технический анализ защищенности) информационных активов на наличие уязвимостей с использованием специализированного программного обеспечения (далее – сканирование). Сканирование информационных активов банка, организации проводится на плановой основе не реже одного раза в 6 (шесть) месяцев. Сканирование проводится работниками банка, организации и (или) внешними специализированными организациями. Результаты сканирования формируются в виде отчета о состоянии информационной безопасности с указанием рекомендаций о корректирующих мерах по устранению выявленных уязвимостей.

125. ИТ-менеджер информационной системы обеспечивает реализацию корректирующих мер по устранению выявленных уязвимостей.

По окончании работ по устранению уязвимостей ИТ-менеджер информационной системы представляет в подразделение по информационной безопасности подтверждение об устранении выявленных уязвимостей.

Параграф 11. Требования к процессу использования средств криптографической защиты информации

126. Процесс использования средств криптографической защиты информации определяется подразделением по информационным технологиям по согласованию с подразделением по информационной безопасности банка, организации, включая, но не ограничиваясь:

1) описание средства криптографической защиты информации (наименование системы, криптоалгоритм, длина ключа);

2) область применения средства криптографической защиты информации;

3) описание настройки средства криптографической защиты информации;

4) порядок управления ключевой информацией: генерации, безопасной передачи (обмена ключами, с учетом требования использования различных каналов для передачи ключа и защищаемой информации), хранения, использования и уничтожения;

5) действия при компрометации ключевой информации;

6) порядок использования средства криптографической защиты информации конечными пользователями;

7) перечень лиц, допущенных к администрированию средства криптографической защиты информации и управлению ключевой информацией.

Параграф 12. Требования к процессу обеспечения физической безопасности центров обработки данных

127. Центр обработки данных банка, организации оснащается следующими системами технической безопасности:

1) системой контроля и управления доступом;

2) охранной сигнализацией;

3) пожарной сигнализацией;

4) системой автоматического пожаротушения;

5) системой поддержания заданных параметров температуры и влажности;

6) системой видеонаблюдения.

Серверное и коммуникационное оборудование подключается к системе электропитания через источники бесперебойного питания.

В случае отсутствия в банке, организации центра обработки данных, требования настоящего пункта распространяются на помещения банка, организации, в которых размещены системы и компоненты информационной инфраструктуры банка, организации.

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

129. Банк, организация ведут журнал системы контроля и управления доступом в центр обработки данных, который хранится не менее 1 (одного) года.

130. Система автоматического пожаротушения центра обработки данных обеспечивает устранение возгорания по всему объему помещения и имеет

резервный запас.

131. Система видеонаблюдения центра обработки данных обеспечивает наблюдение за всеми проходами, входами в центр обработки данных. В центре обработки данных расстановка видеокамер исключает наличие зон внутри помещения центра обработки данных и перед его входом, не покрытых видеонаблюдением.

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

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

134. В целях предотвращения несанкционированного физического доступа к серверам и активному сетевому оборудованию, находящемуся вне центра обработки данных, определяются и реализуются меры по обеспечению их безопасности.

135. Предоставление физического доступа к информационным активам банка, организации определяется банком, организацией.

Параграф 13. Требования к процессу обеспечения защиты рабочих станций, ноутбуков и мобильных устройств работников

136. В банке, организации определяются и внедряются организационные и технические меры, запрещающие пользователям проводить самостоятельно установку и настройку программного обеспечения, рабочих станций, ноутбуков и периферийного оборудования.

137. Пользователям не предоставляются права доступа локального администратора или аналогичные права доступа, за исключением случаев, когда права доступа локального администратора или права, аналогичные правам доступа локального администратора, требуются для функционирования программного обеспечения, автоматизирующего функции, исполняемые пользователем.

138. В случае невозможности исполнения пользователем его функциональных обязанностей без осуществления самостоятельной установки и настройки программного обеспечения и оборудования, такому пользователю предоставляются права локального администратора или аналогичные права.

139. Перечень пользователей, указанных в пунктах 137 и 138 Требований, формируется, актуализируется и утверждается руководителем подразделения по информационным технологиям по согласованию с подразделением по информационной безопасности. Подразделение по информационной безопасности осуществляет контроль использования прав доступа пользователей, указанных в пунктах 137 и 138 Требований.

140. Подразделение по информационным технологиям обеспечивает учет рабочих станций, ноутбуков и мобильных устройств в корпоративной сети банка, организации, который позволяет точно идентифицировать местонахождение данной рабочей станции или принадлежность ноутбука, мобильного устройства.

141. В случае подключения мобильных устройств, ноутбуков к информационным активам банка, организации из-за пределов периметра защиты банка, организации на данных устройствах устанавливается специальное программное обеспечение, обеспечивающее защищенный доступ к информационным активам (шифрование канала связи, обеспечение двухфакторной аутентификации, дистанционное удаление данных с мобильного устройства).

142. При использовании для обработки информационных активов банка, организации личных ноутбуков и мобильных устройств работников банка, организации, на данные ноутбуки и мобильные устройства устанавливается специальное программное обеспечение, обеспечивающие разделение сред обработки личных данных и информационных активов банка, организации.

143. Вся информация банка, организации, размещенная на ноутбуках и мобильных устройствах, хранится в зашифрованном виде.

Глава 10. Требования к обеспечению безопасности программного обеспечения дистанционного оказания услуг банка, организации

Сноска. Требования дополнены главой 10 в соответствии с постановлением Правления Агентства РК по регулированию и развитию финансового рынка от 17.10.2023 № 75 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

144. Программное обеспечение дистанционного оказания услуг банка, 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).

145. Разработка и (или) доработка программного обеспечения дистанционного оказания услуг осуществляется банком, организацией в соответствии с внутренними документами банка, организации, регламентирующими порядок разработки и (или) доработки программного обеспечения, этапы разработки и их участников.

146. В случае, если разработка и (или) доработка программного обеспечения дистанционного оказания услуг банка, организации передана сторонней организации и (или) третьему лицу, банк, организация обеспечивает исполнение сторонней организацией и (или) третьим лицом требований настоящей главы и внутренних документов, отвечает за состояние безопасности программного обеспечения дистанционного оказания услуг.

147. Хранение исходных кодов программного обеспечения дистанционного оказания услуг, разрабатываемых в банке, организации, осуществляется в специализированных системах управления репозиториями кода, размещаемых в периметре защиты банка, организации, с обеспечением резервного копирования.

148. Независимо от принятого в банке, организации подхода к разработке и (или) доработке программного обеспечения дистанционного оказания услуг, обязательным этапом является тестирование безопасности, в ходе которого осуществляются, как минимум, следующие мероприятия:

1) статический анализ исходного кода;

2) анализ компонентов и сторонних библиотек.

149. Статический анализ исходного кода программного обеспечения дистанционного оказания услуг банка, организации 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 приложения;

5) наличие механизмов обхода систем защиты приложения;

6) использование в коде секретов в открытом виде;

7) нарушение шаблонов и практик обеспечения безопасности приложения.

150. Анализ компонентов и (или) сторонних библиотек программного обеспечения дистанционного оказания услуг банка, организации 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.

151. Банк, организация обеспечивают 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.

152. Банк, организация осуществляют ввод в эксплуатацию программного обеспечения дистанционного оказания услуг и (или) его новых версий после согласования с подразделением по информационной безопасности.

153. Банк, организация обеспечивают 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.

154. 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.

155. При первичной регистрации клиента в мобильном приложении банк, организация осуществляют биометрическую идентификацию клиента посредством Центра обмена идентификационными данными (далее - ЦОИД) или с использованием биометрических данных, полученных посредством устройств банка, организации.

156. Изменение кода доступа (пароля) к мобильному приложению осуществляется с применением биометрической идентификации клиента с использованием биометрических данных, подтвержденных ЦОИД или полученных посредством устройств банка, организации.

157. 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 банка, организации.

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

159. Веб-приложение обеспечивает:

1) однозначность идентификации принадлежности веб-приложения банку, 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.

160. Мобильное приложение обеспечивает:

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

2) блокировку функционала по оказанию дистанционных услуг банка, 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 банком, организацией номера мобильного телефона;

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

161. Банк, 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.

e.zan
Қазақстан Республикасының электронды нысандағы нормативтік құқықтық актілердің эталонды бақылау банкі
Эталонный контрольный банк нормативных правовых актов Республики Казахстан в электронном виде
Редакциялау күні 17.10.2023
Сақтау күні 29.03.2024
Дата редакции 17.10.2023
Дата скачивания 29.03.2024

Приложение 2
к постановлению Правления
Национального Банка
Республики Казахстан
от 27 марта 2018 года
№ 48

Правила и сроки предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах

Сноска. Правила в редакции постановления Правления Агентства РК по регулированию и развитию финансового рынка от 29.04.2022 № 30 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

1. Настоящие Правила и сроки предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах (далее – Правила) разработаны в соответствии с пунктом 7 статьи 61-5 Закона Республики Казахстан «О банках и банковской деятельности в Республике Казахстан» и определяют порядок и сроки предоставления банками, филиалами банков-нерезидентов Республики Казахстан (далее – банк) и организациями, осуществляющими отдельные виды банковских операций (далее – организация), информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах.

2. В Правилах используются понятия, предусмотренные Законом Республики Казахстан «Об информатизации», а также следующие понятия:

1) информационная безопасность в сфере информатизации (далее – информационная безопасность) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

2) 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;

3) угроза информационной безопасности – совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

4) информация об инцидентах информационной безопасности – информация об отдельно или серийно возникающих сбоях в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающих угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов банка, организации;

5) инцидент информационной безопасности – отдельно или серийно возникающие сбои в работе информационно-коммуникационной 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 банка, организации;

6) доступ – возможность использования информационных активов;

7) атака типа «отказ в обслуживании» (DoS или DDoS-атака, в зависимости от количества атакующих внешних источников атаки) – атака на информационную систему с целью нарушения штатного режима ее работы или создание условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым ресурсам, либо этот доступ затруднен;

8) уполномоченный орган – уполномоченный орган по регулированию, контролю и надзору финансового рынка и финансовых организаций.

3. Банк, организация предоставляют 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 банком или организацией незамедлительно посредством автоматизированной системы уполномоченного органа, предназначенной для обработки информации о событиях и инцидентах информационной безопасности и интегрированной с системами информационной безопасности или системами банка, организации, осуществляющими в реальном времени сбор и анализ информации о событиях в информационной инфраструктуре (далее – АСОИ) или в электронном формате с использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых данных.

4. Банк, организация обеспечивают передачу сведений об отдельно или серийно возникающих событиях в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, включая системы информационной безопасности, свидетельствующих о нарушении принятых мер обеспечения информационной безопасности либо о ранее неизвестной ситуации, потенциально имеющей отношение к информационной безопасности (далее – сведения о нарушениях, сбоях в информационных системах) посредством АСОИ. Сведения о нарушениях, сбоях в информационных системах предоставляются в автоматизированном режиме путем передачи из систем информационной безопасности или систем банка, организации, осуществляющих в реальном времени сбор и анализ информации о событиях в информационной инфраструктуре банка, организации.

Для организаций, входящих в структуру Национального Банка Республики Казахстан, и юридических лиц, пятьдесят и более процентов голосующих акций которых принадлежат Национальному Банку Республики Казахстан, допускается

передача сведений о нарушениях, сбоях в информационных системах посредством объектов информатизации Национального Банка Республики Казахстан, интегрированных с АСОИ.