«ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ БАНКІ»

РЕСПУБЛИКАЛЫҚ
МЕМЛЕКЕТТІК МЕКЕМЕСІ

РЕСПУБЛИКАНСКОЕ
ГОСУДАРСТВЕННОЕ
УЧРЕЖДЕНИЕ

**«НАЦИОНАЛЬНЫЙ БАНК
РЕСПУБЛИКИ КАЗАХСТАН»**

БАСҚАРМАСЫНЫҢ ҚАУЛЫСЫ

**ПОСТАНОВЛЕНИЕ
ПРАВЛЕНИЯ**

27 марта 2018 года

№ 48

Алматы қаласы

город Алматы

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

В соответствии с подпунктом 86-1) части второй статьи 15 Закона Республики Казахстан от 30 марта 1995 года «О Национальном Банке Республики Казахстан» и 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:**

1. Утвердить:

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

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

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**

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

Требования к обеспечению информационной безопасности банков и организаций, осуществляющих отдельные виды банковских операций

Глава 1. Общие положения

1. Настоящие Требования к обеспечению информационной безопасности банков и организаций, осуществляющих отдельные виды банковский операций, (далее - Требования) разработаны в соответствии с подпунктом 86-1) части второй статьи 15 Закона Республики Казахстан от 30 марта 1995 года «О Национальном Банке Республики Казахстан», пунктом 7 статьи 61-5 Закона Республики Казахстан от 31 августа 1995 года «О банках и банковской деятельности в Республике Казахстан» и устанавливают требования к обеспечению информационной безопасности банков и организаций, осуществляющих отдельные виды банковских операций (далее - организация).

2. В Требованиях используются следующие понятия:

1) штатный носитель информации – носитель информации, являющийся составной частью объекта информационно-коммуникационной инфраструктуры;

2) информация об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах - 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;

3) инцидент информационной безопасности, включая нарушения, сбои в информационных системах (далее - 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;

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

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

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

7) информационная безопасность - состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

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

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

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

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

15) информационно-коммуникационная инфраструктура банка, организации (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;

16) бизнес-процесс – совокупность взаимосвязанных мероприятий или задач, направленных на создание определенного продукта или услуги для внешнего (клиент) или внутреннего (работник, подразделение банка, организации, другой бизнес-процесс) 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 системы и компоненты информационной инфраструктуры 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;

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 между информационными системами;

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;

3) требования к организации доступа к информационным активам;

4) требования к обеспечению безопасности информационной инфраструктуры;

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

6) требования к проведению анализа информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах;

7) требования к средствам криптографической защиты информации;

8) требования к обеспечению информационной безопасности при доступе третьих лиц к информационным активам;

9) требования к проведению внутренних проверок состояния информационной безопасности;

10) требования к процессам системы управления информационной безопасностью.

Глава 2. Требования к организации системы управления информационной безопасностью

4. Банк, организация обеспечивают создание и функционирование 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, допускающую 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.

В организации допускается осуществление функций подразделений, указанных в подпунктах 4), 5), 6), 7), 8), 9), 10) и 11) настоящего пункта, ответственными работниками.

8. Банк, организация при создании и функционировании системы управления информационной безопасностью обеспечивают независимость подразделений 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 доступу к создаваемой, хранимой и обрабатываемой информации в информационных системах банка, организации и мониторинг информации и доступа к ней;

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 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.

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

12. 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 при необходимости представители других подразделений банка, организации. Руководителем коллегиального органа назначается руководитель исполнительного органа банка, организации либо член исполнительного органа банка, организации, курирующий деятельность подразделения по информационной безопасности.

13. 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 решения 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 ограничения по использованию привилегированных учетных записей;

10) организует и проводит мероприятия по обеспечению осведомленности работников банка, организации в вопросах 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.

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

15. Банк, организация определяют возможность делегирования другим подразделениям следующих функций подразделения по информационной безопасности:

1) внедрение и администрирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности банка, организации – подразделению по информационным технологиям;

2) организация и проведение мероприятий по обеспечению осведомленности работников банка, организации в вопросах информационной безопасности – подразделению по работе с персоналом;

3) учет и обработка событий и инцидентов информационной безопасности, связанных с нарушениями состояния информационной безопасности – подразделению по безопасности или отдельно выделенному подразделению обработки инцидентов информационной безопасности, независимому от подразделения по информационным технологиям.

16. Подразделение по информационным технологиям осуществляет следующие функции:

1) разрабатывает схемы информационной инфраструктуры банка, организации;

2) обеспечивает предоставление доступа пользователям 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 конфигурирование системного и прикладного программного обеспечения банка, организации;

4) обеспечивает исполнение установленных 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. 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.

18. 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.

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

20. Подразделение по комплаенс-контролю совместно с юридическим подразделением банка, организации определяет виды информации, подлежащие включению в перечень защищаемой информации, предусмотренный пунктом 10 Требований.

21. 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.

22. Подразделение по управлению рисками информационной безопасности осуществляет функции, предусмотренные в приложении 2 к Правилам формирования системы управления рисками и внутреннего контроля для банков второго уровня, утвержденным постановлением Правления Национального Банка Республики Казахстан от 26 февраля 2014 года № 29, зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 9322.

23. 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.

24. Бизнес-владельцы информационных систем или подсистем:

1) отвечают за соблюдение требований к информационной безопасности при создании, внедрении, модификации, предоставлении клиентам продуктов и услуг;

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

25. 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 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.

26. 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.

27. 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).

28. Информация 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.

29. Информация 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.

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

Глава 3. Требования к категорированию информационных активов

31. Банк, организация осуществляют категорирование информационных активов путем разделения их на критичные и некритичные на основании максимального уровня критичности хранимой и обрабатываемой в них информации.

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

33. Банк, организация обеспечивают информационную безопасность информационных активов, отнесенных к категории критичных в соответствии с Требованиями.

34. Методы и средства защиты информационных активов, отнесенных к категории некритичных, определяются банком, организацией самостоятельно.

35. При определении защищаемой информации банк, организация производят ее категорирование на основе оценки возможного ущерба путем разделения на критичную и некритичную в порядке, определенном внутренним документом банка, организации, регламентирующим процесс категорирования информации.

Глава 4. Требования к организации доступа к информационным активам

36. Предоставление физического доступа к информационным активам банка, организации осуществляется в соответствии с внутренними документами банка.

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

38. Предоставление доступа к информационным системам банка, организации, отнесенным к категории критичных информационных активов (далее – критичные информационные системы), производится путем формирования и внедрения ролей для обеспечения соответствия прав доступа пользователей информационных систем их функциональным обязанностям. Совокупность таких ролей представляет собой матрицу доступа к информационной системе, которая формируется банком, организацией в электронной форме или на бумажном носителе.

39. Процесс создания и использования матриц доступа в информационные системы банка, организации определяется внутренними документами банка, организации, регламентирующими процесс управления доступом к информационным системам, разработанными в соответствии с главой 11 Требований.

40. 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:

посредством ввода пары «учетная запись (идентификатор) – пароль» или с применением способов двухфакторной аутентификации;

с использованием способов биометрической и (или) криптографической и (или)

аппаратной аутентификации.

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

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

43. В информационных системах банка, организации применяются функции по управлению учетными записями и паролями, а также блокировке учетных записей пользователей, определяемые внутренним документом банка, организации, разработанным в соответствии с главой 11 Требований.

Глава 5. Требования к обеспечению безопасности информационной инфраструктуры

44. Подразделение по информационным технологиям банка, организации разрабатывает внутренние документы банка, организации, определяющие:

1) общую схему информационной инфраструктуры с указанием физического расположения ее элементов;

2) перечень ответственных администраторов узлов информационной инфраструктуры (телекоммуникационных устройств, серверов и размещенных на них операционных систем, систем управления базами данных и приложений).

45. ИТ-менеджер информационной системы по согласованию с подразделением по информационной безопасности разрабатывает внутренние документы банка, организации, определяющие типовые настройки:

1) операционных систем;
2) систем управления базами данных;
3) телекоммуникационных устройств;
4) информационных систем;
5) узлов и конечных точек информационной инфраструктуры, рабочих станций и мобильных устройств.

46. Подразделение по информационной безопасности обеспечивает организацию системы контроля изменения настроек безопасности и целостности системных и конфигурационных файлов, а также журналов аудиторского следа в критичных информационных системах.

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

48. Для каждой информационной системы или подсистемы определяется бизнес-владелец. Для инфраструктурных информационных систем бизнес-владельцем является подразделение по информационным технологиям.

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

50. Обеспечение безопасности информационных систем банка, организации в процессе разработки и эксплуатации осуществляется в соответствии с главой 11 Требований.

51. Банк, организация обеспечивают резервное хранение данных критичных 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 критичных

информационных систем из резервных копий определяются внутренним документом банка, организации.

52. Банк, организация обеспечивают антивирусную защиту информационной инфраструктуры в порядке, установленном внутренним документом банка, организации, разработанном в соответствии с главой 11 Требований.

53. Порядок обеспечения физической безопасности центров обработки данных банка, организации определяется внутренним документом банка, организации, разработанных в соответствии с главой 11 Требований.

54. На рабочие станции и корпоративные мобильные устройства работников банка, организации устанавливаются программное обеспечение, необходимое для исполнения функциональных обязанностей.

55. Перед вводом в эксплуатацию в банке, организации программное обеспечение проходит проверку в подразделении по информационной безопасности на предмет соответствия программного обеспечения требованиям к информационной безопасности банка, организации.

56. Банком, организацией определяется перечень программного обеспечения и оборудования, разрешенных к использованию в банке, организации. Программное обеспечение включается в перечень после проведения проверки в соответствии с пунктом 55 Требований.

57. Внутренними документами банка, организации определяются организационные и технические меры, обеспечивающие защиту рабочих станций и мобильных устройств банка, организации, а также носителей информации и сетевых ресурсов в соответствии с главой 11 Требований.

Глава 6. Требования к осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности

58. Банком, организацией проводится мониторинг деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности.

59. Банком, организацией проводится мониторинг событий информационной безопасности и управление инцидентами информационной безопасности.

Подразделение банка, организации, осуществляющее мониторинг, наделяется полномочиями по введению дополнительных контролей, частичную или полную остановку бизнес-процесса в случае выявления инцидента информационной безопасности.

60. Банком, организацией определяются перечень событий информационной безопасности, подлежащих мониторингу, источники событий, периодичность, правила мониторинга и их методы.

61. Перечень событий информационной безопасности, подлежащих мониторингу, источники событий, периодичность, правила мониторинга и их методы пересматриваются банком, организацией не реже одного раза в год с учетом имеющейся статистики и эффективности мониторинга.

62. Банком, организацией определяется порядок отнесения события информационной безопасности к инцидентам информационной безопасности.

63. Порядок управления инцидентами информационной безопасности определяется внутренним документом банка, организации, разработанным в соответствии с главой 11 Требований.

Глава 7. Требования к проведению анализа информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах

64. По результатам обработки инцидента информационной безопасности проводится всесторонний анализ причин возникновения инцидента информационной безопасности, его механизма и последствий. При сборе технических данных с программно-технических средств, вовлеченных в инцидент информационной безопасности, обеспечивается сохранность и неизменность собранных данных.

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

66. Для инцидентов информационной безопасности, вероятность возникновения которых высока и не может быть снижена в короткие сроки, разрабатываются документы, описывающие алгоритм обработки таких инцидентов информационной безопасности, типовых неотложных мер по локализации инцидента информационной безопасности и его последствий, методов обработки инцидента информационной безопасности.

67. Результаты анализа инцидентов информационной безопасности, а также рекомендации по минимизации вероятности возникновения инцидентов информационной безопасности и их возможного ущерба ежегодно выносятся на рассмотрение коллегиального органа и в дальнейшем используются для оценки рисков информационной безопасности, корректировки методов и средств обеспечения информационной безопасности, изменения бизнес-процессов.

Глава 8. Требования к средствам криптографической защиты информации

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

69. Банк, организация утверждают внутренний документ, регламентирующий порядок использования средств криптографической защиты информации в соответствии с главой 11 Требований, а также 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.

Глава 9. Требования к обеспечению информационной безопасности при доступе третьих лиц к информационным активам

70. Внутренним документом банка, организации предусматриваются требования к информационной безопасности при доступе к информационным активам третьих лиц, не являющихся работниками банка, организации (далее – третьи лица).

71. Доступ третьих лиц к информационным активам банка, организации предоставляется на период и в объеме, необходимых для проведения работ на основании соглашения о соблюдении требований к информационной безопасности, за исключением случаев, предусмотренных законодательством Республики Казахстан. В соглашениях о соблюдении требований к информационной безопасности, 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 вмешательством третьих лиц.

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

73. На основании проведенной оценки риска предусматриваются следующие организационные и (или) программно-технические меры по контролю деятельности третьих лиц:

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 специальными программно-техническими комплексами.

74. В случае передачи третьим лицам части информационных активов банка, организации (размещение серверных мощностей в сторонних центрах обработки данных, использование облачных сервисов) предпринимаются следующие меры обеспечения информационной безопасности:

1) отражение в соответствующем договоре с третьим лицом условий о возмещении ущерба, возникшего вследствие нарушения информационной безопасности и работоспособности информационных систем;

2) исключение возможности доступа третьих лиц к информации, которая не может быть передана им 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 10. Требования к проведению внутренних проверок состояния информационной безопасности

75. Состояние информационной безопасности оценивается путем проведения проверок деятельности структурных подразделений:

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.

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

Глава 11. Требования к процессам системы управления информационной безопасностью

Параграф 1. Требования к процессу организации доступа к информационным системам

77. Процесс создания матрицы доступа к информационной системе состоит из следующих этапов:

1) инициирование процесса – инициатором создания матрицы доступа к информационной системе банка, организации является бизнес-владелец информационной системы;

2) владелец бизнес-процесса описывает и формализует функции, автоматизированные в информационной системе, в разрезе каждой роли, с учетом мер по предотвращению предоставления конфликтующих прав доступа, позволяющих обойти

существующие автоматизированные контроли;

3) формализованные функции согласовываются с бизнес-владельцем информационной системы;

4) бизнес-владелец информационной системы готовит техническое задание на разработку ролей в информационной системе;

5) подразделение, ответственное за поддержку информационной системы, разрабатывает подсистему, реализующую роли в информационной системе;

6) бизнес-владелец информационной системы и другие заинтересованные подразделения тестируют созданные роли;

7) подразделение, ответственное за поддержку информационной системы, внедряет роли в информационной системе.

78. Внесение изменений и дополнений в матрицу доступа к информационной системе осуществляется в порядке, установленном пунктом 77 Требований, по инициативе участника автоматизируемого бизнес - процесса.

79. Подсистема управления доступом критичной 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 по согласованию с бизнес-владельцем информационной системы и уведомлением подразделения по информационной безопасности;

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

5) поддержку индивидуальных, групповых, территориальных ограничений на доступ к информационной системе;

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

7) возможность блокирования одновременного доступа под разными учетными данными в одну информационную систему с одного аппаратного средства (компьютера);

8) ведение аудиторского следа.

80. Подсистема управления доступом к данным критичной информационной системы банка, организации включает:

1) обеспечение пользователям доступа к данным информационной системы только через приложение;

2) предоставление выделенным пользователям доступа к данным информационной системы напрямую, минуя приложение. Перечень пользователей информационных систем утверждается членом исполнительного органа банка, организации, курирующим подразделение по информационной безопасности.

81. При изменении функциональных обязанностей работника отключаются все имеющиеся права доступа, и присваиваются новые права доступа, соответствующие его новым функциональным обязанностям. При увольнении работника отключаются все его права доступа в информационные системы. При длительном отсутствии работника на рабочем месте его доступ в информационную систему блокируется в порядке, установленном внутренним документом банка, организации.

82. Подразделением по информационной безопасности производится проверка соответствия прав доступа к информационным системам матрице доступа, а также контроль отключения прав доступа уволенным работникам и блокирования доступа длительно отсутствующим работникам.

83. Банк, организация актуализируют матрицу доступа к информационной системе в порядке, установленном внутренними документами банка, организации, регламентирующими порядок управления доступом к информационным системам. Пересмотр прав доступа к информационным системам производится бизнес-владельцами информационных систем с привлечением заинтересованных подразделений.

84. При отсутствии технической возможности реализации одного или нескольких требований настоящей главы 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

85. 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 (возможно и более раннее предупреждение пользователя). 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 должна запросить 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 с возможностью разблокировки только при вводе аутентификационных данных пользователя.

86. Требования пункта 85 Требований не применяются в случаях, когда:

1) информационная система интегрирована в части аутентификации с информационной системой, соответствующей требованиям пункта 85 Требований;

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

87. Банк, организация разрабатывают внутренний документ, регламентирующий процесс управления учетными записями и паролями, который определяет:

1) описание полномочий администраторов информационных систем по управлению учетными записями пользователей информационных систем и смене их паролей;

2) порядок подачи и рассмотрения заявок на создание учетных записей, а также изменения пароля при возникновении нештатной ситуации;

3) порядок подачи заявок на изменение или удаление учетных записей;

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

5) запрет на передачу паролей третьим лицам, включая администраторов информационных систем и иных работников банка, организации;

6) запрет работы в информационных системах под чужими учетными записями (в целях обеспечения непрерывности деятельности по согласованию с подразделением по информационной безопасности допускается в указанный промежуток времени использование чужой учетной записи, при этом обеспечивается точная идентификация пользователя).

Параграф 3. Требования к процессу обеспечения безопасности информации

88. Порядок защиты информации при использовании Интернета и электронной почты определяется внутренним документом банка, организации с применением любого из следующих методов, включая, но не ограничиваясь ими:

1) организационный: ограничения, установленные внутренними документами банка, организации, 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 внутренними документами банка, организации, 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.

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

1) организационный: ограничения, установленные внутренними документами банка, организации, 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.

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

1) организационный: ограничения, установленные внутренними документами банка, организации, обеспечение осведомленности персонала, ограничение количества работников, имеющих доступ к работе с документами, содержащими информацию;

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

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

1) организационный: ограничения, установленные внутренними документами банка, организации, 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.

92. Уничтожение 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

93. Банком, организацией определяются периметр защиты информационной 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.

94. Телекоммуникационные соединения, за исключением соединений с городской телефонной сетью, выходящие за периметр защиты, а также соединения между территориально удаленными сетями и устройствами банка, организации, используемые для передачи критичной информации, подлежат шифрованию.

95. При использовании беспроводных соединений шифрование производится методами, отличными от методов шифрования, предоставляемых протоколом беспроводного соединения.

96. Допускается шифрование передаваемой информации взамен шифрования соединения.

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

98. Правила доступа, установленные на межсетевых экранах, настраиваются на разрешение только тех соединений, которые необходимы для функционирования бизнес-процессов банка, организации. Указанные правила согласовываются с подразделением по информационной безопасности. Для выявления и отражения атак на периметр защиты используются средства обнаружения и предотвращения вторжений.

99. 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 (договоры с провайдерами телекоммуникационных услуг, установка специализированных систем, имеющих соответствующий функционал по защите от атак данного типа, и другие способы).

100. Доступ 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 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»).

101. 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.

102. Конфигурация средств обеспечения безопасности периметра защиты выполняется с учетом рекомендаций производителей и пересматривается с периодичностью, определенной внутренними документами банка, организации. В обязательном порядке изменяются пароли на предустановленные учетные записи. При отсутствии необходимости учетные записи блокируются или удаляются.

103. С периодичностью, определенной внутренними документами банка, организации, 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

104. ИТ-менеджер информационной системы централизовано синхронизирует все узлы информационной инфраструктуры по времени с эталонным источником.

105. 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.

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

107. 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.

108. При размещении на одном сервере или гипервизоре нескольких информационных систем, обеспечивается защита на уровне, соответствующем максимально критичной информационной системе, размещенной на данном сервере или гипервизоре.

Параграф 6. Требования к процессу обеспечения защиты информационных систем

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

110. 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.

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

112. 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.

113. 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.

114. 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.

115. Защищенный депозитарий программного обеспечения, в котором хранятся эталонные исходные коды (при наличии) и исполняемые модули информационных систем, ведется в удобном для восстановления виде.

116. 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 сбора, консолидации и хранения информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах

117. Информация об инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности, подлежит консолидации, систематизации и хранению.

118. Срок хранения информации об инцидентах информационной безопасности составляет не менее 5 (пяти) лет.

119. В случае, если банком, организацией определена необходимость мониторинга отдельных источников событий информационной безопасности во внерабочее время, создается круглосуточная служба мониторинга.

120. Банком, организацией определяется порядок информирования о произошедшем инциденте информационной безопасности руководящих работников и подразделений банка, организации.

121. Банком, организацией определяется порядок принятия неотложных мер к устранению инцидента информационной безопасности, его причин и последствий.

122. В банке, организации ведется журнал учета инцидентов информационной безопасности с отражением всей информации об инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах, на бумажном носителе либо в электронном виде.

Параграф 8. Требования к процессу работы с персоналом

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

124. При приеме на работу нового работника, не позднее 5 (пяти) рабочих дней с момента приема на работу, он ознакамливается под роспись 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.

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

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

127. 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

внесенными в них изменениями и дополнениями;

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

3) иные методы, определенные банком, организации.

128. 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 праве банка, организации осуществлять мониторинг любой информации, создаваемой, хранимой и обрабатываемой в информационных системах банка, организации;

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

129. 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 два года для каждого работника).

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

1) приему - передаче документов;

2) сдаче удостоверений, пропусков и других разрешительных документов;

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

4) блокировке или удалению учетных записей в информационных системах.

Параграф 9. Требования к процессу ведения аудиторского следа в информационных системах

131. В информационных системах используется функция ведения аудиторского следа, которая отражает следующее:

1) события установления соединений, идентификации, аутентификации и авторизации в информационной системе (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.

132. 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 (CREATE, INSERT, UPDATE, DELETE и другие);

6) результат действия (успешно или не успешно).

133. Срок хранения аудиторского следа составляет не менее 3 (трех) месяцев в

оперативном доступе и не менее 1 (одного) года в архивном доступе. Допускается агрегированное хранение аудиторского следа нескольких информационных систем в специализированной информационной системе хранения, обработки и анализа событий.

134. Банк, организация обеспечивают неизменность аудиторского следа как на организационном, так и на техническом уровне. Администраторам информационных систем предоставляется доступ только на перенос журналов аудиторского следа в архив.

Параграф 10. Требования к процессу обеспечения антивирусной защиты

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

136. 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 виртуальных сред – использование антивирусным программным обеспечением встроенных функций безопасности виртуальных сред (балансировка нагрузки, централизованная установка и проверка на уровне гипервизора и другие функции), 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.

137. 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.

138. Выбор антивирусного программного обеспечения проводится подразделением по информационным технологиям при обязательном участии подразделения по информационной безопасности в порядке, установленном внутренними документами банка, организации.

Внутренние документы банка, организации определяют ответственные структурные подразделения, участвующие в процессе обеспечения антивирусной защиты (установка, сопровождение, мониторинг состояния антивирусного программного обеспечения и реагирование на вирусные атаки).

139. Антивирусное программное обеспечение максимально исключает прерывание пользователем всех служебных процессов (сканирование по расписанию, обновление и

другие процессы). Обновление антивирусного программного обеспечения производится не реже одного раза в сутки, полное сканирование компьютера – не реже одного раза в неделю.

Параграф 11. Требования к процессу управления обновлениями и уязвимостями информационных систем

140. Подразделение по информационным технологиям отслеживает обновления информационных систем и определяет порядок управления обновлениями информационных систем, по согласованию с подразделением по информационной безопасности.

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

142. Обновления информационных систем до установки в промышленную среду проходят испытания в тестовой среде.

143. Подразделение по информационной безопасности проводит сканирование (технический анализ защищенности) информационных систем на наличие уязвимостей с использованием специализированного программного обеспечения (далее - сканирование). Сканирование проводится на плановой основе не реже одного раза в год для каждой информационной системы. Сканирование проводится работниками банка, организации и (или) внешними специализированными компаниями. Результаты сканирования формируются в виде отчета о состоянии информационной безопасности с указанием рекомендаций о необходимых корректирующих и превентивных мерах по устранению выявленных уязвимостей.

144. Банк, организация предпринимают необходимые меры по устранению выявленных уязвимостей.

По окончании работ по устранению уязвимостей проводится повторное сканирование информационной системы, подтверждающее устранение ранее выявленных уязвимостей.

Параграф 12. Требования к процессу использования средств криптографической защиты информации

145. Подразделение по информационным технологиям по согласованию с подразделением по информационной безопасности разрабатывает внутренний документ банка, организации, регулирующий применение средств криптографической защиты информации, включающий в себя как минимум:

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;

8) перечень лиц, допущенных к работе со средствами криптографической защиты информации в качестве пользователей.

Параграф 13. Требования к процессу обеспечения физической безопасности центров обработки данных

146. 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.

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

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

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

150. 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.

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

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

153. 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.

Параграф 14. Требования к процессу обеспечения защиты рабочих станций и мобильных устройств работников

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

155. Предоставление пользователям прав локального администратора или аналогичных прав запрещается, за исключением случаев, когда такие права необходимы для функционирования программного обеспечения, автоматизирующего функции, исполняемые пользователем.

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

157. Перечень пользователей, указанных в пунктах 155 и 156 Требований, формируется, актуализируется и утверждается руководителем подразделения по информационным технологиям по согласованию с подразделением по информационной

безопасности. В случае предоставления пользователям дополнительных прав в соответствии с пунктами 155 и 156 Требований подразделение по информационной безопасности осуществляет контроль их использования.

158. Система учета рабочих станций и мобильных устройств в корпоративной сети банка, организации позволяет точно идентифицировать местонахождение данной рабочей станции или принадлежность мобильного устройства. Система учета формируется в электронном виде либо на бумажном носителе.

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

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

161. Вся информация банка, организации, размещенная на мобильных устройствах, хранится в зашифрованном виде.

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

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 подпунктом 86-1) части второй статьи 15 Закона Республики Казахстан от 30 марта 1995 года «О Национальном Банке Республики Казахстан», пунктом 7 статьи 61-5 Закона Республики Казахстан от 31 августа 1995 года «О банках и банковской деятельности в Республике Казахстан» и определяют порядок и сроки предоставления банками 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 следующие понятия:

1) информация об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах – 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;

2) инцидент информационной безопасности, включая нарушения, сбои в информационных системах (далее - 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;

3) информационная безопасность – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

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

5) информационно-коммуникационная инфраструктура банка, организации (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;

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, несущих угрозу стабильности деятельности банка, организации.

Информация об инцидентах информационной безопасности, указанных в настоящем пункте, предоставляется банком или организацией незамедлительно в виде карты инцидента информационной безопасности по форме, согласно приложению к Правилам.

На каждый инцидент информационной безопасности заполняется отдельная карта инцидента информационной безопасности.

4. Банк, организация проводят анализ выявленных инцидентов информационной безопасности в соответствии с внутренними документами, по результатам которого ежеквартально, не позднее 30 (тридцатого) числа месяца, следующего за отчетным кварталом, представляют в уполномоченный орган в произвольной форме информацию по обработанным инцидентам информационной безопасности, включающую следующие сведения:

1) дата и время регистрации инцидента информационной безопасности;

2) дата и время, когда произошел инцидент информационной безопасности;

3) описание инцидента информационной безопасности;

4) категория инцидента информационной безопасности;

5) сумма ущерба (в тенге);

6) фамилия, имя отчество (при его наличии) ответственного за обработку (сбор, анализ, принятие корректирующих мер) инцидента информационной безопасности;

7) краткое описание выполненных действий по инциденту информационной безопасности;

8) статус инцидента информационной безопасности (дата и время закрытия инцидента информационной безопасности).

Информация по обработанным инцидентам информационной безопасности представляется в электронном формате с использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых данных.

Приложение
к Правилам и срокам предоставления
информации об инцидентах информационной
безопасности, включая сведения о нарушениях,
сбоях в информационных системах

форма

Карта инцидента информационной безопасности

№	Общие сведения	
	Характеристики инцидента информационной безопасности	Информация об инциденте информационной безопасности
1	Наименование инцидента информационной безопасности	
2	Дата и время выявления (дд.мм.гггг и чч:мм с указанием часового пояса UTC+X)	
3	Место выявления (организация, филиал, сегмент информационной инфраструктуры)	
4	Источник информации об инциденте информационной безопасности (пользователь, администратор, администратор информационной безопасности, работник подразделения информационной безопасности или техническое средство)	
5	Использованные методы при реализации инцидента информационной безопасности (социальная инженерия, внедрение вредоносного кода)	
Содержание инцидента информационной безопасности		
6	Симптомы, признаки инцидента информационной безопасности	
7	Основные события (эксплуатация уязвимостей в прикладном и системном программном обеспечении; несанкционированный доступ в информационную систему; атака «отказ в обслуживании» на информационную систему или сеть передачи данных; заражение сервера вредоносной программой или кодом; совершение несанкционированного перевода денежных средств; иные инциденты информационной безопасности, несущие угрозу стабильности деятельности банка, организации)	
8	Пораженные активы (физический уровень информационной инфраструктуры, уровень сетевого оборудования, уровень сетевых приложений и сервисов, уровень операционных систем,	

	уровень технологических процессов и приложений и уровень бизнес-процессов банка, организации)	
9	Статус инцидента информационной безопасности (свершившийся инцидент информационной безопасности, попытка осуществления инцидента информационной безопасности, подозрение на инцидент информационной безопасности)	
10	Ущерб	
11	Источник угрозы (выявленные идентификаторы)	
12	Преднамеренность (намеренный, ошибочный)	
Предпринятые меры по инциденту информационной безопасности		
13	Предпринятые действия (идентификация уязвимости, блокирование, восстановление и иное)	
14	Запланированные действия	
15	Оповещенные лица (фамилия, имя, отчество (при его наличии) должностных лиц, наименование государственных органов, организаций)	
16	Привлеченные специалисты (фамилия, имя, отчество (при его наличии) место работы, должность)	

Руководитель подразделения по информационной безопасности

_____ _____

(фамилия, имя, отчество (при его наличии) (подпись)

Дата _____