УТВЕРЖДЕНО

Постановление Правления
Национального банка
Республики Беларусь

29.12.2025 № 390

СТАНДАРТ ФИНАНСОВЫХ УСЛУГ И ТЕХНОЛОГИЙ

СФУТ 9.03-2025 ”Банковская деятельность.
Обеспечение информационной безопасности.
Общие требования“

РАЗДЕЛ I
ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящий стандарт финансовых услуг и технологий (далее – стандарт) распространяется на банки, небанковские кредитно-финансовые организации и открытое акционерное общество ”Банк развития Республики Беларусь“ (далее – банки) и устанавливает общие требования по обеспечению информационной безопасности (далее – ИБ) в банках.

2. Настоящий стандарт предназначен для применения путем включения ссылок на него и (или) устанавливаемых в нем требований в локальные правовые акты банков, а также в договоры.

3. При применении настоящего стандарта необходимо соблюдать требования законодательства, в том числе нормативных правовых актов Национального банка и обязательных для соблюдения требований технических нормативных правовых актов (далее – ТНПА).

4. Настоящий стандарт применяется при проектировании, построении, аудите системы информационной безопасности (далее – СИБ) и системы менеджмента информационной безопасности (далее – СМИБ) банков.

5. В настоящем стандарте используются термины в значениях, установленных в нормативных правовых актах Национального банка, стандартах финансовых услуг и технологий СФУТ 9.01-2024 ”Банковская деятельность. Обеспечение информационной безопасности. Общие положения и терминология“ и СФУТ 9.02-2024 ”Банковская деятельность. Обеспечение информационной безопасности. Требования к документации по обеспечению деятельности в области информационной безопасности“, утвержденных постановлением Правления Национального банка Республики Беларусь от 20 июня 2024 г. № 185.

РАЗДЕЛ II
ТРЕБОВАНИЯ К СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

6. Выполнение требований к СИБ банков является основой для обеспечения необходимого и достаточного уровня ИБ.

7. Формирование требований к СИБ банков проводится на основе положений настоящего стандарта. Требования к СИБ банков оформляются документально в соответствии со стандартом финансовых услуг и технологий СФУТ 9.02-2024 ”Банковская деятельность. Обеспечение информационной безопасности. Требования к документации по обеспечению деятельности в области информационной безопасности“ .

8. В настоящем стандарте определены базовые требования к СИБ. В случае необходимости, а также с учетом особенностей деятельности отдельных банков данные требования могут быть уточнены в локальных правовых актах банков.

9. При технической невозможности или экономической нецелесообразности реализации отдельных требований к СИБ на этапе проектирования СИБ разрабатываются компенсирующие меры, направленные на нейтрализацию угроз ИБ. Банком обосновывается применение таких мер.

10. Использование средств криптографической защиты информации (далее – СКЗИ) осуществляется в соответствии с законодательством и (или) правилами платежных систем. Работы по обеспечению защиты информации с использованием средств технической и криптографической защиты информации проводятся в соответствии с требованиями законодательства, программной и эксплуатационной документацией на средства защиты информации.

ГЛАВА 2
БАЗОВЫЕ ТРЕБОВАНИЯ К СИБ

11. Базовые требования к СИБ реализуются по следующим направлениям:

обеспечение антивирусной защиты;

обеспечение безопасной разработки программного обеспечения (далее – ПО);

обеспечение безопасности автоматизированных рабочих мест (далее – АРМ);

обеспечение безопасности при работе с глобальной компьютерной сетью Интернет (далее – сеть Интернет);

обеспечение безопасности серверного оборудования;

обеспечение безопасности среды виртуализации;

обеспечение ИБ автоматизированной банковской системы (далее – АБС) на стадиях ее жизненного цикла;

обеспечение криптографической защиты информации с применением СКЗИ;

обеспечение физической безопасности;

обучение и повышение осведомленности по вопросам ИБ;

предотвращение утечек конфиденциальной информации;

управление доступом;

управление событиями и инцидентами ИБ;

управление уязвимостями.

12. В случае выявления событий ИБ, при которых временно отсутствует техническая возможность применения базовых требований к СИБ, банком обеспечивается выполнение уполномоченным персоналом мероприятий по обеспечению непрерывной работы и восстановления работоспособности информационных систем (далее – ИС) в соответствии с планом обеспечения непрерывной работы и восстановления (далее – ПОНРВ).

13. Базовые требования к СИБ сформированы с учетом требований, установленных законодательством в области ИБ и международными стандартами.

14. При оценке СИБ банка используются только базовые требования к СИБ.

ГЛАВА 3
ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ АНТИВИРУСНОЙ ЗАЩИТЫ

15. На всех АРМ и серверах АБС, если иное не предусмотрено банковским технологическим процессом, применяются средства антивирусной защиты. Банком определяются, выполняются, регистрируются и контролируются процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на АРМ и серверах АБС.

При обеспечении антивирусной защиты используются средства антивирусной защиты, имеющие сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной

экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь.

16. Функционирование средств антивирусной защиты организовывается в автоматическом режиме на постоянной основе без возможности их отключения (за исключением лиц, осуществляющих администрирование средств антивирусной защиты). Установки обновлений антивирусного программного обеспечения и его баз данных осуществляются в автоматическом или ручном режиме.

Банком определяются, внедряются, выполняются, регистрируются и контролируются процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных), а также контроля за отключением антивирусных средств, на всех технических средствах АБС. При этом администрирование средств антивирусной защиты проводится от имени специальных учетных записей в соответствии с рекомендациями разработчика средств антивирусной защиты.

Контроль за установкой и функционированием средств антивирусной защиты возлагается на подразделение ИБ.

17. Полное сканирование АРМ и серверов (в случае технической возможности без нарушения технологических процессов) обеспечивается на регулярной (не менее 1 раза в месяц) основе в период их низкой загрузки и (или) в нерабочее время.

18. При подключении съемных машинных носителей информации (далее – МНИ) к средствам вычислительной техники (далее – СВТ) перед началом использования проводится их антивирусная проверка, как правило, на АРМ, не используемом в банковском технологическом процессе.

19. Документально определяются и выполняются процедуры предварительной проверки устанавливаемого или изменяемого ПО на отсутствие вирусов. После установки или изменения программного обеспечения выполняется антивирусная проверка. Данные о результатах установки, изменения программного обеспечения и антивирусной проверки хранятся не менее одного года.

20. Разрабатываются и вводятся в действие инструкции и рекомендации по защите от вредоносного программного обеспечения (далее – ВПО), учитывающие особенности банковских технологических процессов.

21. До клиентов банка доводятся рекомендации по защите информации от воздействия ВПО.

22. Реализуется защита от вредоносного кода на уровне контроля общедоступных объектов доступа (в том числе банкоматов, платежных терминалов).

23. Банком организуется проверка всего входящего трафика на наличие вредоносного кода потоковым антивирусом (за исключением зашифрованного трафика, а также трафика, передаваемого в специально организованных с платежными системами технологических каналах).

24. Определяются, внедряются, регистрируются и контролируются процедуры, выполняемые в случае обнаружения ВПО, в которых, в частности, необходимо фиксировать:

необходимые меры по отражению и устранению последствий вирусной атаки;

порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки).

25. Обязанности работников банка, имеющих доступ к АРМ и (или) АБС, по выполнению мер антивирусной защиты предусматриваются локальными правовыми актами по организации антивирусной защиты.

ГЛАВА 4
ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАЗРАБОТКИ ПО

26. Процессы безопасной разработки ПО осуществляются на плановой основе.

27. На этапе разработки ПО разработчик формирует и предъявляет требования безопасности к разрабатываемому ПО, а заказчик эти требования согласовывает.

28. Проектирование архитектуры ПО осуществляется разработчиком с учетом результатов моделирования угроз безопасности информации.

29. Разработчик ПО формирует и поддерживает в актуальном состоянии правила написания исходного кода.

30. При разработке ПО осуществляется:

управление доступом к исходному коду. Доступ к исходному коду программ ограничивается.

контроль целостности исходного кода.

31. Экспертиза исходного кода вновь разрабатываемого ПО проводится как в отношении собственного разработанного кода, так и в отношении кода, заимствованного у сторонних разработчиков ПО. Экспертиза исходного кода осуществляется одним из следующих способов или их комбинацией:

самостоятельно банком;

разработчиком ПО;

третьей стороной на основе договорных отношений.

В случае проведения экспертизы разработчиком ПО или третьей стороной на основе договорных отношений, ее результаты передаются банку.

По результатам экспертизы исходного кода ПО, в случае необходимости, проводится доработка ПО.

32. При выполнении тестирования ПО разработчик реализовывает:

функциональное тестирование ПО;

нефункциональное тестирование ПО;

тестирование на проникновение;

фаззинг-тестирование ПО.

33. При разработке ПО используется безопасная система сборки ПО и обеспечивается безопасность сборочной среды ПО.

34. Среда разработки, тестирования и рабочая среда отделяются друг от друга для снижения рисков несанкционированного доступа (далее – НСД) или изменений в рабочей среде.

35. Разработчик ПО соответствующим образом защищает безопасные среды разработки и интеграции ПО, охватывающие весь цикл разработки.

36. В ходе разработки ПО обеспечивается безопасность информации, распространение и (или) предоставление которой ограничено, в том числе путем применения в соответствии с законодательством средств криптографической защиты информации или иными методами.

ГЛАВА 5
ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ АРМ

37. Банком разрабатывается и внедряется политика безопасности, определяющая правила работы с информацией и ресурсами АРМ.

38. На АРМ исключается возможность доступа пользователей к настройкам BIOS (базовая система ввода-вывода) или UEFI (унифицированный расширяемый микропрограммный интерфейс).

39. Банком разрабатываются и внедряются механизмы идентификации и авторизации пользователей АРМ, в том числе с использованием многофакторной аутентификации (для АРМ, попадающих в область действия стандарта индустрии платежных карт PCI DSS, а также на АРМ работников, используемых для администрирования АБС банка). Возможность работы на АРМ неавторизованных пользователей исключается.

40. Разрабатываются, внедряются и контролируются правила генерации и смены паролей пользователей АРМ.

41. Хранение аутентификационных данных в открытом виде на АРМ и в АБС не допускается. Для защиты аутентификационных данных на

АРМ используются методы шифрования, а также их хранение на специальном сервере аутентификации.

42. После истечения установленного времени бездействия (неактивности) пользователя АРМ или по его запросу обеспечивается блокировка доступа к ресурсам АРМ.

43. Банком организовываются и выполняются процедуры разграничения прав доступа к информации и ресурсам АРМ в соответствии с должностными обязанностями работников.

44. В банке определяется, внедряется и контролируется порядок использования съемных МНИ. По умолчанию устанавливается запрет на несанкционированное подключение и использование съемных МНИ.

45. На АРМ, на которых обрабатывается информация, распространение и (или) предоставление которой ограничено, все операции с МНИ, такие как подключение, отключение, копирование файлов, регистрируются и контролируются с использованием программных и (или) аппаратных решений, направленных на защиту информации от несанкционированного доступа.

46. Исключается возможность неконтролируемого доступа лиц к аппаратной части АРМ, а также установки и (или) запуска пользователями АРМ не разрешенного для использования ПО. Одновременно определяется перечень разрешенного ПО и регламентируется порядок его установки и использования на АРМ.

47. На АРМ пользователей не допускается использование портов ввода-вывода информации, кроме минимально необходимых для выполнения служебных обязанностей. Ввод-вывод информации на АРМ контролируется с использованием программно-технических средств и (или) организационными мерами.

48. Доступ в помещения, где расположены АРМ, ограничивается (за исключением случаев их использования в банковском платежном технологическом процессе для оказания сервисов и услуг), а также принимаются меры по защите аппаратного обеспечения АРМ.

49. Процедуры контроля отсутствия размещения на устройствах, задействованных в осуществлении банковского платежного технологического процесса, находящихся в общедоступных местах вне зоны постоянного контроля, в том числе банкоматах и платежных терминалах, специализированных средств, используемых для несанкционированного съема информации, определяются, внедряются и контролируются.

50. В банке процедуры обслуживания АРМ, в том числе используемых в банковском платежном технологическом процессе, включая замену их программных и (или) аппаратных частей определяются, внедряются и контролируются.

51. На регулярной основе осуществляется обновление ПО, установленного на АРМ.

52. В банке на постоянной основе осуществляется проведение инструктажей и обучение работников по вопросам ИБ при работе на АРМ.

53. В банке осуществляется эффективный контроль за учетом АРМ, их использованием и функционированием.

ГЛАВА 6
ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С СЕТЬЮ ИНТЕРНЕТ

54. Доступ к сети Интернет предоставляется ограниченному кругу работников банка в целях выполнения ими служебных (должностных) обязанностей, требующих непосредственного подключения к внешним информационным ресурсам и сервисам.

55. Порядок использования сети Интернет с указанием целей такого использования устанавливается локальными правовыми актами банка.

Использование сети Интернет в неустановленных целях не допускается.

С целью ограничения нецелевого использования сети Интернет устанавливаются перечни ресурсов и сервисов, доступных для работников банка. Наделение работников банка правами на использование сети Интернет оформляется документально и выполняется в соответствии с их служебными (должностными) обязанностями и в соответствии с назначенными им ролями.

56. Банком документально определяется порядок подключения и использования ресурсов и сервисов сети Интернет.

Разрабатываются и вводятся в действие инструкции и регламенты по использованию сети Интернет, учитывающие особенности банковских технологических процессов.

Определяются и выполняются процедуры протоколирования посещения ресурсов и сервисов сети Интернет работниками банка. Работникам подразделения ИБ обеспечивается доступ к данным о посещенных работниками банка ресурсах и сервисах сети Интернет.

57. Доступ в сеть Интернет с АРМ, используемых для администрирования ИС банка, не допускается. В этом случае доступ осуществляется: с выделенных АРМ, VDI (технология виртуализации рабочих мест) и/или терминального приложения, размещенных в выделенном сегменте сети банка, не связанных с работой АБС и банковскими технологическими процессами (сегментация сети) с использованием средств защиты информации (далее – СЗИ) или иным

способом, не противоречащим законодательству в области защиты информации.

58. Передача информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, посредством сети Интернет осуществляется с применением СКЗИ.

Передача общедоступной информации с использованием сети Интернет осуществляется при условии обеспечения ее защиты от модификации (изменения), блокирования правомерного доступа к ней, недопущения ее уничтожения.

59. При осуществлении доступа к сети Интернет банком применяются средства защиты информации (межсетевые экраны, антивирусные средства, маршрутизаторы и коммутаторы, выполняющие функцию маршрутизации и др.), обеспечивающие прием и передачу информации в установленном формате и для конкретной технологии.

60. При осуществлении дистанционного банковского обслуживания применяются защитные меры, предотвращающие возможность подмены клиента, прошедшего авторизацию, злоумышленником в рамках сеанса работы. Все попытки таких подмен регистрируются в установленным банком порядке.

61. Операции клиентов в течение всего сеанса работы с системой дистанционного банковского обслуживания (далее – СДБО) выполняются после прохождения процедур идентификации, многофакторной аутентификации (криптографический токен и (или) средства выработки электронной цифровой подписи) и авторизации. В случае нарушения или разрыва соединения обеспечивается закрытие текущей сессии и повторное выполнение процедур идентификации, многофакторной аутентификации и авторизации.

Для доступа клиентов к СДБО используется специализированное клиентское ПО со встроенными механизмами защиты.

62. Обмен сообщениями электронной почты посредством сети Интернет осуществляется с использованием защитных мер, перечень и порядок применения которых должен быть определен документально.

Обмен сообщениями электронной почты организовывается путем использования внешнего (подключенного к сети Интернет) и внутреннего (подключенного к внутренним сетям банка) почтовых серверов с безопасной системой репликации почтовых сообщений между ними.

63. Все входящие и исходящие сообщения электронной почты архивируются. Целями создания архивов сообщений электронной почты являются:

контроль информационных потоков, в том числе с целью предотвращения утечек информации;

использование архивов при проведении разбирательств по фактам утечек информации.

Банком самостоятельно определяется срок хранения архивов сообщений электронной почты, но не менее одного года.

Определяются, выполняются, регистрируются и контролируются правила и процедуры доступа к информации архива и ее изменения, предусматривающие возможность доступа работникам подразделения ИБ к информации архива.

64. Хранение и обработка информации ограниченного распространения, не относящейся к государственным секретам, на СВТ с доступом в сеть Интернет определяется бизнес-целями банка и документально разрешается его руководством.

65. Определяется состав и порядок применения мер ИБ, применяемых при взаимодействии с сетью Интернет и позволяющих обеспечить противодействие атакам злоумышленников и распространению спама.

ГЛАВА 7
ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ СЕРВЕРНОГО ОБОРУДОВАНИЯ

66. Серверное оборудование размещается и защищается так, чтобы снизить риски, связанные с природными угрозами и опасностями, а также возможностью НСД.

67. Серверные помещения оборудуются системами пожарной сигнализации и автоматического пожаротушения.

68. В серверных помещениях для нормального функционирования серверного оборудования поддерживаются оптимальные температура и влажность с помощью систем кондиционирования и вентиляции.

69. Серверное оборудование защищается от перебоев в электроснабжении и других нарушений, вызванных перебоями в работе служб обеспечения.

70. Доступ в помещения, в которых размещается серверное оборудование, ограничивается и контролируется с применением систем контроля и управления доступом (далее – СКУД), видеонаблюдения.

71. Обеспечивается синхронизация временных меток и (или) системного времени серверного оборудования.

72. Реквизиты доступа к системному ПО серверного оборудования, установленные (используемые) по умолчанию, изменяются либо блокируется возможность их использования.

73. Доступ к ресурсам серверного оборудования предоставляется по принципу минимальной достаточности для выполнения служебных

обязанностей. Для доступа привилегированных пользователей к указанным ресурсам используется многофакторная аутентификация.

При эксплуатации сетей электросвязи общего пользования доступ к ресурсам серверного оборудования осуществляется с применением сертифицированных средств линейного шифрования.

74. Процедуры внесения изменений в конфигурацию аппаратной и программной частей серверного оборудования, предусматривающие согласование вносимых изменений с работниками подразделения ИБ, регламентируются и контролируются.

75. Работникам подразделения ИБ предоставляется доступ к конфигурации аппаратной и программной частей серверного оборудования без возможности внесения изменений в конфигурации.

76. На постоянной основе обеспечивается резервирование конфигурационных файлов и создание резервных копий данных серверного оборудования. Данный процесс регламентируется и документируется.

77. Операционные системы и ПО, установленные на серверном оборудовании, регулярно обновляются.

78. Для защиты данных серверного оборудования от НСД применяются средства межсетевого экранирования (файрволы) с применением сегментации сети.

79. В ПОНРВ предусматриваются мероприятия на случай возникновения инцидентов безопасности с серверным оборудованием и размещенных на нем данных, включающие процедуры реагирования, восстановления данных и работоспособности серверного оборудования.

80. На регулярной основе (не реже 1 раза в год) осуществляется проведение аудита ИБ и тестов на проникновение в информационную инфраструктуру банка с целью оценки эффективности принимаемых мер защиты информации, размещенной на серверном оборудовании.

81. Серверное оборудование надлежащим образом обслуживается, чтобы гарантировать его постоянную работоспособность.

82. Банком разрабатывается и реализуется механизм контроля за составом аппаратной части серверного оборудования.

ГЛАВА 8
ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ СРЕДЫ ВИРТУАЛИЗАЦИИ

83. В АБС, СЗИ и среде виртуализации обеспечивается синхронизация временных меток и (или) системного времени.

84. Реализуются меры по защите от агрессивного потребления ресурсов виртуальной инфраструктуры потребителями услуг.

85. При использовании среды виртуализации осуществляется сегментация вычислительных сетей, в том числе виртуальных вычислительных сетей, реализованных с использованием функциональных возможностей гипервизора. Обмен данными между сегментами (группами сегментов) вычислительных сетей обеспечивается с применением средств межсетевого экранирования.

86. Запрещается использовать физическое СВТ (хост-сервер), на котором размещается гипервизор, для функционирования ПО, не имеющего непосредственного отношения к работе гипервизора.

87. Регламентируются и выполняются процессы жизненного цикла базовых образов виртуальных машин, в том числе процесс создания и модернизации базовых образов виртуальных машин.

88. Состав ПО каждого из базовых образов виртуальных машин согласовывается с подразделением ИБ банка.

89. При создании базовых образов виртуальных машин осуществляются процедуры, необходимые для выполнения последующего контроля их целостности.

90. Тестирование ПО в виртуальной среде на этапах создания и (или) модернизации АБС проводится в специально организованном виртуальном тестовом сегменте, доступ к которому осуществляется по отдельному физическому сетевому интерфейсу.

91. Созданный или измененный базовый образ виртуальной машины перед размещением в рабочей среде на основном оборудовании, реализующем технологию виртуализации, подлежит проверке в тестовом сегменте на:

корректность работы программных компонентов;

отсутствие вредоносного кода;

соответствие настроек включенных в образ программных компонентов СЗИ требованиям, установленным соответствующей эксплуатационной документацией.

92. Не допускается выполнение копирования текущих образов виртуальных машин, используемых для функционирования серверных компонентов АБС банка, за исключением случаев создания копий, в том числе резервных, в соответствии с установленными регламентами технологических процессов банка.

Не допускается копирование текущих образов виртуальных машин, использующих средства криптографической защиты информации, с загруженными криптографическими ключами без применения мер по защите этих ключей.

93. Для защиты информации, обрабатываемой и хранимой в среде виртуализации, используются СЗИ.

94. АРМ, используемые для выполнения задач администрирования серверных компонентов виртуализации, располагаются в специально выделенном сегменте вычислительных сетей. Размещение в указанном выделенном сегменте вычислительных сетей СВТ, не связанных с выполнением задач управления и администрирования, запрещено.

Доступ с иных АРМ, не входящих в специально выделенный сегмент вычислительных сетей, для выполнения задач управления и администрирования серверных компонентов виртуализации не допускается.

95. На СВТ, используемых для функционирования серверных компонентов виртуализации, используется минимально необходимый и регламентированный набор устройств (портов) ввода-вывода информации.

96. Техническими средствами, в том числе средствами серверных компонентов виртуализации, осуществляется контроль и протоколирование следующих событий:

запуск (остановка) виртуальных машин;

изменение настроек виртуальных сетевых сегментов, реализованных средствами гипервизора;

создание и удаление виртуальных машин;

создание, изменение, копирование, удаление образов виртуальных машин;

копирование текущих образов виртуальных машин;

изменение полномочий доступа к серверным компонентам виртуализации, создание и удаление учетных записей, необходимых для доступа к серверным компонентам виртуализации;

изменение настроек серверных компонентов виртуализации;

идентификация и аутентификация персонала, обеспечивающего эксплуатацию и администрирование среды виртуализации, при осуществлении доступа к серверным компонентам виртуализации;

запуск (остановка) ПО серверных компонентов виртуализации, в том числе ПО гипервизора;

изменение настроек физических СВТ (хост-серверов), используемых для функционирования серверных компонентов виртуализации;

изменение настроек СЗИ, используемых для реализации доступа к серверным компонентам виртуализации;

изменение настроек СЗИ, используемых для целей обеспечения защиты информации виртуальных машин;

события ИБ виртуальной инфраструктуры.

97. Для серверных компонентов виртуализации осуществляется защита от воздействия вредоносного кода, функционирующая на уровне гипервизора.

98. При реализации технологии виртуализации рабочих мест пользователей исключается возможность одновременной работы пользователя с разными виртуальными машинами, размещенными в разных сегментах вычислительных сетей и не включенными в один контур безопасности.

99. В случае использования централизованных (общих) СЗИ, эксплуатируемых с использованием технологии виртуализации для целей обеспечения защиты информации более чем двух виртуальных машин, указанные средства защиты информации размещаются на отдельной виртуальной машине, предназначенной только для этой цели.

100. На виртуальных АРМ пользователей ограничивается использование портов ввода-вывода информации набором, минимально необходимым для выполнения служебных обязанностей пользователя.

Техническими средствами и (или) организационными мерами организовывается контроль использования данного набора портов ввода-вывода информации АРМ пользователей.

101. Техническими средствами (или) организационными мерами ограничивается возможность самостоятельного:

изменения пользователями настроек виртуального АРМ, включая аппаратные и программные компоненты виртуального АРМ;

подключения и использования пользователями дополнительных (несанкционированных) периферийных устройств, в том числе взамен ранее подключенных.

102. Реализуется идентификация и аутентификация пользователей серверными компонентами виртуализации и (или) средствами централизованных сервисов аутентификации при предоставлении доступа к виртуальным машинам.

103. Реализуются меры безопасного перемещения виртуальных машин и обрабатываемых на них данных.

104. Реализуются меры резервного копирования эксплуатируемых виртуальных машин.

ГЛАВА 9
ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИБ АБС НА СТАДИЯХ ЕЕ ЖИЗНЕННОГО ЦИКЛА

105. В разрезе обеспечения ИБ рассматриваются следующие общие стадии жизненного цикла АБС:

разработка технических заданий;

проектирование;

создание и тестирование;

приемка и ввод в эксплуатацию;

эксплуатация;

сопровождение и модернизация;

вывод из эксплуатации.

В случае самостоятельной разработки АБС банком рассматриваются все общие стадии жизненного цикла АБС, в случае приобретения готовых АБС – общие стадии жизненного цикла АБС, указанные в абзацах пятом – восьмом части первой настоящего пункта.

106. Выполнение работ (оказание услуг) по обеспечению ИБ на всех стадиях жизненного цикла АБС осуществляется по согласованию и под контролем подразделения ИБ.

107. При привлечении к выполнению работ (оказанию услуг) в области защиты информации сторонних организаций соблюдаются требования законодательства об информации, информатизации и защите информации и о лицензировании (лицензируемый вид деятельности – деятельность по технической и (или) криптографической защите информации).

108. В технические задания на разработку или модернизацию АБС включаются требования по обеспечению ИБ, установленные и используемые в рамках технологических процессов банка, реализуемых создаваемой или модернизируемой АБС.

109. Разработка технических заданий на СДБО осуществляется с учетом того, что защита информации обеспечивается в условиях:

попыток НСД к информации, объектам, информационным ресурсам пользователей, не прошедших авторизацию (анонимных), с использованием сетей общего пользования;

возможности ошибок пользователей систем, прошедших авторизацию;

возможности ненамеренного или неадекватного использования защищаемой информации пользователями, прошедшими авторизацию.

110. На стадии создания и тестирования АБС и (или) ее компонентов банк обеспечивает реализацию запрета на использование защищаемой информации в качестве тестовых данных, анонимность данных и контроль адекватности предоставления и разграничения доступа к информации, объектам, информационным ресурсам, за исключением случаев тестирования (приемки) результатов разработки АБС с использованием закрытого тестового контура банка.

111. На стадии эксплуатации АБС определяются, выполняются и регистрируются процедуры контроля:

работоспособности (функционирования, эффективности) реализованных в АБС защитных мер, в том числе реализации организационных защитных мер, состава и параметров настройки, применяемых технических защитных мер;

отсутствия уязвимостей в оборудовании и программном обеспечении АБС;

внесения изменений в параметры настройки АБС и применяемых технических защитных мер;

необходимого обновления программного обеспечения АБС, включая программное обеспечение технических защитных мер.

112. На стадии эксплуатации АБС определяются, выполняются, регистрируются и контролируются процедуры, необходимые для обеспечения восстановления всех реализованных функций по обеспечению ИБ.

113. На стадии эксплуатации АБС определяются, выполняются и регистрируются процедуры контроля состава устанавливаемого и (или) используемого ПО АБС.

114. На стадии эксплуатации АБС определяются, выполняются и контролируются процедуры, необходимые для обеспечения сохранности носителей защищаемой информации.

115. На стадии сопровождения (модернизации) определяются, выполняются и регистрируются процедуры контроля, обеспечивающие защиту от:

умышленного несанкционированного раскрытия, модификации или уничтожения информации;

неумышленного раскрытия, модификации или уничтожения информации;

отказа в обслуживании или ухудшения качества обслуживания.

116. На стадии сопровождения (модернизации) АБС, в которых обрабатывается защищаемая информация, в том числе АБС, задействованных в реализации банковского платежного технологического процесса, определяются, выполняются и регистрируются процедуры:

фиксации внесенных изменений;

проверки функциональности АБС, в том числе применяемых мер защиты информации, после внесения изменений.

117. На стадии вывода из эксплуатации АБС определяются, выполняются и документируются процедуры, обеспечивающие удаление информации, несанкционированное использование которой может причинить ущерб банку, и информации, используемой средствами обеспечения ИБ, из постоянной памяти АБС и внешних носителей, за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены соответствующим законодательством, в том числе нормативными правовыми актами Национального банка, и (или) договорами.

118. Банком определяются и назначаются роли, связанные с эксплуатацией и контролем эксплуатации АБС и применяемых технических защитных мер, в том числе с внесением изменений в параметры их настройки.

Для всех АБС определяются и выполняются процедуры контроля их эксплуатации в части обеспечения ИБ подразделением ИБ. Проведение мероприятий по контролю эксплуатации АБС и их результаты регистрируются.

ГЛАВА 10
ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ СКЗИ

119. СКЗИ используются для криптографической защиты информации, направленной на обеспечение конфиденциальности, контроля целостности и подлинности информации.

Использование СКЗИ осуществляется в соответствии с законодательством и требованиями платежных систем.

120. СКЗИ применяются в соответствии с моделями угроз ИБ и нарушителя ИБ, принятыми банком. Применение СКЗИ отражается в политике ИБ банка или в разработанной частной политике ИБ по использованию СКЗИ в банке.

121. Работы по обеспечению ИБ с применением СКЗИ осуществляются в соответствии с законодательством, в том числе нормативными документами, регламентирующими вопросы безопасной эксплуатации СКЗИ, программной и эксплуатационной документацией на СКЗИ и требованиями Оперативно-аналитического центра при Президенте Республики Беларусь в сфере защиты информации.

122. Для обеспечения безопасности применяются СКЗИ:

допускающие встраивание в банковские технологические процессы обработки информации, обеспечивающие взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;

поставляющиеся разработчиками (поставщиками) с полным комплектом программной и эксплуатационной документации на СКЗИ, включая описание управления криптографическими ключами, правила работы с ними, обоснование необходимого организационно-штатного обеспечения.

После встраивания СКЗИ до ввода в эксплуатацию проводится анализ корректности встраивания реализаций криптографических алгоритмов в соответствии с требованиями безопасности, предъявляемыми к СКЗИ.

123. Установка и ввод в эксплуатацию, а также эксплуатация СКЗИ осуществляются в соответствии с требованиями безопасности, предъявляемыми к СКЗИ, программной и эксплуатационной документации к таким СКЗИ.

При использовании носителей ключевой информации для выполнения криптографических сервисов в СКЗИ применяются внешние носители, которые определены программной и эксплуатационной документацией к СКЗИ.

124. При применении СКЗИ поддерживается непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности ПО для среды функционирования СКЗИ, представляющую собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

125. Управление криптографическими ключами (генерация, распределение, хранение, доступ, уничтожение) СКЗИ осуществляется в соответствии с требованиями ТНПА, программной и эксплуатационной документацией на СКЗИ.

126. В целях повышения уровня безопасности при эксплуатации СКЗИ и управления их криптографическими ключами обеспечивается аудит и мониторинг событий безопасности, связанных с функционированием СКЗИ.

127. Порядок применения СКЗИ определяется руководством банка с учетом требований пункта 108 настоящего стандарта, ТНПА, программной и эксплуатационной документации на СКЗИ и включает процессы:

ввода в эксплуатацию, в том числе процедуры встраивания СКЗИ в АБС;

эксплуатации;

обновления;

восстановления работоспособности в аварийных ситуациях;

внесения изменений;

вывода из эксплуатации;

управления криптографическими ключами СКЗИ;

обращения с носителями ключевой информации, в том числе действий при смене и компрометации ключей.

128. Криптографические ключи СКЗИ генерируются уполномоченными работниками банка и (или) клиентом банка самостоятельно. Отношения, возникающие между банками и их клиентами, регулируются договорами.

ГЛАВА 11
ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

129. Для обеспечения защиты мест нахождения защищаемых в рамках СИБ активов (ценные ресурсы банка - информация, оборудование, ПО, процессы и т.д., которые необходимо защищать для поддержания их конфиденциальности, целостности и доступности), банком определяются периметры безопасности, на которых применяются меры обеспечения физической защиты (СКУД, системы видеонаблюдения, освещения, охраны и т.д.). Набор данных мер определяется банком самостоятельно, исходя из требований законодательства и локальных правовых актов банка.

130. Разрабатываются и применяются меры физической защиты от стихийных бедствий, аварий и противоправных действий.

131. Несанкционированное перемещение защищаемых активов банка за пределы периметра безопасности запрещается. В случае санкционированного перемещения активов за периметр безопасности принимаются меры по обеспечению их безопасности от уничтожения, модификации и утечки информации.

132. Обеспечиваются контроль и ограничение доступа в помещения, где расположены защищаемые активы (серверные, центры обработки данных и т.д.), с помощью физических барьеров (двери, замки), электронных систем контроля доступа (СКУД, биометрических систем и т.д.), а также ведение учета доступа.

133. Доступ в помещения, где расположены защищаемые активы, предоставляется только уполномоченным лицам в рамках исполнения ими служебных (должностных) обязанностей.

134. Для удаленных АРМ, в том числе банкоматов и платежных терминалов, расположенных за периметром безопасности, определяются и реализуются соответствующие меры безопасности посредством контроля и управления ими, исходя из оценки рисков (в том числе рисков информационной безопасности).

135. С работниками банка на регулярной основе организовывается проведение инструктажей по физической безопасности, повышение их осведомленности о рисках и мерах защиты.

136. Определяются, внедряются и проводятся процедуры проверок системы безопасности, выявления уязвимостей и их устранения.

ГЛАВА 12
ТРЕБОВАНИЯ ПО ОБУЧЕНИЮ И ПОВЫШЕНИЮ ОСВЕДОМЛЕННОСТИ ПО ВОПРОСАМ ИБ

137. Руководством банка (подразделением ИБ) на регулярной основе организовывается работа с работниками банка в направлении обучения и повышения осведомленности в области ИБ.

138. Разрабатываемая, внедряемая и соблюдаемая банком политика ИБ в обязательном порядке содержит требования по обучению и повышению осведомленности работников банка по вопросам ИБ.

139. Ежегодно разрабатываются планы, программы обучения и повышения осведомленности в области ИБ.

140. В планах обучения и повышения осведомленности в области ИБ устанавливаются требования к периодичности обучения и повышения осведомленности в области ИБ.

141. Программы обучения и повышения осведомленности в области ИБ разрабатываются для различных групп работников банка с учетом их служебных (должностных) обязанностей и выполняемых ролей и в обязательном порядке включают информацию:

по существующим политикам ИБ;

по применяемым в банке защитным мерам;

по правильному использованию защитных мер в соответствии с документами банка;

о значимости и важности деятельности работников для обеспечения ИБ банка.

142. Обучение и повышение осведомленности включает не только теоретические, но и практические занятия, тренинги, симуляции, разбор реальных инцидентов ИБ, а также актуальную информацию о новых угрозах и трендах в области ИБ.

143. Обучение и повышение осведомленности работников адаптировано под специфику деятельности банка, включает примеры из его опыта и практические сценарии, которые работники смогут применить в своей служебной деятельности.

144. По результатам прохождения обучения и повышения осведомленности по вопросам ИБ осуществляется проверка полученных знаний.

145. Процессы обучения и повышения осведомленности в банке документируются (планы, графики, отчеты о прохождении обучения и результаты тестов). Свидетельствами выполнения программ обучения и повышения осведомленности в области ИБ являются:

документы (журналы), подтверждающие прохождение руководителями и работниками банка обучения в области ИБ, с указанием уровня образования, навыков, опыта и квалификации обучаемых;

документы, содержащие результаты проверок осведомленности в области ИБ в банке.

146. Для работника, получившего новую роль, организовывается обучение или инструктаж в области ИБ, соответствующие полученной роли, связанные с применением организационных мер защиты информации и (или) использованием технических средств защиты информации.

147. В банке определяются роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю результатов, а также назначаются ответственные за выполнение указанных ролей.

148. Банк обеспечивает регулярное информирование клиентов о рисках, мерах защиты и правилах безопасного использования банковских продуктов и услуг любым незапрещенным законодательством способом, в том числе через:

сайты и мобильные приложения банка;

электронную почту и SMS-рассылки;

социальные сети;

обучающие материалы, размещенные в местах оказания банковских услуг и сервисов;

консультации с работниками банка.

ГЛАВА 13
ТРЕБОВАНИЯ ПО ПРЕДОТВРАЩЕНИЮ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

149. Определяются, выполняются, регистрируются и контролируются процедуры выявления, учета и классификации (отнесение к одному из видов информации в соответствии с законодательством) информационных активов банка.

150. Банком применяются меры по защите информации любой категории, в том числе по предотвращению ее утечки. Защита информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено, осуществляется в соответствии с законодательством.

151. Разрабатывается, выполняется и контролируется порядок хранения и обращения информации, подлежащей защите, а также порядок доступа к ней.

152. Доступ к защищаемой информации ограничивается на основе принципа минимальных привилегий и предоставляется тем работникам банка, которым он действительно нужен для выполнения их служебных (должностных) обязанностей.

153. Все работники банка ознакамливаются под подпись с локальными правовыми актами, содержащими требования по ИБ, и дают письменные обязательства о соблюдении конфиденциальности, приверженности правилам корпоративной этики, которые включают требования по недопущению конфликта интересов.

154. Доступ в помещения, где хранится и обрабатывается защищаемая информация, ограничивается, в том числе путем внедрения пропускной системы. Для хранения носителей защищаемой информации используются сейфы и (или) запираемые шкафы, ограничивающие свободный доступ к их содержимому.

155. Для доступа к ресурсам АРМ и АБС используется аутентификация. При этом требуется внедрение строгой политики использования паролей, включающей требования к сложности паролей, их регулярной смене, запрет на хранение паролей в незащищенных местах.

156. Внедряются системы предотвращения утечек информации по техническим каналам связи, которые позволяют контролировать потоки данных, выявлять и предотвращать утечки защищаемой информации, контролировать и анализировать содержимое передаваемых данных.

157. Передача защищаемой информации с использованием сети Интернет осуществляется только при условии обеспечения ее защиты от несанкционированного доступа и модификации, в том числе с использованием СКЗИ.

158. Запрещается несанкционированное руководством банка хранение и обработка защищаемой информации на СВТ, размещенных в сегментах вычислительных сетей банка, имеющих подключение к сети Интернет.

159. МНИ, предназначенные для обработки и хранения защищаемой информации, подлежат учету и контролируются. Порядок использования таких МНИ определяется документально.

160. При осуществлении вывода МНИ из эксплуатации или вывода из эксплуатации СВТ, в состав которых входят указанные МНИ, а также при необходимости их передачи в сторонние организации удаление информации с МНИ осуществляется средствами, обеспечивающими полную перезапись данных.

161. Уполномоченными работниками банка проводится анализ инцидентов безопасности для выявления причин утечек и принятия мер по их предотвращению в будущем.

ГЛАВА 14
ТРЕБОВАНИЯ ПО УПРАВЛЕНИЮ ДОСТУПОМ

162. Права доступа работников и клиентов банка к его активам учитываются и фиксируются.

163. В АБС реализуются защитные меры от НСД, в том числе с использованием соответствующих средств защиты информации.

Защитные меры от НСД обеспечивают сокрытие вводимых работниками и клиентами банка (далее – субъекты доступа) аутентификационных данных на устройствах отображения информации. Размещение устройств отображения информации АБС осуществляется образом, препятствующим ее несанкционированному просмотру.

164. В банке определяются, выполняются, регистрируются и контролируются правила и процедуры:

идентификации, аутентификации, авторизации субъектов доступа, в том числе внешних субъектов доступа, которые не являются работниками банка, и программных процессов (сервисов);

разграничения доступа к информационным активам на основе ролевого метода (прав доступа), с определением для каждой роли полномочий по доступу к информационным активам;

управления предоставлением, отзывом и блокированием доступа, в том числе доступа, осуществляемого через внешние информационно-телекоммуникационные сети;

регистрации действий субъектов доступа с обеспечением контроля целостности и защиты данных регистрации;

управления идентификационными данными, аутентификационными данными и средствами аутентификации;

управления учетными записями субъектов доступа;

контроля за соблюдением правил генерации (создания) и смены паролей субъектов доступа;

выявления и блокирования неуспешных попыток доступа;

блокирования сеанса доступа после установленного времени бездействия или по запросу субъекта доступа, требующего выполнения процедур повторной аутентификации и авторизации для продолжения работы;

ограничения действий пользователей по изменению настроек АРМ (использование ограничений на изменение BIOS (UEFI);

управления набором разрешенных действий субъектов доступа до выполнения ими идентификации и аутентификации;

ограничения действий пользователей по изменению параметров настроек АБС и реализации контроля действий персонала,

обеспечивающего эксплуатацию и администрирование АБС банка, по изменению параметров настроек АБС;

выявления и блокирования несанкционированного перемещения (копирования) информации, в том числе баз данных, файловых ресурсов, виртуальных машин;

использования технологий беспроводного доступа к информации, в случае их применения, и защиты внутренних беспроводных соединений;

использования мобильных устройств для доступа к информации в случае их применения.

Процедуры управления доступом применяются с обязательным условием соблюдения принципа минимальных и достаточных полномочий и исключают возможность наделения пользователем самого себя доступом к информационным активам.

165. В банке применяются меры, направленные на обеспечение защиты от НСД, повреждения или нарушения целостности данных о действиях и операциях, а также меры по защите информации, необходимой для идентификации, аутентификации и (или) авторизации клиентов и работников банка. Все попытки НСД к такой информации регистрируются. Доступ к данным о действиях и операциях предоставляется только с целью выполнения служебных обязанностей.

При увольнении или изменении должностных обязанностей работников банка, имевших доступ к указанным данным, выполняются регламентированные процедуры соответствующего пересмотра прав доступа.

166. Доступ всех работников и клиентов банка в АБС осуществляется под уникальными и персонифицированными учетными записями с минимально необходимыми привилегиями.

167. Субъекты доступа получают доступ только к тем информационным активам банка, для которых у них есть авторизация.

168. В банке определяются, выполняются, регистрируются и контролируются правила назначения и применения привилегированных прав доступа. Предоставление таких прав доступа носит ограниченный характер.

169. Банк на регулярной основе пересматривает права доступа пользователей к его активам, в том числе при увольнении или изменении служебных (должностных) обязанностей работников банка.

170. Определяются, выполняются, регистрируются и контролируются правила и процедуры проверки отсутствия незаблокированных учетных записей:

работников, с которыми прекращены трудовые отношения;

работников, отсутствующих на рабочем месте более 60 календарных дней;

работников внешних (подрядных) организаций, прекративших свою деятельность в банке;

неопределенного назначения.

ГЛАВА 15
ТРЕБОВАНИЯ ПО УПРАВЛЕНИЮ СОБЫТИЯМИ И ИНЦИДЕНТАМИ ИБ

171. В банке определяются, выполняются, регистрируются и контролируются правила и процедуры мониторинга событий ИБ, анализа и хранения данных о действиях и операциях, позволяющие выявлять неправомерные или подозрительные операции и транзакции. Для этого:

определяется состав информации о событиях ИБ, подлежащих регистрации в соответствии с требованиями законодательства, таких как идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения ИБ и другое;

определяются сроки хранения информации о событиях ИБ, но не менее одного года;

обеспечивается централизованный сбор и хранение информации о событиях ИБ в течение установленного срока хранения;

обеспечивается резервирование необходимого объема памяти для записи и хранения данных о событиях ИБ;

определяется способ и периодичность мониторинга (просмотра, анализа) событий ИБ уполномоченными на это работниками банка;

обеспечивается реагирование на сбои при регистрации действий и операций, в том числе аппаратные и программные ошибки, сбои в технических средствах сбора данных;

обеспечивается синхронизация системного времени на технических средствах, используемых для целей мониторинга ИБ, анализа и хранения данных.

172. В банке обеспечивается ведение журналов действий и операций АРМ, серверного и сетевого оборудования, межсетевых экранов и АБС с целью их использования при реагировании на инциденты ИБ.

173. Журналы действий и операций защищаются от уничтожения и несанкционированных изменений. Доступ к таким журналам регистрируется.

174. Обеспечивается хранение данных о действиях и операциях не менее одного года, если иные сроки хранения не установлены законодательством.

175. Для осуществления мониторинга событий ИБ и анализа данных о действиях и операциях используются специализированные программные и (или) технические средства (SIEM-системы).

176. Процедуры мониторинга событий ИБ и анализа данных о действиях и операциях используют зафиксированные критерии выявления неправомерных или подозрительных действий и операций. Указанные процедуры мониторинга событий ИБ и анализа применяются на регулярной основе ко всем выполненным действиям и операциям (транзакциям).

177. Процедуры мониторинга событий ИБ подвергаются регулярным и регистрируемым пересмотрам в связи с выявлением новых угроз и уязвимостей ИБ, а также на основе данных, полученных в ходе анализа зафиксированных событий ИБ, с целью внесения изменений в состав и способы реализации защитных мер ИБ.

178. В банке определяются роли, связанные с выполнением процедур мониторинга событий ИБ и их пересмотром, а также назначаются ответственные за выполнение этих ролей.

179. Оповещения о событиях ИБ автоматически доводятся до уполномоченных работников банка по соответствующим каналам управления незамедлительно.

180. В банке регистрируются и контролируются события ИБ, связанные с действиями работников:

по управлению учетными записями и правами субъектов доступа;

обладающих правами по изменению параметров настроек средств и систем защиты информации, параметров настроек АРМ и АБС, связанных с обеспечением защиты информации;

обладающих правами по управлению криптографическими ключами и СКЗИ.

181. Работники банка информируются о порядке действий при обнаружении событий ИБ и порядке информирования о них ответственных за обеспечение ИБ. Данные действия регистрируются и контролируются банком.

182. События ИБ подлежат оценке, на основании которой принимается решение, следует ли их классифицировать как инцидент ИБ.

183. Инциденты ИБ классифицируются в соответствии с требованиями законодательства с учетом степени их влияния (критичности) на предоставление финансовых услуг, реализацию бизнес-процессов и (или) технологических процессов банка.

184. В банке документально определяются, выполняются, регистрируются и контролируются процедуры обработки инцидентов ИБ, такие как:

процедуры обнаружения инцидентов ИБ;

процедуры информирования об инцидентах ИБ, в том числе информирования подразделения ИБ;

процедуры классификации инцидентов и оценки ущерба, нанесенного инцидентом ИБ;

процедуры реагирования на инцидент ИБ;

процедуры анализа причин инцидентов ИБ и оценки результатов реагирования на инциденты ИБ (при необходимости с участием внешних экспертов в области ИБ).

185. Разрабатываются и внедряются планы реагирования на инциденты ИБ, включающие в себя конкретные действия по локализации, устранению и восстановлению после инцидентов ИБ.

186. В банке определяются роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ, а также назначаются ответственные за выполнение этих ролей.

187. Процедуры расследования инцидентов ИБ учитывают законодательство, в том числе положения нормативных правовых актов Национального банка, а также документов банка в области ИБ.

188. Решения по всем выявленным в банке инцидентам ИБ принимаются, фиксируются и выполняются.

189. Знания, полученные из анализа и разрешения инцидентов ИБ, используются для уменьшения вероятности инцидентов в будущем или их воздействия на деятельность банка.

190. Сбои в системах мониторинга событий ИБ обнаруживаются, регистрируются и оперативно устраняются.

ГЛАВА 16
ТРЕБОВАНИЯ ПО УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

191. Банком создается документированная база активов, подлежащих защите. Для этого:

определяются и инвентаризируются все активы (АБС, ИС, оборудование, ПО, данные и т.д.);

классифицируются инвентаризированные активы по степени их критичности или важности;

назначаются ответственные за активы лица, т.е. закрепляется каждый актив за конкретным работником или группой работников.

192. Документально определяются, выполняются, регистрируются и контролируются процедуры сканирования уязвимостей активов, подлежащих защите.

193. Банк обеспечивает хранение информации о результатах сканирования уязвимостей в течение установленного им срока хранения, но не менее года.

194. Доступ к информации о результатах сканирования уязвимостей ограничивается и предоставляется только тем работникам, которым он необходим для выполнения их служебных (должностных) обязанностей.

195. По результатам сканирования осуществляются:

определение степени риска ИБ каждой выявленной уязвимости, исходя из ее потенциального воздействия на активы;

определение вероятности эксплуатации уязвимости;

принятие соответствующих мер для обработки рисков ИБ, связанных с выявленной уязвимостью.

196. Реализация мер по устранению выявленных уязвимостей осуществляется в максимально короткие сроки. В первую очередь устраняются наиболее критичные уязвимости, способные оказать негативное воздействие на предоставление финансовых услуг, реализацию бизнес-процессов и (или) технологических процессов банка.

197. Обеспечивается оперативное устранение уязвимостей, использование которых может позволить:

осуществить несанкционированное информационное взаимодействие между внутренними сетями банка и сетью Интернет;

несанкционированное (неконтролируемое) информационное взаимодействие между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов) и сетью Интернет;

несанкционированный удаленный доступ к защищаемым активам.

198. Устранение выявленных уязвимостей осуществляется путем реализации следующих мер:

применение исправлений и обновлений ПО, предоставленных производителями;

внедрение дополнительных мер безопасности, таких как применение межсетевых экранов, систем обнаружения и предотвращения вторжений, антивирусного ПО.

внесение изменений в настройки АБС;

ограничение доступа к активам;

сегментация информационно-вычислительной сети для ограничения распространения ВПО;

внедрение резервирования серверов и сетевого оборудования.

199. Организовывается проведение повторного сканирования после устранения уязвимостей для проверки эффективности осуществленных исправлений.

200. Осуществляется постоянный мониторинг событий безопасности для своевременного выявления попыток эксплуатации уязвимостей.

201. Регулярно (не реже 1 раза в год) проводится внешнее и внутреннее тестирование на проникновение (пентест) с целью выявления уязвимостей и оценки эффективности принимаемых мер безопасности.

РАЗДЕЛ III
ТРЕБОВАНИЯ К СИСТЕМЕ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ

ГЛАВА 17
ОБЩИЕ ПОЛОЖЕНИЯ

202. В основе СМИБ лежит модель непрерывного улучшения качества, также известная как цикл Деминга: ”планирование – реализация – проверка – совершенствование“ или цикл PDCA ”Plan-Do-Check-Act“. Данные четыре процесса СМИБ необходимы для реализации и поддержания на должном уровне ИБ в банке.

203. Этап ”планирование“ является одним из основополагающих, так как с него начинается запуск ”жизненного цикла“ СМИБ и его дальнейшее функционирование. Деятельность на этапе ”планирование“ заключается в определении:

области действия СМИБ;

политики ИБ;

ролей и обязанностей в области ИБ;

процессов оценки и обработки рисков ИБ;

задач в области ИБ и планирование их достижения;

документов СМИБ;

ресурсов, необходимых для функционирования СМИБ.

204. Этап ”реализация“ выполняется в соответствии с результатами выполнения этапов ”планирование“ и (или) ”совершенствование“ и заключается во внедрении и совершенствовании СМИБ. В ходе данного этапа банк обеспечивает:

функционирование процессов ИБ;

выполнение задач по ИБ;

оценку рисков ИБ;

обработку рисков ИБ;

Банк выбирает защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от реализации угроз. Банк применяет только те защитные меры, правильность работы которых может быть проверена и оценена эффективность их применения.

205. Этап ”проверка“ необходим для анализа результатов деятельности предыдущих этапов ”планирование“ и ”реализация“ с целью

получения достаточной уверенности в том, что СМИБ, включая защитные меры, функционирует надлежащим образом и адекватна существующим угрозам ИБ. В ходе данного этапа банк осуществляет:

мониторинг, измерение, анализ и оценку деятельности в области ИБ;

проведение внутренних аудитов;

контроль со стороны руководства банка.

На этапе ”проверка“ осуществляется мониторинг и контроль используемых защитных мер, периодически оценивается соответствие ИБ банка требованиям настоящего стандарта.

Результат выполнения деятельности на этапе ”проверка“ является основой для выполнения деятельности по совершенствованию СМИБ.

206. Этап ”совершенствование“ включает в себя деятельность по принятию решений об улучшении пригодности, соответствия и результативности СМИБ. В ходе данного этапа банк осуществляет:

выполнение корректирующих действий по устранению выявленных на предыдущем этапе несоответствий;

улучшение СМИБ.

Переход к этапу ”совершенствование“ реализуется только тогда, когда результатом выполнения этапа ”проверка“ являются данные, свидетельствующие о необходимости совершенствования СМИБ. При этом сама деятельность по совершенствованию СМИБ должна реализовываться в рамках групп процессов ”реализация“ и, при необходимости, ”планирование“.

207. Банк накапливает, обобщает и использует как свой опыт, так и опыт других организаций на всех уровнях принятия решений по улучшению функционирования СМИБ и их исполнения.

208. Банк организует и обеспечивает функционирование СМИБ с учетом следующих требований:

требования к организации и функционированию подразделения ИБ банка;

требования к определению области действия СМИБ;

требования к выбору подхода к оценке рисков ИБ и проведению оценки рисков ИБ;

требования к разработке и реализации процесса обработки рисков ИБ;

требования к разработке документов, регламентирующих деятельность в области обеспечения ИБ;

требования к принятию руководством банка решений о реализации и эксплуатации СМИБ;

требования к разработке и реализации программ по обучению и повышению осведомленности работников банка в области ИБ;

требования к организации обнаружения и реагирования на инциденты ИБ;

требования к организации обеспечения непрерывности ИБ и ее восстановления после сбоев;

требования к мониторингу и оценке эффективности СМИБ;

требования к проведению внутреннего аудита ИБ;

требования к анализу функционирования СМИБ;

требования к анализу СМИБ со стороны руководства банка;

требования к принятию решений по улучшению СМИБ.

ГЛАВА 18
ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЮ ПОДРАЗДЕЛЕНИЯ ИБ БАНКА

209. Для разработки, внедрения, поддержания функционирования и постоянного улучшения СМИБ в банке создается подразделение ИБ или назначается уполномоченное должностное лицо.

Потребность подразделения ИБ в кадрах определяется руководством банка и зависит от нескольких ключевых факторов, включая:

уровень зрелости организации в области ИБ;

сложность и масштаб инфраструктуры банка;

задачи и функции, возложенные на подразделение ИБ;

текущие и прогнозируемые риски;

количество и сложность используемых технологий;

компетенцию работников в области обеспечения ИБ;

требования законодательства, в том числе положения нормативных правовых актов, а также документов банка;

бюджет на обеспечение ИБ.

210. При создании подразделения ИБ определяются:

цели и задачи его деятельности;

его структура;

права и обязанности его работников;

порядок его взаимодействия с другими подразделениями банка.

211. Руководством банка подразделение ИБ наделяется полномочиями и обеспечивается ресурсами, необходимыми для выполнения установленных целей и задач. Из числа руководства банка назначается куратор подразделения ИБ.

212. Банком, имеющим сеть филиалов или региональных представительств, в случае необходимости создаются соответствующие подразделения ИБ (уполномоченные лица) на местах, которые обеспечиваются необходимыми ресурсами.

213. Подразделение ИБ наделяется следующими минимальными полномочиями:

организовывать и выполнять деятельность по обеспечению ИБ банка;

разрабатывать и вносить предложения по изменению политик ИБ банка;

организовывать изменение существующих и принятие руководством банка новых документов, регламентирующих деятельность по обеспечению ИБ банка;

определять требования к мерам обеспечения ИБ банка;

осуществлять согласование возможности предоставления или изменения прав доступа для работников банка;

осуществлять контроль прав доступа работников банка и их отзыва;

контролировать работников банка в части выполнения ими требований документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих привилегированные полномочия по доступу к защищаемым информационным активам;

осуществлять установку, внедрение и эксплуатацию средств защиты информации;

осуществлять мониторинг событий, связанных с обеспечением ИБ;

участвовать в расследовании событий, связанных с инцидентами ИБ, и в случае необходимости выходить с предложениями по применению санкций в отношении лиц, нарушивших требования нормативных правовых и документов по обеспечению ИБ;

осуществлять взаимодействие с уполномоченными органами по вопросам обеспечения ИБ;

участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий;

осуществлять контроль обеспечения ИБ на стадиях жизненного цикла АБС, в том числе при тестировании и вводе в эксплуатацию подсистем ИБ АБС;

проводить мониторинг состояния безопасности и оценку эффективности СИБ;

участвовать в создании, поддержании, эксплуатации и совершенствовании СМИБ банка.

ГЛАВА 19

ТРЕБОВАНИЯ К ОПРЕДЕЛЕНИЮ ОБЛАСТИ ДЕЙСТВИЯ СМИБ

214. Для определения области действия СМИБ определяются границы и применимость этой системы в рамках банка.

Для определения границ выделяются объекты, активы, процессы и подразделения банка, которые будут включены в область действия СМИБ.

При определении применимости устанавливается, какие стандарты, политики и процедуры безопасности будут применяться к каждому элементу, включенному в область действия СМИБ.

215. При определении области действия СМИБ:

учитываются внешние и внутренние факторы, оказывающие влияние на ИБ и эффективность функционирования СМИБ;

устанавливаются иные участники, оказывающие влияние на функционирование СМИБ и их требования, которые необходимо учесть при реализации и (или) совершенствовании СМИБ;

учитываются процессы во взаимоотношениях между банком и другими организациями.

216. Область действия СМИБ документируется и доступна для ознакомления всем заинтересованным сторонам.

217. В случае изменения области действия СМИБ осуществляется ее коррекция.

ГЛАВА 20
ТРЕБОВАНИЯ К ВЫБОРУ ПОДХОДА К ОЦЕНКЕ РИСКОВ ИБ И ПРОВЕДЕНИЮ ОЦЕНКИ РИСКОВ ИБ

218. Банком самостоятельно выбирается и принимается подход к оценке рисков ИБ. Выбор подхода к оценке рисков ИБ зависит от множества факторов, включающих:

величину самого банка;

сложность бизнес-процессов в нем;

критичность обрабатываемой информации;

доступность ресурсов;

зрелость существующей СИБ.

Банк может использовать комбинацию подходов для комплексной оценки рисков.

219. В случае возникновения ситуаций, при которых проводимая оценка рисков ИБ дает противоречивые и необоснованные результаты, осуществляется коррекция подхода к оценке рисков ИБ.

220. Выбранный подход к оценке рисков ИБ понятен и применим для специалистов, ответственных за обеспечение ИБ в банке.

221. Выбранный банком подход к оценке рисков ИБ определяет способ и порядок качественного или количественного оценивания риска ИБ на основании оценивания:

степени возможности реализации угроз ИБ, выявленными и (или) предполагаемыми источниками угроз ИБ, зафиксированными в моделях угроз и нарушителя, в результате их воздействия на объекты среды информационных активов банка;

степени тяжести последствий от потери свойств ИБ, в частности свойств доступности, целостности и конфиденциальности для рассматриваемых информационных активов.

222. Порядок оценки рисков ИБ определяет необходимые процедуры оценки таких рисков, а также последовательность их выполнения.

223. Оценка рисков ИБ осуществляется для идентификации рисков, связанных с потерей конфиденциальности, целостности и доступности информации в рамках области действия СМИБ и определения владельцев риска.

224. Банком определяются критерии принятия рисков ИБ и уровень допустимого риска ИБ.

225. Полученные в результате оценки рисков ИБ значения рисков соотносятся с уровнем допустимого риска, принятого в банке. Результатом выполнения указанной процедуры является зафиксированный, ранжированный по степени критичности перечень недопустимых рисков ИБ.

226. В банке определяются роли, связанные с деятельностью по выбору и определению подхода к оценке рисков ИБ, и назначаются ответственные лица за выполнение указанных ролей.

227. Оценка рисков ИБ осуществляется на плановой основе, но не реже 1 раза в год, а также в случае изменения области действия СМИБ и (или) выявлении новых угроз и уязвимостей.

228. Оценка рисков ИБ носит документированный характер.

ГЛАВА 21
ТРЕБОВАНИЯ К РАЗРАБОТКЕ И РЕАЛИЗАЦИИ ПРОЦЕССА ОБРАБОТКИ РИСКОВ ИБ

229. После проведения оценки рисков ИБ банком определяется и выполняется процесс обработки рисков ИБ, в ходе которого:

выбираются соответствующие меры обработки рисков ИБ с учетом результатов оценки рисков ИБ;

определяются средства, необходимые для реализации выбранных мер обработки рисков ИБ;

разрабатывается план обработки рисков ИБ.

230. План обработки рисков ИБ включает определение мер, необходимых для снижения или устранения рисков, распределение ответственности за их реализацию, а также сроки реализации и внедрения мер защиты.

231. Для каждого из рисков ИБ, который является недопустимым, выбирается один из возможных методов его обработки:

снижение риска (внедрение мер безопасности для уменьшения вероятности реализации угрозы и (или) минимизации ущерба);

перенос риска (передача риска сторонней организации);

избежание риска (полный отказ от деятельности или процесса, который может привести к появлению риска);

принятие риска (сознательное признание риска и готовность смириться с его последствиями в случае их наступления).

232. План обработки рисков ИБ согласовывается с владельцами процессов, подверженным рискам, руководителем подразделения ИБ (уполномоченным должностным лицом) и утверждается руководством банка.

233. Пересмотр и корректировка плана обработки рисков ИБ осуществляется на регулярной и плановой основе (не реже 1 раза в год), а также при изменении условий, влияющих на риски ИБ.

234. В банке определяются роли по разработке плана обработки рисков ИБ и назначаются ответственные лица за выполнение указанных ролей.

235. Результаты обработки рисков ИБ документируются.

ГЛАВА 22
ТРЕБОВАНИЯ К РАЗРАБОТКЕ ДОКУМЕНТОВ, РЕГЛАМЕНТИРУЮЩИХ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИБ

236. Разработка и (или) коррекция документов, регламентирующих деятельность в области обеспечения ИБ в банке, проводится с учетом положений и требований СФУТ 9.02-2024 ”Банковская деятельность. Обеспечение информационной безопасности. Требования к документации по обеспечению деятельности в области информационной безопасности“.

237. В банке разрабатываются следующие документы:

политика ИБ банка;

частные политики ИБ банка;

документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ банка.

Кроме того, определяются перечень и формы документов, являющихся свидетельством выполнения банком деятельности по обеспечению ИБ.

238. Политика ИБ банка утверждается руководством.

239. В политике ИБ банка определяются:

цели, задачи и принципы обеспечения ИБ;

область действия политики ИБ;

намерения обеспечения ИБ, направленного на достижение указанных целей и реализацию принципов обеспечения ИБ;

общие сведения об активах банка, подлежащих защите;

правила и требования в области ИБ, представляющие особую важность для банка;

соответствия требованиям законодательства, в том числе нормативным правовым актам Национального банка в области информации, информатизации и защиты информации;

требования к управлению ИБ;

требования по предотвращению и обнаружению компьютерных вирусов и другого ВПО;

требования по управлению непрерывностью ИБ;

последствия нарушений политики ИБ и ответственность за эти нарушения;

общие роли и обязанности, связанные с обеспечением ИБ, включая информирование об инцидентах ИБ;

перечень частных политик ИБ, развивающих и детализирующих положения политики ИБ банка, а также указание подразделений банка, ответственных за их соблюдение и (или) реализацию;

положения по контролю реализации политики ИБ банка;

ответственность за реализацию и поддержку политики ИБ банка;

сроки и условия пересмотра (изменения или изложения в новой редакции) политики ИБ банка.

240. В частных политиках ИБ банка определяются:

цели и задачи ИБ, на обеспечение которых направлена частная политика ИБ;

область действия частной политики ИБ, объекты (активы) защиты,

уязвимости ИБ, угрозы и оценка рисков ИБ, связанных с объектами защиты;

сведения о виде деятельности, на обеспечение ИБ которой направлено действие положений частной политики ИБ;

подразделения банка (филиала, структурного подразделения), работники банка (отделения), на которых распространяется действие частной политики ИБ;

требования и правила ИБ;

обязанности по обеспечению ИБ в рамках области действия частной политики ИБ;

положения по контролю реализации частной политики ИБ;

ответственные за реализацию и поддержку частной политики ИБ;

сроки и условия пересмотра частной политики ИБ.

241. Повторение одинаковых правил в различных частных политиках ИБ запрещается. Включение в частную политику ИБ правил, содержащихся в другой действующей политике ИБ, частной политике ИБ, осуществляется посредством соответствующей ссылки.

242. Разработка документов, регламентирующих деятельность в области обеспечения ИБ, проводится на основе законодательства, в том числе нормативных правовых актов Оперативно-аналитического центра при Президенте Республики Беларусь, контрольных (надзорных) органов Республики Беларусь, а также предписаний контрольных (надзорных) органов Республики Беларусь, результатов оценки рисков ИБ.

243. Совокупность документов, регламентирующих деятельность в области обеспечения ИБ, содержит требования по обеспечению ИБ всех активов банка, входящих в область действия СМИБ банка.

244. Документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, детализируют положения политики (частных политик) ИБ и не противоречат им.

245. Определяется порядок разработки, актуализации, пересмотра и контроля исполнения документов, регламентирующих деятельность по обеспечению ИБ в банке.

246. В банке осуществляется управление документами, регламентирующими деятельность по обеспечению ИБ.

247. В банке определяются роли по разработке, актуализации, пересмотру и контролю исполнения документов, регламентирующих деятельность по обеспечению ИБ, а также назначаются ответственные лица за выполнение указанных ролей.

ГЛАВА 23
ТРЕБОВАНИЯ К ПРИНЯТИЮ РУКОВОДСТВОМ БАНКА РЕШЕНИЙ О РЕАЛИЗАЦИИ И ЭКСПЛУАТАЦИИ СМИБ

248. Решения о реализации и эксплуатации СМИБ принимаются и утверждаются руководством банка.

249. В банке фиксируются решения руководства банка:

о внедрении СМИБ;

о планировании этапов внедрения СМИБ, в частности, требований по обеспечению ИБ, изложенных в разделах II и III настоящего стандарта;

о распределении ролей в области обеспечения ИБ банка;

об анализе и принятии остаточных рисков ИБ;

о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований разделов II и III настоящего стандарта и снижение рисков ИБ;

о выделении ресурсов, необходимых для реализации и эксплуатации СМИБ.

250. Все планы внедрения СМИБ, в том числе планы реализации требований разделов II и III настоящего стандарта, планы обработки рисков ИБ и внедрения защитных мер утверждаются руководством банка. Указанные планы определяют:

последовательность выполнения мероприятий в рамках указанных планов;

сроки начала и окончания запланированных мероприятий;

лиц, ответственных за выполнение каждого указанного мероприятия.

251. Определяется порядок разработки, актуализации, пересмотра и контроля исполнения планов по обеспечению ИБ банка.

252. Фиксируются решения руководства банка, связанные с назначением и распределением ролей в рамках функционирования СМИБ для всех структурных подразделений банка в соответствии с положениями документов, регламентирующих деятельность по обеспечению ИБ банка.

ГЛАВА 24
ТРЕБОВАНИЯ К РАЗРАБОТКЕ И РЕАЛИЗАЦИИ ПРОГРАММ ПО ОБУЧЕНИЮ И ПОВЫШЕНИЮ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ БАНКА В ОБЛАСТИ ИБ

253. Руководством банка (подразделением ИБ) на постоянной основе организовывается, документально оформляется и утверждается работа в направлении повышения осведомленности и обучения в области ИБ работников, деятельность которых влияет на состояние ИБ банка.

254. Разрабатываются планы (программы) обучения и повышения осведомленности в области ИБ.

255. В планах обучения и повышения осведомленности устанавливаются:

цели проведения обучения и (или) повышения осведомленности;

целевая аудитория программ обучения и (или) повышения осведомленности;

формат проведения обучения и (или) повышения осведомленности;

требования к периодичности обучения и (или) повышения осведомленности;

лица, ответственные за организацию и проведение обучения и повышения осведомленности.

256. Программы обучения и повышения осведомленности разрабатываются для различных групп работников банка с учетом их должностных обязанностей и выполняемых ролей и включают информацию:

по существующим политикам ИБ;

по применяемым в банке защитным мерам;

по правильному использованию защитных мер в соответствии с документами банка;

о значимости соблюдения и выполнения установленных в банке требований ИБ на результативность СМИБ;

о последствиях невыполнения требований СМИБ;

о новых угрозах и уязвимостях в сфере ИБ;

о значимости и важности деятельности работников для обеспечения ИБ банка.

257. По результатам прохождения программ обучения и повышения осведомленности осуществляется проверка полученных знаний.

258. Определяется перечень свидетельств выполнения работниками программ обучения и повышения осведомленности в области ИБ. Такими свидетельствами могут являться:

подтверждение прохождения руководителями и работниками банка обучения в области ИБ с указанием уровня образования, навыков, опыта и квалификации обучаемых;

документы, подтверждающие участие работников в различных краткосрочных образовательных программах в области ИБ (форумах, тренингах, семинарах и т.д.);

документы, содержащие результаты проверок обучения и (или) повышения осведомленности в области ИБ.

259. Для работника, получившего новую роль, организовывается обучение или инструктаж в области ИБ, соответствующие полученной роли.

260. В банке определяются роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ, контролю результатов, а также назначаются ответственные лица за выполнение указанных ролей.

ГЛАВА 25
ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

261. Определяются, выполняются, регистрируются и контролируются процедуры обработки инцидентов ИБ, включающие:

процедуры подготовки к обнаружению и реагированию на инциденты ИБ;

процедуры обнаружения и информирования об инцидентах ИБ, в том числе информирования подразделения ИБ;

процедуры анализа и классификации инцидентов, а также оценки ущерба, нанесенного инцидентом ИБ;

процедуры реагирования на инцидент ИБ;

процедуры анализа причин инцидентов ИБ и оценки результатов реагирования на инциденты ИБ;

процедуры документирования и отчетности.

262. Разрабатываются и утверждаются руководством банка политика и план реагирования на инциденты ИБ.

263. В плане реагирования на инциденты ИБ устанавливаются:

цели и задачи;

область действия плана;

типы инцидентов;

уровни критичности инцидентов;

процедуры реагирования на инциденты в соответствии с выбранным банком жизненным циклом реагирования на инциденты;

роли и обязанности работников, задействованных в процедурах реагирования на инциденты;

процедуры взаимодействия как для внутренних, так и для внешних коммуникаций.

264. Определяются, выполняются, регистрируются и контролируются процедуры хранения и распространения информации об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ.

265. Определяются, выполняются, регистрируются и контролируются действия работников банка при обнаружении событий, связанных с ИБ, и информировании о данных событиях ответственных лиц. Работники банка осведомляются о порядке действий в случае обнаружении событий, связанных с ИБ.

266. Процедуры расследования инцидентов ИБ учитывают законодательство, в том числе нормативные правовые акты Национального банка, Оперативно-аналитического центра при Президенте Республики Беларусь, а также локальные правовые акты и организационно-распорядительные документы банка в области ИБ.

267. В банке принимаются, фиксируются и выполняются решения по всем выявленным инцидентам ИБ.

268. В банке определяются роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ и назначаются ответственные лица за выполнение указанных ролей.

ГЛАВА 26
ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ ИБ И ЕЕ ВОССТАНОВЛЕНИЯ ПОСЛЕ СБОЕВ

269. Непрерывность ИБ встраивается в систему менеджмента обеспечения непрерывности бизнеса организации.

270. Разрабатываются и утверждаются руководством банка политика обеспечения непрерывности ИБ.

271. В ПОНРВ предусматриваются инструкция и порядок действий работников банка по восстановлению ИБ и в части восстановления ИБ включаются:

цели плана;

область действия плана;

условия активации плана;

процедуры определения критически важных информационных активов;

оценка рисков ИБ, оценка уязвимостей и анализ их влияния на ИБ;

действия, которые должны быть предприняты после инцидента ИБ;

требования по обучению и повышению осведомленности работников банка в области ИБ;

процедуры резервного копирования и восстановления;

процедуры тестирования и проверки плана;

обязанности работников банка с указанием ответственных лиц за выполнение каждого из пунктов плана.

272. Разработка плана обеспечения непрерывности ИБ и ее восстановления после сбоев основывается на результатах оценок рисков ИБ и уязвимостей банка применительно к критически важным информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после сбоев.

273. Применение защитных мер обеспечения непрерывности ИБ и ее восстановления после сбоев основывается на соответствующих требованиях по обеспечению ИБ.

274. План обеспечения непрерывности ИБ и ее восстановления после сбоев коррелирует с планом реагирования на инциденты ИБ и процедурами обработки таких инцидентов, принятыми в банке.

275. Определяются, выполняются, регистрируются и контролируются процедуры периодического тестирования мероприятий плана обеспечения непрерывности ИБ и ее восстановления после прерывания. По результатам тестирования при необходимости проводится

соответствующая корректировка плана. Сценарий тестирования составляется с учетом разработанной в банке модели угроз и нарушителей, а также результатов оценок рисков ИБ и уязвимостей.

276. В банке реализуется программа обучения и повышения осведомленности работников в области обеспечения непрерывности ИБ и ее восстановления после сбоев.

277. В банке определяются роли по разработке плана обеспечения непрерывности ИБ и ее восстановления после сбоев и назначаются ответственные лица за выполнение указанных ролей.

ГЛАВА 27
ТРЕБОВАНИЯ К МОНИТОРИНГУ И ОЦЕНКЕ ЭФФЕКТИВНОСТИ СМИБ

278. Определяются, выполняются и регистрируются процедуры мониторинга и оценки эффективности СМИБ, включая процессы и средства управления ИБ.

279. В ходе реализации процедуры мониторинга и оценки эффективности СМИБ банком определяются:

объекты мониторинга и оценки эффективности, включая процессы и средства управления ИБ;

методы мониторинга и оценки эффективности, обеспечивающие достоверность результатов;

когда должен выполняться мониторинг и оценка эффективности;

кто должен осуществлять мониторинг и оценку эффективности.

280. При определении объектов мониторинга в их число в обязательном порядке включаются следующие системы, процессы и действия:

реализация процессов СМИБ;

управление инцидентами ИБ;

управление уязвимостями;

управление конфигурациями;

обучение и повышение осведомленности;

сбор и регистрация событий ИБ;

аудит ИБ;

оценка рисков ИБ;

обработка рисков ИБ;

управление непрерывностью ИБ;

управление физической безопасностью;

мониторинг информационной инфраструктуры.

В число объектов мониторинга банком в случае необходимости включаются и иные системы, процессы и действия, оказывающие существенное значение на обеспечение ИБ.

281. При определении объектов оценки эффективности в их число в обязательном порядке включаются следующие процессы и действия СМИБ:

планирование;

поддержка со стороны руководства банка;

управление рисками ИБ;

управление политикой;

управление ресурсами;

анализ управления;

обмен информацией;

документирование;

мониторинг.

В число объектов оценки эффективности банком в случае необходимости включаются иные процессы и действия СМИБ.

282. Банк самостоятельно определяет конкретные временные рамки проведения мониторинга и оценки эффективности СМИБ, но с учетом требований законодательства, в том числе нормативных правовых актов Национального банка, документов банка в области ИБ, международных стандартов и требований.

283. Банк самостоятельно определяет, кто будет проводить мониторинг и оценку эффективности СМИБ, указав конкретных лиц и их роли. При этом участие подразделения ИБ в процедуре мониторинга и оценки эффективности СМИБ является обязательным.

284. Мониторинг и оценка эффективности СМИБ выполняются вручную или с использованием средств автоматизации.

285. Процедуры мониторинга и оценки эффективности подвергаются регулярным, регистрируемым пересмотрам в связи с изменениями в СМИБ.

286. Результаты мониторинга и оценки эффективности СМИБ документируются и хранятся в банке.

ГЛАВА 28
ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ ВНУТРЕННЕГО АУДИТА ИБ

287. Документально определяется и реализуется программа проведения аудитов ИБ, содержащая информацию, необходимую для планирования и организации внутренних аудитов ИБ, контроля их проведения, анализа и совершенствования, а также обеспечения

ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в определенные сроки.

288. Проведение внутренних аудитов ИБ осуществляется банком.

289. В банке документально определяются, выполняются и контролируются процедуры:

формирования, сбора и хранения свидетельств внутренних аудитов ИБ;

хранения и использования результатов внутренних аудитов ИБ.

290. Для каждого проводимого в банке внутреннего аудита ИБ подготавливается план проведения аудита, содержащий информацию о:

цели проведения аудита ИБ;

критериях аудита ИБ;

области аудита ИБ;

дате начала и продолжительности проведения аудита ИБ;

составе работников банка, связанных с проведением аудита ИБ, и их обязанности;

проводимых в рамках аудита ИБ мероприятиях и деятельности;

распределении ресурсов при проведении аудита ИБ.

291. Банк обеспечивает объективность и беспристрастность процесса внутреннего аудита ИБ.

292. По результатам проведения внутренних аудитов ИБ подготавливаются документированные отчеты, содержащие рекомендации по устранению выявленных нарушений и несоответствий ИБ. Результаты внутренних аудитов ИБ, а также соответствующие отчеты доводятся до руководства банка.

293. В банке документально определяются роли, связанные с выполнением программы внутренних аудитов ИБ, и назначаются ответственные лица за выполнение указанных ролей.

ГЛАВА 29
ТРЕБОВАНИЯ К АНАЛИЗУ ФУНКЦИОНИРОВАНИЯ СМИБ

294. Определяются, выполняются, регистрируются и контролируются процедуры анализа функционирования СМИБ, использующие в том числе:

результаты мониторинга и оценки защищенности СМИБ;

сведения об инцидентах ИБ;

результаты проведения аудитов ИБ;

данные об угрозах и уязвимостях ИБ;

данные о внутренних и внешних факторах, оказывающих серьезное влияние на функционирование СМИБ, включая процессы и средства управления ИБ.

295. Анализ функционирования СМИБ включает:

анализ соответствия комплекта документов, регламентирующих деятельность по обеспечению ИБ в банке, требованиям законодательства, в том числе ТНПА, а также договорным условиям (требованиям) банка;

анализ соответствия локальных правовых актов, регламентирующих деятельность по обеспечению ИБ в банке, требованиям политик ИБ банка;

оценку рисков ИБ банка, включая оценку уровня остаточного и допустимого риска, а также оценку адекватности модели угроз банка существующим угрозам ИБ;

проверку адекватности используемых мер защиты требованиям документов банка и результатам оценки рисков ИБ;

анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании мер защиты.

296. Результаты анализа функционирования СМИБ документируются и хранятся в банке.

297. В банке определяются роли, связанные с процедурами анализа функционирования СМИБ, и назначаются ответственные лица за выполнение указанных ролей.

ГЛАВА 30
ТРЕБОВАНИЯ К АНАЛИЗУ СМИБ СО СТОРОНЫ РУКОВОДСТВА БАНКА

298. Руководство банка на плановой и регулярной основе осуществляет анализ СМИБ для того, чтобы удостовериться в следующем:

СМИБ разработана и функционирует с учетом специфики деятельности банка, его бизнес-процессов, информационных ресурсов и систем, угроз и рисков;

СМИБ разработана и функционирует в соответствии с законодательством, в том числе ТНПА, а также международными стандартами и требованиями;

СМИБ достигает поставленных целей обеспечения ИБ.

299. В банке устанавливается перечень документов (свидетельств, данных), необходимых для формирования информации, предоставляемой руководству банка с целью проведения анализа СМИБ. В частности, в указанный перечень входят:

документы (свидетельства, данные), содержащие информацию о действиях, предпринятых по итогам предыдущих анализов СМИБ, осуществленных руководством банка;

документы (свидетельства, данные), содержащие информацию об изменениях в состоянии внешних и внутренних факторов, которые оказывают существенное влияние на функционирование СМИБ;

документы с результатами мониторинга и оценкой защищенности СМИБ;

документы с результатами анализа функционирования СМИБ;

отчеты с результатами аудитов ИБ;

документы (свидетельства, данные), содержащие информацию о новых, выявленных уязвимостях и угрозах ИБ;

документы (свидетельства, данные), содержащие информацию по выявленным инцидентам ИБ и их обработке;

документы (свидетельства, данные), подтверждающие выполнение требуемой деятельности по достижению целей в области обеспечения ИБ;

документы (свидетельства, данные), содержащие информацию о результатах оценки рисков ИБ и выполнения плана обработки рисков ИБ;

документы (свидетельства, данные), подтверждающие выполнение требований непрерывности ИБ и ее восстановления после сбоев;

документы (свидетельства, данные), содержащие информацию о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СМИБ.

300. По результатам анализа СМИБ руководством банка принимаются решения о необходимости проведения мероприятий, направленных на повышение эффективности и надежности защиты информации в банке.

301. Результаты анализа СМИБ со стороны руководства банка документируются и хранятся в банке.

302. В банке определяются роли, связанные с подготовкой информации, необходимой для анализа СМИБ руководством банка, и назначаются ответственные лица за выполнение указанных ролей.

ГЛАВА 31
ТРЕБОВАНИЯ К ПРИНЯТИЮ РЕШЕНИЙ ПО УЛУЧШЕНИЮ СМИБ

303. Банком на постоянной основе осуществляется улучшение СМИБ, направленное на обеспечение соответствия требованиям безопасности, минимизацию рисков ИБ и повышение эффективности управления ИБ в банке.

304. Для принятия решений, связанных с улучшением СМИБ, рассматриваются, среди прочего, результаты

аудитов ИБ,

мониторинга и оценки защищенности СМИБ,

анализа функционирования СМИБ,

обработки инцидентов ИБ,

инвентаризации информационных активов банка,

выявления новых угроз и уязвимостей ИБ,

оценки рисков ИБ,

анализа СМИБ со стороны руководства банка,

анализа успешных практик в области ИБ,

а также изменения

состояния внешних и внутренних факторов, оказывающих существенное влияние на функционирование СМИБ,

интересов, целей и задач банка, в том числе в части обеспечения ИБ,

контрактных обязательств банка.

305. При выявлении фактов несоответствия СМИБ установленным требованиям, включая политики, процедуры и средства управления ИБ:

документируются выявленные несоответствия;

принимаются меры для скорейшего устранения выявленных несоответствий;

оцениваются возможные последствия выявленных несоответствий и принимаются меры к их минимизации и (или) устранению;

анализируются предпосылки, причины и обстоятельства возникновения несоответствий с целью недопущения их повторного возникновения;

оценивается результативность и эффективность принятых корректирующих мер;

информируются заинтересованные стороны о внесении изменений в СМИБ.

306. Деятельность по улучшению СМИБ осуществляется в рамках разработанного плана улучшений СМИБ, содержащего информацию о:

процедурах и процессах СМИБ, подлежащих улучшению;

планируемых мероприятиях по их улучшению;

сроках проведения мероприятий;

ответственных лицах за проведение мероприятий;

результатах выполненных мероприятий по улучшению СМИБ.

307. Вся деятельность по улучшению СМИБ документируется.

308. Принятие и осуществление корректирующих мер в рамках улучшения СМИБ согласовывается подразделением ИБ, санкционируется и контролируется руководством банка.

309. Определяются, выполняются, регистрируются и контролируются процедуры информирования руководства и структурных подразделений банка об улучшениях СМИБ, в частности, об изменениях, касающихся требований по обеспечению ИБ и ответственности за их невыполнение.

310. В банке определяются и назначаются роли по улучшению СМИБ и назначаются ответственные лица за выполнение указанных ролей.