Рег. № 04-11/28
«4» июня 2026 года

«УТВЕРЖДЕНО»
Наблюдательным советом
АО «ANOR BANK»
Протоколом №25 от
«26» мая 2026 года

Председатель Наблюдательного совета
АО «ANOR BANK»

_____
(подпись)
Носиров Ш. Н.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АКЦИОНЕРНОГО ОБЩЕСТВА

«ANOR BANK»

Ташкент - 2026

Содержание

Приложение 9	Перечень программного обеспечения, разрешённого к использованию
Приложение 10	Правила работы с сетью Интернет и корпоративной электронной почтой
Приложение 11	Правила управления информационными активами
Приложение 12	Правила организации технической защиты информации
Приложение 13	Правила организации криптографической защиты информации
Приложение 14	Порядок восстановления деятельности в чрезвычайных ситуациях и обеспечения непрерывности деятельности
Приложение 15	Регламент реагирования на инциденты информационной безопасности
Приложение 16	Журнал ознакомления с Политикой информационной безопасности
Приложение 17	Методология оценки рисков информационной безопасности
Приложение 18	Перечень аппаратно-программных и программных средств, используемых в Банке

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Введение

Политика информационной безопасности Акционерного общества «ANOR BANK» (далее - Банк) (далее - Политика) определяет подходы и методы обеспечения информационной безопасности, принятые руководством Банка в целях осуществления деятельности, представляет собой систематизированный комплекс целей и задач высокого уровня в области защиты информации, которыми Банк должен руководствоваться в своей деятельности, а также устанавливает основные принципы построения системы управления информационной безопасностью Банка (далее - СУИБ).

Банк является коммерческим цифровым банком и уделяет приоритетное внимание осуществлению деятельности по предоставлению банковских услуг в интерактивном режиме через веб-сайт или мобильные приложения (далее - цифровые банковские услуги) на территории Республики Узбекистан.

Для осуществления своей деятельности Банк эффективно внедряет и применяет цифровые технологии, на основе которых формируется и развивается информационно-коммуникационная инфраструктура Банка.

Обеспечение информационной безопасности является приоритетной задачей в условиях необходимости предоставления цифровых банковских услуг, а также обеспечения надёжного и бесперебойного функционирования информационно-коммуникационной инфраструктуры в целях соблюдения требований законодательства Республики Узбекистан в области информационной безопасности.

Обеспечение информационной безопасности включает любую деятельность, направленную на защиту информационных ресурсов и информационных систем Банка.

Основной целью настоящей Политики является снижение угроз информационной безопасности в пределах всей информационной инфраструктуры Банка для повышения устойчивости его деятельности в целом.

Информационная безопасность рассматривается с точки зрения обеспечения конфиденциальности, целостности и доступности защищаемой конфиденциальной информации, включая коммерческую и банковскую тайну, персональные данные работников и клиентов Банка, сведения об имуществе Банка, а также обеспечения непрерывного и бесперебойного функционирования процессов обработки информации. В область обеспечения информационной безопасности входят информационные системы и информационные ресурсы Банка, включая автоматизированную банковскую систему (далее - АБС).

Информационная безопасность достигается посредством внедрения и реализации комплекса мер, включающего политики, практики, процедуры и организационные структуры.

Комплекс мер по обеспечению информационной безопасности должен обеспечивать защиту информации (данных) и информационно-коммуникационной инфраструктуры Банка от широкого спектра угроз в целях поддержания непрерывности предоставления цифровых банковских услуг, минимизации ущерба от реализации угроз, прогнозирования и предотвращения их воздействия, сохранения деловой репутации Банка и соблюдения требований законодательства.

Настоящая Политика представляет собой совокупность документированных руководящих принципов, правил, процедур и практических методов в области обеспечения информационной безопасности, которыми Банк руководствуется при осуществлении своей деятельности.

Настоящая Политика распространяется на все структурные подразделения Банка и является обязательной для исполнения всеми работниками и должностными лицами Банка. Положения настоящей Политики подлежат применению при разработке и использовании внутренних нормативных документов Банка.

1.2. Нормативные документы, используемые при разработке

1) Политика информационной безопасности Банка разработана в целях обеспечения информационной безопасности объектов информатизации в соответствии со следующими нормативно-правовыми актами Республики Узбекистан:

2) Закон Республики Узбекистан от 11 декабря 2003 года № 560-II «Об информатизации».

3) Закон Республики Узбекистан от 30 августа 2003 года № 530-II «О банковской тайне».

4) Закон Республики Узбекистан от 29 апреля 2004 года № 611-II «Об электронном документообороте».

5) Закон Республики Узбекистан от 4 апреля 2006 года № 30 «О защите информации в автоматизированной банковской системе».

6) Закон Республики Узбекистан от 11 сентября 2014 года №-374 «О коммерческой тайне».

7) Закон Республики Узбекистан от 2 июля 2019 года №-547 «О персональных данных».

8) Закон Республики Узбекистан от 1 ноября 2019 года №-578 «О платежах и платежных системах».

9) Закон Республики Узбекистан от 5 ноября 2019 года №-580 «О внесении изменений и дополнений в Закон Республики Узбекистан „О банках и банковской деятельности“».

10) Закон Республики Узбекистан от 15 апреля 2022 года №-764 «О кибербезопасности».

11) Закон Республики Узбекистан от 29 сентября 2022 года №-792 «Об электронной коммерции».

12) Закон Республики Узбекистан от 12 октября 2022 года №-793 «Об электронной цифровой подписи».

13) Указ Президента Республики Узбекистан от 15 июня 2020 года № УП-6007 «О мерах по внедрению государственной системы защиты информационных систем и ресурсов Республики Узбекистан».

14) Постановление Президента Республики Узбекистан от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан».

15) Постановление Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572 «О мерах по защите национальных информационных ресурсов».

16) Постановление Президента Республики Узбекистан от 21 ноября 2018 года № ПП-4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций и обеспечением их защиты».

17) Постановление Президента Республики Узбекистан от 14 сентября 2019 года № ПП-4452 «О дополнительных мерах по совершенствованию системы мониторинга внедрения информационных технологий и коммуникаций и организации их защиты».

18) Постановление Президента Республики Узбекистан от 15 июня 2020 года № ПП-4751 «О мерах по дальнейшему совершенствованию системы обеспечения кибербезопасности в Республике Узбекистан».

19) Постановление Президента Республики Узбекистан от 1 июля 2021 года № ПП-5170 «О мерах по совершенствованию кибербезопасности в деятельности операторов платежных систем, кредитных организаций и платежных организаций».

20) Постановление Президента Республики Узбекистан от 31 мая 2023 года № ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан».

21) Постановление Кабинета Министров Республики Узбекистан от 26 марта 1999 года № 137 «Об утверждении Положения о порядке подготовки и распространения информационных ресурсов Республики Узбекистан в сетях передачи данных, включая сеть Интернет».

22) Постановление Кабинета Министров Республики Узбекистан от 22 ноября 2005 года № 256 «О совершенствовании нормативно-правовой базы в сфере информатизации».

23) Постановление Кабинета Министров Республики Узбекистан от 4 мая 2011 года № 126 «О мерах по внедрению и использованию единой защищённой электронной почты и системы электронного документооборота в исполнительном аппарате Кабинета Министров, органах государственного и хозяйственного управления, а также органах государственной власти на местах».

24) Постановление Кабинета Министров Республики Узбекистан от 7 ноября 2011 года № 296 «О мерах по реализации Постановления Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572 „О дополнительных мерах по защите национальных информационных ресурсов“».

25) Постановление Кабинета Министров Республики Узбекистан от 16 октября 2015 года № 295 «Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан».

26) Постановление Кабинета Министров Республики Узбекистан от 17 декабря 2015 года № 365 «О мерах по формированию централизованных баз данных физических и юридических лиц и внедрению Единой информационной системы идентификации пользователей системы „Электронное правительство“».

27) Постановление Кабинета Министров Республики Узбекистан от 21 ноября 2019 года № 930 «Об утверждении перечня объектов, подлежащих охране подразделениями Главного управления охраны Национальной гвардии Республики Узбекистан».

28) Постановление Кабинета Министров Республики Узбекистан от 5 октября 2022 года № 570 «Об утверждении отдельных нормативно-правовых актов в сфере обработки персональных данных».

29) Постановление Правления Центрального банка Республики Узбекистан «Об утверждении Положения об обеспечении информационной безопасности в платежных системах операторов платежных систем и поставщиков платежных услуг», зарегистрированное Министерством юстиции Республики Узбекистан 14 февраля 2006 года за № 1545.

30) Постановление Правления Центрального банка Республики Узбекистан от 25 января 2020 года № 2/4 «Об утверждении Положения о защите информации в автоматизированных системах коммерческих банков Республики Узбекистан», зарегистрированное Министерством юстиции Республики Узбекистан 10 марта 2020 года за № 3224 (новая редакция - № 3224-2 от 2023 года).

31) Постановление Правления Центрального банка Республики Узбекистан «Об утверждении Положения об обеспечении информационной безопасности в платежных системах операторов платежных систем и поставщиков платежных услуг», зарегистрированное Министерством юстиции Республики Узбекистан 21 мая 2024 года за № 3531.

32) Приказ Председателя Службы государственной безопасности Республики Узбекистан от 4 сентября 2023 года № 91 «Об утверждении Положения о порядке оценки уровня обеспечения кибербезопасности в Республике Узбекистан и кибербезопасности объектов критической информационной инфраструктуры», зарегистрированный Министерством юстиции Республики Узбекистан 22 сентября 2023 года за № 3458.

33) Приказ Министерства юстиции Республики Узбекистан от 14 ноября 2023 года № 19-мх «Об утверждении Типового порядка организации деятельности структурного подразделения или уполномоченного лица,

обеспечивающего обработку и защиту персональных данных владельцем и (или) оператором базы персональных данных», зарегистрированный Министерством юстиции Республики Узбекистан 15 ноября 2023 года за № 3477.

34) Приказ Министерства юстиции Республики Узбекистан от 15 ноября 2023 года № 20-мх «Об утверждении Порядка обработки персональных данных», зарегистрированный Министерством юстиции Республики Узбекистан 15 ноября 2023 года за № 3478.

35) Инструкция о порядке учёта, обработки и хранения документов, файлов и изданий, содержащих сведения ограниченного распространения, утверждённая 5 декабря 2006 года председателем Межведомственной комиссии по обеспечению сохранности государственных секретов при заместителе Премьер-министра Республики Узбекистан.

36) Национальный стандарт 816:2025 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по разработке политики информационной безопасности».

37) ГС РУз 1092:2009 «Информационные технологии. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

38) ГС РУз 1108:2011 «Информационные технологии. Взаимосвязь открытых систем. Структура сертификата открытого ключа и атрибутного сертификата».

39) ГС РУз 1047:2018 «Информационные технологии. Термины и определения».

40) ГС РУз 1109:2013 «Информационные технологии. Криптографическая защита информации. Термины и определения».

41) ГС РУз 2927:2015 «Информационные технологии. Информационная безопасность. Термины и определения».

42) ГС РУз 2590:2012 «Информационные технологии. Требования к интеграции и взаимодействию информационных систем, используемых государственными органами в рамках формирования национальной информационной системы».

43) ГС РУз 2814:2014 «Информационные технологии. Автоматизированные системы. Классификация по уровням защищённости от несанкционированного доступа к информации».

44) ГС РУз 2815:2014 «Информационные технологии. Межсетевые экраны. Классификация по уровням защищённости от несанкционированного доступа к информации».

45) ГС РУз 2816:2014 «Информационные технологии. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недекларированных возможностей».

46) ГС РУз 2817:2014 «Информационные технологии. Средства вычислительной техники. Классификация по уровням защищённости от несанкционированного доступа к информации».

47) ГС РУз 2875:2014 Требования к центрам обработки данных. Обеспечение готовности и безопасности инфраструктуры телекоммуникационных объектов в соответствии со стандартом «Инфраструктура и обеспечение информационной безопасности».

48) ГС РУз 3078:2016 «Телекоммуникационные сети. Виртуальные частные сети (VPN). Общие требования».

49) ГС РУз 3243:2017 «Информационные технологии. Локальные и корпоративные вычислительные сети. Общие технические требования».

50) ГС РУз 3386:2019 (ГС РУз ISO/IEC 27035-1:2016, MOD) «Информационные технологии. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы управления инцидентами».

51) ГС РУз 3387:2019 (ГС РУз ISO/IEC 27035-2:2016, MOD) «Информационные технологии. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 2. Руководящие указания по планированию реагирования на инциденты и подготовке к ним».

52) ГС РУз ISO/IEC 11770-1:2017 «Информационные технологии. Методы обеспечения безопасности. Управление ключами. Часть 1. Основные положения».

53) ГС РУз ISO/IEC 13335-1:2009 «Информационные технологии. Методы обеспечения безопасности. Управление безопасностью информационных и коммуникационных технологий. Часть 1. Концепции и модели управления безопасностью информационных и коммуникационных технологий».

54) ГС РУз ISO/IEC 15408-1:2016 «Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

55) ГС РУз ISO/IEC 15408-2:2016 «Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности».

56) ГС РУз ISO/IEC 15408-3:2016 «Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

57) ГС РУз ISO/IEC 27000:2022 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Общий обзор и словарь».

58) ГС РУз ISO/IEC 27001:2020 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования».

59) ГС РУз ISO/IEC 27002:2016 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью».

60) ГС РУз ISO/IEC 27003:2022 «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью».

61) O‘zMSt ISO/IEC 27005:2024 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по управлению рисками информационной безопасности».

62) ГС РУз ISO/IEC 27007:2022 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие указания по аудиту систем управления информационной безопасностью».

63) ГС РУз ISO/IEC 27008:2022 «Информационные технологии. Методы обеспечения безопасности. Руководство для аудиторов по оценке мер управления информационной безопасностью».

64) ГС РУз ISO/IEC 27010:2015 «Информационные технологии. Методы обеспечения безопасности. Руководство по управлению информационной безопасностью при межотраслевых и межорганизационных коммуникациях».

65) ГС РУз ISO/IEC 27014:2018 «Информационные технологии. Методы обеспечения безопасности. Корпоративное управление информационной безопасностью».

66) ГС РУз ISO/IEC 27031:2016 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению готовности информационно-коммуникационных технологий для поддержания непрерывности деятельности».

67) ГС РУз ISO/IEC 27032:2017 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности».

68) ГС РУз ISO/IEC 27033-1:2016 «Информационные технологии. Методы обеспечения безопасности. Сетевая безопасность. Часть 1».

69) ГС РУз ISO/IEC 27033-2:2016 «Информационные технологии. Методы обеспечения безопасности. Сетевая безопасность. Часть 2. Руководящие указания по проектированию и внедрению сетевой безопасности».

70) ГС РУз ISO/IEC 27033-4:2016 «Информационные технологии. Методы обеспечения безопасности. Сетевая безопасность. Часть 4. Обеспечение безопасности взаимодействия сетей с использованием шлюзов безопасности».

71) ГС РУз ISO/IEC 27033-5:2016 «Информационные технологии. Методы обеспечения безопасности. Сетевая безопасность. Часть 5. Коммуникации для обеспечения межсетевой безопасности с использованием виртуальных частных сетей (VPN)».

72) ГС РУз ISO/IEC 27033-6:2018 «Информационные технологии. Методы обеспечения безопасности. Сетевая безопасность. Часть 6. Безопасный доступ к беспроводным IP-сетям».

73) ГС РУз ISO/IEC 27037:2017 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по идентификации, сбору, получению и сохранению цифровых доказательств».

74) ГС РУз ISO/IEC 27039:2018 «Информационные технологии. Методы обеспечения безопасности. Выбор, внедрение и эксплуатация систем обнаружения вторжений».

75) ГС РУз ISO/IEC 27040:2018 «Информационные технологии. Методы обеспечения безопасности. Безопасность хранения данных».

76) Стандарт безопасности данных индустрии платёжных карт PCI DSS (Payment Card Industry Data Security Standard) - международный стандарт информационной безопасности в индустрии платёжных карт, устанавливающий совокупность требований к обеспечению безопасности данных держателей платёжных карт.

77) Правила контроля доступа в Банке, утверждённые протоколом Правления Банка № 7 от 24 сентября 2020 года.

78) Порядок управления чрезвычайными ситуациями в сфере ИТ-услуг, утверждённый протоколом Правления Банка № 26 от 22 августа 2022 года.

79) Инструкция о порядке учёта, ведения и хранения документов и файлов, содержащих сведения ограниченного распространения (ДСП), утверждённая протоколом Правления Банка № 32 от 12 февраля 2022 года.

80) Положение о соблюдении режима коммерческой тайны (конфиденциальности), утверждённое протоколом Правления Банка № 32 от 2 декабря 2022 года.

81) Положение о порядке обработки персональных данных работников АО «ANOR BANK», утверждённое протоколом Правления Банка № 7-1 от 16 мая 2023 года.

1.3. Термины и определения

В настоящей Политике используются следующие термины, определения и сокращения:

Автоматизированная банковская система (АБС) - система, состоящая из средств автоматизации банковских процессов и персонала Банка, обеспечивающая применение банковских информационных технологий для выполнения определённых функций.

информационные ресурсы - информация в электронной форме, банки данных и базы данных, входящие в состав информационной системы.

информационная система - организационно упорядоченная совокупность информационных ресурсов, информационных технологий и средств связи, обеспечивающая сбор, хранение, поиск, обработку и использование информации.

инцидент информационной безопасности - единичное событие либо серия нежелательных или неожиданных событий информационной

безопасности, которые создают высокую вероятность компрометации информации либо реализации угроз информационной безопасности.

аутентификация - процесс проверки подлинности идентификатора, представленного пользователем для получения права доступа к информационному ресурсу; подтверждение правомерности доступа к ресурсу.

объект информатизации - информационные системы различного уровня и назначения, телекоммуникационные сети, технические средства обработки информации, помещения, в которых данные средства размещаются и эксплуатируются, а также помещения, предназначенные для проведения переговоров, включая конфиденциальные переговоры.

система управления информационной безопасностью (суиб) - часть общей системы управления, основанная на использовании методов оценки бизнес-рисков и предназначенная для разработки, внедрения, функционирования, мониторинга, анализа, сопровождения и постоянного совершенствования информационной безопасности.

защита информации - деятельность, направленная на предотвращение распространения защищаемой информации, а также на предотвращение несанкционированного или непреднамеренного воздействия на защищаемую информацию и программно-технические средства доступа к ней.

информационная безопасность - состояние защищённости информации, её носителей и инфраструктуры от раскрытия информации (нарушения конфиденциальности), нарушения целостности баз данных и информационных ресурсов, утраты либо снижения уровня доступности информации.

информационная инфраструктура - совокупность базовых информационных сервисов и сетей, вычислительных систем, систем хранения, обработки и передачи данных, обеспечивающих функционирование любых информационных услуг.

интеллектуальная собственность - изобретения, разработки, товарные знаки, фирменные наименования, коммерческие обозначения, наименования и изображения, являющиеся собственностью банка.

система мониторинга и управления инцидентами информационной безопасности (siem) - система, обеспечивающая сбор, хранение, мониторинг и управление событиями информационной безопасности, выявление инцидентов на основе анализа потока событий и оперативное информирование аналитиков о выявленных событиях.

событие информационной безопасности (далее - событие) - выявленное состояние системы, сервиса или сети, указывающее на возможное нарушение политики безопасности, отказ средств защиты либо ранее неизвестную ситуацию, которая может иметь отношение к безопасности.

средства криптографической защиты информации (скзи) - совокупность программных и технических компонентов систем обработки данных, способных функционировать самостоятельно либо в составе других систем и осуществляющих криптографическое преобразование информации для обеспечения её безопасности.

банковская тайна - охраняемые банком сведения:

- об операциях, счетах и вкладах своих клиентов (корреспондентов);
- полученные банком о клиенте (корреспонденте) в связи с оказанием ему банковских услуг;
- о наличии, характере и стоимости имущества клиента (корреспондента), находящегося в сейфах и помещениях банка;
- о межбанковских сделках и сделках, совершённых по поручению либо в интересах клиента (корреспондента);
- о клиенте (корреспонденте) другого банка, ставшие известными в результате обмена сведениями, составляющими банковскую тайну, между банками.

Банковская телекоммуникационная сеть Центрального банка Республики Узбекистан (БТС) - совокупность технологий, обеспечивающих централизованный контроль, управление процессами сбора и обработки банковской информации, управление ресурсами, а также эффективность, надёжность и безопасность функционирования платёжной системы.

бизнес-процесс - последовательность технологически взаимосвязанных операций по предоставлению продуктов, оказанию услуг и (или) осуществлению определённого вида деятельности.

нарушитель - физическое или юридическое лицо, заинтересованное в несанкционированном доступе к информационной системе и её ресурсам и предпринимающее преднамеренные действия для получения либо изменения информации без соответствующих полномочий.

виртуальная частная сеть (vpn) - технология, обеспечивающая установление защищённого соединения через сеть интернет.

программное обеспечение - совокупность программ и программной документации, необходимых для функционирования системы обработки данных.

конфиденциальная информация - документированная информация, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством.

система контроля и управления доступом (скуд) - совокупность программно-аппаратных средств контроля и управления доступом.

система обнаружения и предотвращения вторжений (idps) - совокупность программных и (или) аппаратных средств, предназначенных для выявления и предотвращения попыток несанкционированного доступа к корпоративной системе.

система электронного документооборота (сэд) - система обмена электронными документами внутри банка, а также с партнёрскими организациями и государственными органами, обеспечивающая создание, согласование, отправку, получение, архивирование и повторное использование информации.

электронная цифровая подпись (эцп) - реквизит электронного документа, позволяющий подтвердить авторство, время подписания документа и отсутствие внесённых в него изменений.

база данных - совокупность данных (статей, расчётов), представленных в объективной форме и систематизированных таким образом, чтобы их можно было находить и обрабатывать с использованием электронно-вычислительной техники.

система управления базами данных (субд) - программное обеспечение, предназначенное для создания, управления, актуализации и анализа баз данных.

центр обработки данных (цод) - физический объект, предназначенный для размещения вычислительного оборудования и сопутствующих аппаратных средств.

контролируемая зона - место (территория, здание или часть здания), в котором запрещено неконтролируемое пребывание посторонних лиц и транспортных средств, не имеющих постоянного или разового разрешения на доступ.

Примечание**.** Границей контролируемой зоны могут являться:

– периметр контролируемой территории организации;

– ограждающие конструкции защищаемого здания либо его охраняемой части, если они расположены вне защищённой территории.

оценка рисков - процесс сопоставления рассчитанного риска с установленными критериями риска в целях определения его характера и значимости.

риск информационной безопасности - возможность использования определённой уязвимости системы обработки данных при реализации конкретной угрозы.

анализ рисков - систематическое выполнение процессов идентификации ресурсов системы обработки данных, угроз этим ресурсам и уязвимостей системы по отношению к данным угрозам.

несанкционированный доступ - доступ субъекта к объекту или информации с нарушением установленных правил разграничения доступа в системе.

обработка риска - процесс выбора и реализации мер по изменению (снижению) риска.

персональные данные - информация, относящаяся к идентифицированному или идентифицируемому физическому лицу и позволяющая установить его личность.

угроза - потенциальная возможность нарушения безопасности компьютерной системы либо информационных ресурсов.

коммерческая тайна - сведения, имеющие коммерческую ценность вследствие неизвестности третьим лицам, относящиеся к научно-технической, технологической, производственной, финансовой, экономической и иной деятельности, к которым отсутствует свободный доступ на законном основании и в отношении которых их владелец принимает меры по обеспечению конфиденциальности.

уязвимость - недостаток системы обработки данных, использование которого может привести к нарушению её целостности и некорректному функционированию.

Система управления привилегированным доступом (Privilege Access Management, PAM) - система, предназначенная для обеспечения безопасности критически важных активов корпоративной сети клиента (информационных систем, информационных ресурсов и оборудования) при организации доступа разработчиков, администраторов, а также представителей сторонних организаций для выполнения работ по сопровождению и администрированию.

интеллектуальная собственность - изобретения, разработки, товарные знаки, фирменные наименования, коммерческие обозначения, а также принадлежащие Банку наименования и графические изображения.

учётная запись - совокупность сведений о пользователе, хранящихся в компьютерной системе и необходимых для его идентификации (аутентификации), а также предоставления доступа к персональным данным и настройкам. Как правило, учётная запись представляет собой комбинацию логина и пароля.

1.4. Область применения

Политика информационной безопасности Банка определяет цели и задачи Банка в области информационной безопасности, а также правила, процедуры, практики и руководящие документы, которыми Банк руководствуется в своей деятельности.

Политика информационной безопасности Банка должна использоваться в качестве основы для создания интегрированной системы управления информационной безопасностью (СУИБ), включая разработку внутренних нормативных документов Банка по информационной безопасности, а также реализацию организационно-технических и иных мер по обеспечению информационной безопасности.

Требования настоящей Политики распространяются на всю защищаемую информацию Банка и средства её создания, обработки, хранения, передачи, защиты и уничтожения, за исключением информации, содержащей сведения, составляющие государственную тайну. Защита информации, содержащей государственную тайну, обеспечивается в соответствии с законодательством Республики Узбекистан в области защиты государственных секретов.

В состав Банка входят:

а) Головной офис - здание, предназначенное для размещения структурных подразделений Головного офиса, а также организации пункта обслуживания клиентов на первом этаже (г. Ташкент, ул. Сайрам, 5-й проезд, собственное здание);

б) ИТ-офис - здание, в котором размещены ИТ-подразделения Головного офиса (г. Ташкент, ул. Мукими, дом 59, на условиях аренды);

в) офисы продаж - пункты обслуживания клиентов Банка.

Кроме того, в структуру Банка входят основной центр обработки данных (ЦОД), расположенный в Головном офисе, а также резервный центр обработки данных, размещённый в дата-центре АТС-233 АК «Узбектелеком» (г. Ташкент, ул. Истиклол, 51).

Для организации основного и резервного центров обработки данных Банк использует собственные средства обработки и хранения информации (серверы и системы хранения данных).

Для организации резервного центра обработки данных Банк арендует помещения в центре обработки данных АТС-233 АК «Узбектелеком» и использует инфраструктуру, обеспечивающую функционирование дата-центра (системы бесперебойного электроснабжения, кондиционирования, пожаротушения и иные инженерные системы).

Подключение указанных центров обработки данных к корпоративной сети Банка и внешним сетям Центрального банка Республики Узбекистан (сети Интернет, Банковской телекоммуникационной сети (далее - БТС)) организуется Банком самостоятельно.

Требования настоящей Политики распространяются на:

а) все информационные системы и информационные ресурсы Банка;

б) всех работников Банка (штатных, временных, работающих по договору и иных), независимо от их места работы и занимаемой должности;

в) третьих лиц, взаимодействующих с Банком (клиентов Банка, поставщиков, арендаторов, подрядчиков, аудиторов, посетителей, обслуживающий персонал, внешних пользователей информационных систем и иных лиц), которые по каким-либо основаниям имеют законный доступ к помещениям и объектам защиты Банка, включая его информационные ресурсы и информационные системы.

Правление Банка, руководители структурных подразделений, а также Управление информационной безопасности обязаны обеспечивать постоянный мониторинг соблюдения требований настоящей Политики.

Функции и задачи управления информационной безопасностью утверждаются в установленном порядке в составе соответствующего Положения о подразделении.

2. ЦЕЛИ И ЗАДАЧИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКЕ

2.1. Цели обеспечения информационной безопасности Банка

Целями обеспечения информационной безопасности Банка являются:

– защита субъектов информационных отношений Банка и пользователей банковских услуг (далее - клиенты Банка) от материального, физического, морального и иного ущерба, который может быть причинён в результате случайной или преднамеренной реализации угроз информационной безопасности;

– обеспечение конфиденциальности, целостности и доступности информации, связанной с деятельностью Банка, а также обеспечение функционирования критически важных информационных ресурсов, информационных систем и иных объектов информатизации;

– обеспечение соблюдения требований законодательства Республики Узбекистан в области информационной безопасности, нормативных документов, инструкций, положений и настоящей Политики;

– защита законных прав субъектов информационных отношений и клиентов Банка на неразглашение сведений, составляющих коммерческую тайну, банковскую тайну, персональных данных и иной конфиденциальной информации;

– защита объектов информатизации Банка от угроз информационной безопасности в целях обеспечения их устойчивого и надёжного функционирования, необходимого для успешного и непрерывного предоставления банковских услуг;

– обеспечение устойчивости деятельности Банка посредством гарантирования доступности необходимой информации и поддержания непрерывности деятельности;

– формирование сбалансированного подхода к защите от угроз информационной безопасности посредством применения экономически и технически обоснованных, а также необходимых и достаточных мер обеспечения информационной безопасности.

2.2. Задачи обеспечения информационной безопасности Банка

Для достижения целей обеспечения информационной безопасности в Банке решаются следующие задачи:

– создание, внедрение и развитие системы управления информационной безопасностью (СУИБ) в соответствии с требованиями бизнеса, законодательства и нормативных документов;

– внедрение эффективных методов и средств управления информационной безопасностью для защиты объектов информатизации Банка и защищаемой информации от различных угроз, а также для снижения рисков информационной безопасности;

– обеспечение постоянного мониторинга состояния информационной безопасности в целях своевременного выявления и устранения угроз информационной безопасности;

– создание механизмов и условий для оперативного реагирования на угрозы информационной безопасности и инциденты информационной безопасности;

– повышение уровня осведомлённости пользователей и работников Банка, а также уровня квалификации специалистов в области информационной безопасности, обеспечение их вовлечённости в процессы управления информационной безопасностью;

– обеспечение контроля за соблюдением пользователями и работниками Банка требований по защите информации в процессе её обработки;

– разработка и совершенствование нормативной и методологической базы по обеспечению информационной безопасности;

– организация антивирусной защиты информационных активов Банка;

– повышение уровня защищённости и надёжности функционирования критически важных объектов информатизации Банка.

–

3. ОСНОВНЫЕ ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Политика информационной безопасности Банка основывается на следующих принципах

1) Законность - соблюдение требований законодательства и нормативных документов при обеспечении информационной безопасности.

2) Вовлечённость - руководство Банка и все работники Банка участвуют в процессах управления информационной безопасностью.

3) Разграничение обязанностей - роли, полномочия и ответственность в вопросах обеспечения информационной безопасности должны быть чётко распределены между работниками Банка.

4) Персональная ответственность - работники Банка несут персональную ответственность за соблюдение требований информационной безопасности, предусмотренных трудовыми договорами, должностными инструкциями, а также иными договорами (соглашениями), заключёнными с Банком.

5) Профессионализм - уровень знаний и профессиональная квалификация работников Банка, ответственных за обеспечение информационной безопасности, должны постоянно совершенствоваться и применяться в процессах управления информационной безопасностью.

6) Взаимодействие и координация действий - деятельность по обеспечению информационной безопасности осуществляется во взаимодействии с заинтересованными сторонами и на основе согласованности целей, задач, принципов и средств обеспечения информационной безопасности.

7) Усиленная защита - меры обеспечения информационной безопасности должны выбираться с учётом необходимости организации эффективной защиты от всех видов угроз информационной безопасности.

8) Системный подход - при построении системы управления информационной безопасностью (СУИБ) Банка должны учитываться все элементы, условия и факторы, оказывающие влияние на обеспечение информационной безопасности и изменяющиеся во времени.

9) Комплексность - комплексное применение методов и средств защиты информации предполагает согласованное использование разнородных средств защиты при построении целостной системы защиты, исключающей наличие уязвимостей в отдельных её элементах и обеспечивающей перекрытие всех существенных каналов реализации угроз.

10) Непрерывность защиты - процесс обеспечения информационной безопасности должен осуществляться на постоянной основе и охватывать все уровни деятельности Банка.

11) Многоуровневая защита - процессы управления информационной безопасностью должны реализовываться на всех уровнях и во всех структурных звеньях Банка.

12) Подотчётность и регистрация действий - обеспечение мониторинга соблюдения работниками Банка требований информационной безопасности, управление доступом к информационным активам, а также регистрация всех действий работников, связанных с использованием информационных активов.

13) Своевременность - предполагает проактивный характер мер по обеспечению информационной безопасности, предусматривающий постановку задач по комплексной защите информации и реализацию мер обеспечения информационной безопасности на ранних этапах создания и развития информационных систем и систем защиты информации.

14) Достаточность - уровень затрат на обеспечение информационной безопасности должен соответствовать ценности информационных ресурсов и размеру потенциального ущерба, который может возникнуть вследствие их раскрытия, утраты, утечки, уничтожения или искажения. Применяемые меры и средства обеспечения информационной безопасности не должны существенно ухудшать эргономические характеристики компонентов информационных систем Банка.

15) Персональная ответственность - каждый работник несёт ответственность за обеспечение безопасности информации и систем её обработки в пределах своих полномочий. В соответствии с данным принципом распределение прав и обязанностей работников должно быть организовано таким образом, чтобы в случае возникновения нарушения круг ответственных лиц мог быть однозначно определён либо максимально ограничен.

3.2. В процессе реализации задач по обеспечению информационной безопасности Банк:

- формирует нормативную базу, регулирующую процессы обеспечения информационной безопасности банковской информационно-коммуникационной инфраструктуры Банка;
- определяет и классифицирует информацию Банка и иные объекты защиты;
- осуществляет объективный и всесторонний анализ и прогнозирование угроз информационной безопасности, а также анализ и оценку рисков информационной безопасности;
- разрабатывает требования и меры по обеспечению информационной безопасности в банковской информационно-коммуникационной инфраструктуре Банка;
- организует деятельность необходимых структурных подразделений по реализации комплекса мероприятий, направленных на предупреждение, отражение и нейтрализацию угроз информационной безопасности;

– обеспечивает внедрение, развитие и контроль использования средств защиты информации, а также организует сертификацию и лицензирование деятельности в области информационной безопасности в соответствии с требованиями законодательства;

– осуществляет периодическую оценку состояния защищённости информационных активов, выявляет, регистрирует и обеспечивает оперативное реагирование на действующие, продолжающиеся или потенциальные нарушения информационной безопасности.

3.3. Конкретные методы и мероприятия, реализуемые в рамках выполнения задач по обеспечению информационной безопасности Банка, приведены в разделе 7 настоящей Политики.

4. ОБЪЕКТЫ ЗАЩИТЫ

4.1. Основными объектами защиты информационной безопасности Банка являются:

1) Конфиденциальная информация, включая:

– служебную (деловую) информацию ограниченного распространения;

– сведения, составляющие коммерческую тайну Банка, его клиентов, партнёров и контрагентов в рамках договорных отношений;

– сведения, составляющие банковскую тайну;

– персональные данные работников и клиентов Банка;

– платёжную информацию и документацию платёжных систем.

2) Технологические процессы Банка,

включая информационные и платёжные процессы, реализуемые в информационных системах Банка.

3) Субъекты информационных отношений:

– клиенты Банка и сведения об осуществляемых ими операциях;

– работники Банка;

– разработчики программного обеспечения информационных систем Банка.

4) Объекты интеллектуальной собственности Банка.

5) Аппаратные средства:

рабочие станции, ноутбуки, планшеты, серверы, системы хранения данных (СХД), а также иные средства обработки и хранения информации.

6) Программное обеспечение:

операционные системы, прикладные программы и приложения, исходные коды, системы управления базами данных (СУБД), диагностические программы, средства разработки и служебные утилиты.

Банк ведёт перечень программного обеспечения, разрешённого к использованию. Требования к ведению указанного перечня, а также требования, связанные с установкой и использованием программного обеспечения, регулируются Перечнем программного обеспечения, разрешённого к использованию (Приложение 9 к настоящей Политике).

7) Сервисы и системы информационного обмена:

– корпоративная электронная почта, организованная с использованием собственного почтового сервера Банка для всех работников Банка. Порядок использования корпоративной электронной почты, а также сети Интернет регулируется Правилами работы с сетью Интернет и корпоративной электронной почтой (Приложение 10 к настоящей Политике);

– система электронного документооборота (СЭД) Myanor.uz;

– корпоративный мессенджер Anor Chat, предназначенный для оперативного обмена сообщениями между работниками Банка;

– система IP-телефонии и Контакт-центр (Call-центр);

– система видеоконференцсвязи.

8) Системы физической безопасности:

– система контроля и управления доступом (СКУД), обеспечивающая контроль доступа работников Банка в защищаемые помещения Головного офиса и ИТ-офиса с использованием пластиковых идентификационных карт и биометрических данных (идентификация по лицу);

– система видеонаблюдения, обеспечивающая видеоконтроль и сбор видеоданных посредством видеокамер, установленных по периметру и внутри помещений Головного офиса, ИТ-офиса и в местах размещения банкоматов.

9) Сетевая инфраструктура Банка, включающая:

– серверы контроллеров домена для организации управляемой сети Банка (основной и резервный серверы, размещённые в основном центре обработки данных Банка);

– основные коммутаторы корпоративной сети, а также коммутаторы доступа локальных сетей Головного офиса, ИТ-офиса и офисов продаж;

– локальные вычислительные сети, организованные в Головном офисе, ИТ-офисе и офисах продаж;

– каналы связи корпоративной сети Банка (соединения между основным центром обработки данных, резервным центром обработки данных, ИТ-офисом и офисами продаж), а также внешние каналы связи для подключения корпоративной сети Банка к сети Интернет и Банковской телекоммуникационной сети (БТС) Центрального банка Республики Узбекистан;

– собственные волоконно-оптические линии связи («тёмное волокно») между основным центром обработки данных Банка (Головной офис) и резервным центром обработки данных, размещённым в дата-центре АТС-233 АК «Узбектелеком».

10) Информационные ресурсы:

– официальный веб-сайт Банка: **https://anorbank.uz/**, размещённый преимущественно в центре обработки данных Банка;

– веб-портал системы дистанционного банковского обслуживания (Интернет-банкинг BSS), размещённый в основном центре обработки данных Банка;

– файловое хранилище, организованное на сервере основного центра обработки данных Банка для структурных подразделений Банка;

– базы данных информационных систем, включая базу данных автоматизированной банковской системы (АБС) Банка, а также их электронные архивы.

11) Носители защищаемой информации.

12) Защищаемые помещения:

– служебные помещения Головного офиса Банка, в которых осуществляется обработка конфиденциальной информации;

– серверное помещение основного центра обработки данных Банка.

13) Средства обеспечения информационной безопасности:

межсетевые экраны, системы обнаружения и предотвращения вторжений (IDPS), средства организации VPN-соединений, средства антивирусной защиты и иные средства защиты информации.

14) Информационные системы Банка.

15) Нематериальные активы Банка.

4.2. В Банке функционируют следующие информационные системы:

1) Автоматизированная банковская система (АБС) - система осуществления банковских операций для клиентов Банка.

АБС включает следующий программно-аппаратный комплекс:

– серверы баз данных (два физических сервера баз данных, функционирующие в кластерном режиме в основном и резервном центрах обработки данных);

– серверы приложений для доступа работников Головного офиса Банка к АБС (пользователей АБС) через корпоративную сеть Банка, размещённые на виртуальных серверах основного центра обработки данных с резервированием в резервном центре обработки данных.

Пользователями АБС являются работники Банка.

2) Система дистанционного банковского обслуживания BSS (далее - система ДБО BSS) - система интернет-банкинга для предоставления цифровых банковских услуг юридическим лицам, а также система мобильного банкинга (мобильное приложение «Anor Business») для юридических лиц и мобильное приложение «Anorbank» для физических лиц.

Система ДБО BSS включает два виртуальных сервера баз данных и три виртуальных сервера приложений.

Пользователями системы ДБО BSS являются клиенты и работники Банка.

3) Система управления бизнес-процессами ELMA (далее - система ELMA), предназначенная для автоматизации процессов обслуживания клиентов Банка.

Система размещена на виртуальных серверах основного центра обработки данных с резервированием на отдельных физических серверах основного и резервного центров обработки данных.

Пользователями системы являются работники Банка.

4) Система Wings - система сбора и обработки информации о кредитоспособности клиентов Банка (кредитный рейтинг заёмщиков).

Система состоит из двух виртуальных серверов баз данных и двух виртуальных серверов приложений с резервированием в центре обработки данных.

Пользователями системы Wings являются работники Банка.

5) Система BillMaster - расчётная система, размещённая на виртуальных серверах основного центра обработки данных с резервированием на отдельных физических серверах основного и резервного центров обработки данных.

Пользователями системы BillMaster являются работники Банка.

6) Система взаиморасчётов BillMaster (далее - система BillMaster), состоящая преимущественно из виртуальных серверов центральной базы данных с резервированием на отдельных физических серверах основной и резервной баз данных.

Пользователями системы являются работники Банка.

7) AGC (предыдущая версия - ADPMS) - платформа, объединяющая все базы данных Банка в единую систему для удобного управления, администрирования и использования работниками Банка.

Пользователями системы являются работники Банка.

8) AnorHub - централизованная платформа управления доступом, предназначенная для организации авторизованного взаимодействия с информационными системами и информационными ресурсами Банка через единый центр доступа, а также обеспечивающая регистрацию (логирование) всех обращений.

Пользователями системы являются работники Банка.

9) Qlik Sense - платформа анализа и визуализации данных в режиме реального времени с использованием централизованного хранилища данных и специализированного языка запросов.

Пользователями системы являются работники Банка.

10) Confluence - система внутреннего использования, предназначенная для формирования единой базы знаний организации, включая ведение технической документации, проектной документации, матриц привилегий и алгоритмов использования информационных ресурсов Банка.

Пользователями системы являются работники Банка.

11) GitLab - система управления репозиториями исходного кода на базе Git, включающая встроенную Wiki, систему отслеживания ошибок, конвейер CI/CD и иные функции разработки программного обеспечения.

Пользователями системы являются работники Банка.

12) Jira - платформа для планирования, распределения, управления проектами и задачами ИТ-подразделений, обеспечивающая эффективное взаимодействие между командами.

Пользователями системы являются работники Банка.

13) Keycloak - программный продукт, обеспечивающий централизованное управление идентификацией пользователей и доступом к информационным системам.

14) MerchantCabinet - платформа для взаимодействия с партнёрами АО «ANOR BANK», предназначенная для мониторинга событий, анализа отчётности и формирования отчётов по расчётам с партнёрами.

15) ServiceDesk - платформа для организации процессов поддержки ИТ-услуг.

16) Verifix - система учёта присутствия работников в торговых подразделениях Банка.

17) WEBIM - платформа для консолидации обращений, поступающих через мобильное приложение, Instagram и Telegram-боты, в единую систему обработки запросов клиентов для обеспечения оперативного реагирования сотрудниками Контакт-центра в режиме 24/7.

18) Superset - платформа анализа и визуализации данных в режиме реального времени на основе централизованного хранилища данных и специализированного языка запросов.

Пользователями системы являются работники Банка.

19) IC - система бухгалтерского и налогового учёта, обеспечивающая сопровождение всей финансово-хозяйственной деятельности Банка.

4.3. Автоматизированная банковская система (АБС) Банка интегрирована со всеми внутренними информационными системами Банка, включая систему ДБО BSS, системы ELMA, Wings, BillMaster и иные информационные системы.

4.4. АБС Банка взаимодействует (осуществляет обмен данными) с внешними информационными системами, включая информационные системы Центрального банка Республики Узбекистан, процессинговые системы HUMO и UzCard, систему Кредитного бюро Ассоциации банков, а также информационные системы иных организаций.

4.5. Взаимодействие АБС с внешними информационными системами осуществляется через Банковскую телекоммуникационную сеть (БТС) Центрального банка Республики Узбекистан с использованием защищённых каналов связи IPSec VPN.

4.6. В соответствии с государственным стандартом ГС РУз 2814:2014 «Информационные технологии. Автоматизированные системы. Классификация по уровням защищённости от несанкционированного доступа к информации» автоматизированная банковская система (АБС) Банка относится к классу защищённости 3В.

4.7. Классификация информационных ресурсов Банка по уровням безопасности приведена в Реестре информационных ресурсов Банка, являющемся приложением к настоящей Политике (Приложение 11).

4.8. Базы данных информационных систем Банка, указанные в Таблице 1, содержат персональные данные работников и клиентов Банка.

В соответствии с Постановлением Кабинета Министров Республики Узбекистан от 5 октября 2022 года № 570 «Об утверждении отдельных

нормативно-правовых актов в сфере обработки персональных данных» для указанных баз данных установлены соответствующие уровни защиты.

Требования к защите персональных данных, обрабатываемых в информационных системах Банка, определены Положением о порядке обработки персональных данных работников АО «ANOR BANK», утверждённым протоколом Правления Банка № 7-1 от 16 мая 2023 года.

Таблица 1. Перечень баз данных Банка, предназначенных для обработки персональных данных, с установленным уровнем защиты

Наименование базы данных	**Вид персональных данных**	**Уровень защиты**
База данных АБС	Персональные данные клиентов Банка	2 уровень
База данных системы ДБО BSS	Персональные данные клиентов Банка	2 уровень
База данных системы Wings	Персональные данные клиентов Банка	2 уровень
База данных системы BillMaster	Персональные данные клиентов Банка	2 уровень
База данных системы Keycloak	Персональные данные клиентов Банка	2 уровень
База данных системы Oktell	Персональные данные клиентов Банка	2 уровень
База данных СКУД	Персональные данные работников Банка	1 уровень

4.9. Объекты защиты Банка создаются и функционируют с использованием аппаратно-программных и программных средств, перечень которых приведён в Приложении 18 к настоящей Политике.

5. МОДЕЛЬ РИСКОВ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Модель угроз информационной безопасности Банка определяется для каждого критически важного объекта защиты, указанного в разделе 4 настоящей Политики, и включает:

- описание объекта защиты;
- перечень и описание возможных угроз информационной безопасности объекта защиты;
- модель нарушителя информационной безопасности;
- возможные уязвимости;
- способы реализации угроз;
- последствия реализации угроз.

5.2. По характеру возникновения угрозы информационной безопасности Банка могут быть: естественными (объективными); искусственными (субъективными).

5.3. Источники угроз информационной безопасности могут быть: внутренними - когда источник угрозы находится внутри Банка; внешними - когда источник угрозы находится за пределами Банка.

5.4. Угрозы информационной безопасности могут быть: преднамеренными - реализуемыми умышленно для достижения определённой цели; случайными - возникающими вследствие ошибок оборудования, программного обеспечения или персонала.

5.5. Основная модель угроз информационной безопасности Банка приведена в Таблице 2.

5.6. В целях определения уровня информационной безопасности Банк осуществляет анализ и оценку рисков информационной безопасности. Риск информационной безопасности определяется вероятностью возникновения ущерба и потерь в случае реализации угроз информационной безопасности. Риски информационной безопасности возникают вследствие наличия реальной возможности воздействия угроз на объекты защиты.

Таблица 2. Основная модель угроз информационной безопасности Банка

Категория	**Код**	**Наименование угрозы**	**Вид, характер и источник угрозы***	**Объекты воздействия и последствия**
Физические угрозы	TP01	Пожар	A, D, E, F, B, C	Все объекты защиты. Отказ или утрата
	TP02	Затопление	A, D, E, F, B, C	
	TP03	Загрязнение, вредное излучение	A, D, E, F, B, C	
	TP04	Крупная авария	A, D, E, F, B, C	
	TP05	Взрыв, катастрофа	A, D, E, F, B, C	
	TP06	Пыль, коррозия, обледенение	A, D, E, F, B, C	
Природные угрозы	TN01	Климатические явления	A, E, C	Все объекты защиты. Отказ или утрата

Категория	Код	Наименование угрозы	Вид, характер и источник угрозы*	Объекты воздействия и последствия
	TN02	Сейсмические явления	A, E, C	
	TN03	Вулканические явления	A, E, C	
	TN04	Метеорологические явления	A, E, C	
	TN05	Наводнение	A, E, C	
	TN06	Пандемия / эпидемия	A, E, C	
Отказ инфраструктуры	TI01	Отказ систем обеспечения	A, D, F, C	Аппаратные и программные средства, рабочие станции и серверы, локальная сеть, корпоративная электронная почта, информационные системы и информационные ресурсы. Отказ, прекращение функционирования
	TI02	Отказ системы охлаждения или вентиляции	A, D, F, B, C	
	TI03	Нарушение электроснабжения	A, D, E, F, C	
	TI04	Отказ телекоммуникационной сети	A, D, E, F, C	
	TI05	Отказ телекоммуникационного оборудования	A, D, F, B	
	TI06	Электромагнитное излучение	A, D, E, F, C	

Категория	Код	Наименование угрозы	Вид, характер и источник угрозы*	Объекты воздействия и последствия
	TI07	Тепловое излучение	A, D, E, F, B, C	
	TI08	Электромагнитный импульс	A, D, E, F, C	
Технические сбои	TT01	Отказ устройства или системы	A, F, B	Аппаратные и программные средства, рабочие станции, серверы, локальная сеть, информационные системы и информационные ресурсы. Отказ, прекращение функционирования, потеря оборудования или данных
	TT02	Перегрузка информационной системы	A, D, F, B	
	TT03	Нарушение ремонтопригодности информационной системы	A, D, F, B	
Действия персонала	TH01	Терроризм, нападение, диверсия	D, F, B, C	Все объекты защиты. Отказ или утрата
	TH02	Социальная инженерия	D, F, B, C	Аппаратные и программные средства сетей и информационных систем. Нарушение конфиденциальности, целостности и доступности

Категория	Код	Наименование угрозы	Вид, характер и источник угрозы*	Объекты воздействия и последствия
	TH03	Перехват излучений оборудования	D, F, B, C	Информация. Нарушение конфиденциальности
	TH04	Удалённый мониторинг	D, F, B, C	
	TH05	Прослушивание	D, F, B, C	
	TH06	Хищение носителей информации или документов	D, F, B, C	Носители и хранилища информации, документы. Нарушение целостности и конфиденциальности
	TH07	Хищение оборудования	D, F, B, C	Оборудование. Утрата, нарушение деятельности
	TH08	Хищение цифрового идентификатора или учётных данных	D, F, B, C	Рабочие станции, серверы, сети и информационные системы. Несанкционированный доступ
	TH09	Получение данных с выброшенных либо повторно используемых носителей информации	D, F, B, C	Информация. Нарушение конфиденциальности
	TH10	Разглашение информации	A, D, F, B, C	Информация. Нарушение конфиденциальности

Категория	Код	Наименование угрозы	Вид, характер и источник угрозы*	Объекты воздействия и последствия
	TH11	Ввод данных из недоверенных источников	A, D, F, B, C	Информация. Нарушение достоверности
	TH12	Повреждение оборудования	D, F, B, C	Оборудование и данные. Нарушение функциональности, целостности, конфиденциальности и доступности
	TH13	Повреждение программного обеспечения	A, D, F, B, C	Программное обеспечение и данные. Нарушение функциональности, целостности, конфиденциальности и доступности
	TH14	Эксплуатация уязвимостей через веб-соединения (Drive-by Exploitation)	D, F, B, C	Информационные ресурсы и информационные системы. Несанкционированный доступ
	TH15	Атака повторного воспроизведения (Replay Attack), атака «человек посередине» (Man-in-the-Middle)	D, F, B, C	Данные. Несанкционированный доступ
	TH16	Несанкционированная обработка персональных данных	A, D, F, B, C	Персональные данные. Нарушение конфиденциальности
	TH17	Несанкционированный доступ к объектам	D, F, B, C	Все объекты защиты. Несанкционированный доступ

Категория	Код	Наименование угрозы	Вид, характер и источник угрозы*	Объекты воздействия и последствия
	TH18	Несанкционированное использование оборудования	D, F, B, C	Оборудование. Отказ, прекращение функционирования
	TH19	Неправильная эксплуатация оборудования	A, D, F, B, C	Оборудование. Отказ, прекращение функционирования
	TH20	Повреждение оборудования или носителей информации	A, D, F, B, C	Оборудование, носители информации. Отказ, прекращение функционирования
	TH21	Копирование нелицензионного программного обеспечения	D, F, B, C	Программное обеспечение. Нарушение функциональности и авторских прав
	TH22	Использование контрафактного или нелицензионного программного обеспечения	A, D, F, B, C	
	TH23	Повреждение данных	D, F, B, C	Данные. Нарушение целостности
	TH24	Незаконная обработка данных	D, F, B, C	Данные. Незаконное использование информации, нарушение авторских прав
	TH25	Передача или распространение вредоносного программного обеспечения	A, D, E, F, B, C	Рабочие станции, сеть, информационные системы и информационные ресурсы. Отказ, утрата, несанкционированный доступ

Категория	Код	Наименование угрозы	Вид, характер и источник угрозы*	Объекты воздействия и последствия
	TH26	Определение местоположения	D, F, B, C	Информация. Нарушение конфиденциальности
Нарушение сервисов или функций	TC01	Ошибки использования	A, F, B, C	Аппаратные и программные средства, сеть, информационные системы, информационные ресурсы и информация. Отказ, утрата, несанкционированный доступ
	TC02	Злоупотребление правами или разрешениями	A, D, F, B, C	
	TC03	Подделка прав или разрешений	D, F, B, C	
	TC04	Отказ от совершённых действий (Repudiation)	D, F, B, C	
Организационные угрозы	TO01	Недостаточность персонала	A, E, F, B	Аппаратные и программные средства, сеть, информационные системы, информационные ресурсы и информация. Нарушение деятельности
	TO02	Недостаточность ресурсов	A, E, F, B	
	TO03	Неплатёжеспособность поставщика услуг	A, E, F, C	

Категория	Код	Наименование угрозы	Вид, характер и источник угрозы*	Объекты воздействия и последствия
	TO04	Нарушение требований законодательства и нормативных документов	A, D, F, B, C	
Угрозы системам хранения данных и инфраструктуре	TD01	Несанкционированное использование	D, F, B, C	Системы хранения данных и инфраструктура хранения, данные в хранилищах, носители информации. Нарушение целостности, доступности и конфиденциальности информации
	TD02	Несанкционированный доступ	D, F, B, C	
	TD03	Юридическая ответственность за несоблюдение законодательства и нормативных требований	A, D, F, B, C	
	TD04	DoS- и DDoS-атаки на системы хранения данных	D, F, C	
	TD05	Повреждение, изменение или уничтожение данных	A, D, F, B, C	
	TD06	Утечка данных	D, F, B	
	TD07	Хищение либо случайная утрата носителя информации	A, D, F, B, C	

Категория	Код	Наименование угрозы	Вид, характер и источник угрозы*	Объекты воздействия и последствия
	TD08	Атака вредоносного программного обеспечения или внедрение вредоносного кода	D, F, B, C	
	TD09	Ненадлежащая обработка или утилизация после завершения использования	A, D, F, B	

*Примечание

Угрозы могут классифицироваться по следующим критериям:

- по источнику возникновения: B - внутренние; C - внешние;
- по причине возникновения: A - случайные; D - преднамеренные;
- по характеру возникновения: E - природные (объективные); F - субъективные.

5.7. В Банке идентификация рисков осуществляется посредством выявления, анализа и оценки рисков информационной безопасности в соответствии с требованиями национального стандарта O‘zMSt ISO/IEC 27005:2024 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по управлению рисками информационной безопасности».

5.8. Результаты идентификации рисков служат основой для определения соответствующих управленческих решений и приоритетных направлений управления информационной безопасностью, а также должны быть направлены на реализацию выбранных мер, методов и средств защиты от выявленных рисков информационной безопасности.

5.9. Идентификация рисков включает системный подход к оценке рисков (анализ рисков), а также сопоставление оценённых рисков с критериями принятия рисков для определения уровня их значимости.

Помимо идентификации рисков, процесс управления рисками должен включать: обработку рисков; принятие рисков; информирование и консультирование по вопросам рисков; мониторинг и анализ рисков.

5.10. Идентификация рисков информационной безопасности осуществляется Управлением информационной безопасности.

5.11. Методология оценки рисков информационной безопасности, а также порядок расчёта рисков информационной безопасности в отношении

основных объектов защиты Банка приведены в Приложении 17 к настоящей Политике.

5.12. Результаты оценки рисков информационной безопасности сопоставляются с критериями принятия рисков. Риски, значение которых превышает установленный критерий принятия риска, считаются неприемлемыми. Критерии принятия рисков информационной безопасности Банка приведены в Таблице 3.

Таблица 3. Критерии принятия рисков информационной безопасности Банка

Уровень риска	**Оценка риска**	**Количественное значение**	**Описание**
Низкий (зелёный)	Принимается без дополнительных мер	0–1	Риск может быть принят без выполнения дополнительных мероприятий
Средний (жёлтый)	Принимается при наличии средств контроля	1–2	Необходимо определить и реализовать мероприятия по управлению рисками в рамках процессов постоянного совершенствования в среднесрочной и долгосрочной перспективе
Высокий (красный)	Неприемлемый	Более 2	Необходимо принять меры по снижению риска в краткосрочной перспективе

5.13. Результаты оценки рисков информационной безопасности в отношении основных объектов защиты Банка после их сопоставления с критериями принятия рисков представляются в виде цветовой матрицы рисков и приведены в Таблице 4.

5.14. Риск информационной безопасности, имеющий значение «Высокий» (красный уровень), означает, что его величина превышает критерии принятия риска и требует принятия мер по снижению риска. Указанные меры могут быть направлены на: снижение вероятности возникновения угрозы либо её устранение; устранение либо снижение уровня соответствующей уязвимости.

5.15. После реализации мероприятий по обработке рисков выполняется повторная оценка рисков с учётом новых значений параметров угроз и уровня существующих уязвимостей. Полученное новое значение риска является остаточным риском информационной безопасности.

Мероприятия по снижению рисков информационной безопасности высокого уровня, а также значения остаточных рисков информационной безопасности после реализации соответствующих мер приведены в Таблице 5.

5.16. Для снижения рисков информационной безопасности высокого уровня также должны выбираться необходимые средства защиты информации, обладающие требуемыми характеристиками безопасности. Требования к средствам защиты информации, применяемым в Банке, приведены в Разделе 7 настоящей Политики.

Таблица 4. Результаты оценки рисков информационной безопасности в отношении объектов защиты Банка

№	Описание угрозы	Автоматизированная	Система дистанционно	Системы ELMA, CRM,	Системы BillMaster,	Системы Wings, Qlik	Системы Jira, ServiceDesk,	Системы Confluence и	Корпоративная электронная	Система IP-телефонии и	Сервер-контроллер	Файловый сервер	Официальный	Рабочие конечные	Система контроля и	Система видеонаблюд
TP01	Пожар	0,59	0,59	0,52	0,46	0,39	0,33	0,26	0,46	0,39	0,46	0,46	0,28	0,54	0,30	0,26
TP02	Затопление	0,47	0,47	0,42	0,37	0,32	0,26	0,21	0,37	0,32	0,37	0,37	0,23	0,44	0,26	0,23
TP03	Загрязнение, вредное	0,18	0,18	0.16	0,14	0,12	0,10	0,08	0,14	0,12	0,14	0,14	0,10	0,18	0,14	0,12
TP04	Крупная авария	0,66	0,66	0,58	0,51	0,44	0,36	0,29	0,51	0,44	0,51	0,51	0,33	0,59	0,48	0,41
TP05	Взрыв, катастрофа	0,23	0,23	0,21	0,18	0,15	0,13	0,10	0,18	0,15	0,18	0,18	0,11	0,23	0,24	0,21
TP06	Пыль, коррозия, обледенение	0,23	0.23	0,21	0,18	0,15	0,13	0,10	0,18	0,15	0,18	0,18	0,11	0,21	0,17	0,15
TN01	Климатические явления	0,90	0,90	0,80	0,70	0,60	0,50	0,40	0,70	0,60	0,70	0,70	0,48	0,96	0,35	0,30
TN02	Сейсмические явления	0,68	0,68	0,60	0,53	0,45	0,38	0,30	0,53	0,45	0,53	0.53	0,50	1,05	0,53	0,45
TN03	Вулканические явления	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0.00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
TN04	Метеорологические явления	0,48	0,48	0,43	0,37	0,32	0,27	0,21	0,37	0,32	0,37	0,37	0,32	0,64	0,28	0,24
TN05	Наводнение	0.84	0,84	0,75	0,65	0,56	0,47	0,37	0,65	0,56	0,65	0,65	0,37	0,80	0,65	0,56
TN06	Пандемия / эпидемия	0,54	0,54	0,48	0,42	0.36	0,30	0.24	0,42	0.36	0,42	0,42	0.40	0,84	0,42	0,36
TI01	Отказ систем обеспечения	1,26	1,26	1,12	0,98	0,84	0,70	0,56	0,98	0,72	1,12	1,12	0,64	1,32	1,12	0,96
TI02	Отказ системы охлаждения или	1,58	1,58	1,40	1,23	1,12	0,93	0,75	1,39	1,12	1,47	1,55	0,84	1,75	1,47	1,26
TIO3	Нарушение электроснабжения	1,80	1,80	1,60	1,40	1,28	1,07	0,85	1,59	1,36	1,59	1,68	0,91	1,88	1,47	1,26
TI04	Отказ телекоммуникационной	1,89	1,89	1,68	1,47	1,32	1,10	0,88	1,61	1,44	1,68	1,61	0,72	1,68	1,61	1,38

TI05	Отказ телекоммуникационного оборудования	1,62	1,68	1,49	1,31	1,16	0,97	0,77	1,40	1,20	1,49	1,49	0,88	1,80	1,45	1,24
TI06	Электромагнитное излучение	0,54	0,54	0,48	0,42	0,36	0,30	0,24	0,42	0,36	0,42	0,42	0,24	0,48	0,2	0,18
TI07	Тепловое излучение	0,72	0,72	0,64	0,56	0,48	0,40	0,32	0,56	0,48	0,56	0,56	0,32	0,48	0,5	0,48
TI08	Электромагнитный импульс	0,54	0,54	0,48	0,42	0,36	0,30	0,24	0,42	0,36	0,42	0,42	0,24	0,48	0,1	0,12
TT01	Отказ устройства или системы	3,40	3,35	2,98	2,61	1,81	1,84	1,47	2,58	2,22	1,96	2,53	1,42	1,90	1,9	1,80
TT02	Перегрузка информационной системы	1,35	1,35	1,20	1,05	0,90	0,75	0,60	1,05	0.90	1,05	1,05	0,72	1,38	0,84	0,72
TTO3	Нарушение ремонтопригодности	0,92	0,92	0.81	0,71	0,63	0,53	0,42	0,76	0,63	0,79	0,81	0,48	0,89	0,76	0,65
TH01	Терроризм, нападение,	0,37	0,38	0,34	0,30	0,26	0,22	0,18	0,35	0,27	0,33	0,31	0,21	0,38	0,2	0,25
TH02	Социальная инженерия	1,26	1,32	1,17	1,02	0,92	0,76	0.61	1,25	0,95	1,16	1,07	0,79	1,34	0.9	0,84
THO3	Перехват побочных электромагнитных излучений оборудования	0,81	0.81	0,72	0,63	0,54	0,45	0,36	0,63	0,54	0,63	0.63	0,36	0,72	0,63	0,54
TH04	Удалённый мониторинг	0,70	0,70	0,62	0,55	0,50	0,42	0,34	0,59	0,50	0,63	0,59	0,38	0,68	0,5	0,50
TH05	Прослушивание	0,86	0,86	0,77	0,67	0,65	0,54	0,43	0,76	0,65	0,84	0,76	0,53	1,08	0,7	0,65
TH06	Хищение носителей информации или документов	1,37	1,37	1,22	1,06	0,94	0,78	0,62	1,09	0,94	1,12	1,09	0,72	1,42	1,06	0,91
TH07	Хищение оборудования	0,83	0,83	0,74	0,64	0,58	0.48	0,38	0,67	0,58	0,70	0,67	0,46	0,84	0,6	0,58
TH08	Хищение цифрового идентификатора или учётных данных	1,27	1,27	1,13	0,99	0,87	0,73	0,58	1,02	0,87	1,05	1,02	0,69	1,21	1,02	0,87
TH09	Получение информации с выброшенных или повторно используемых носителей информации	1,44	1,44	1,28	1,12	1,02	0.85	0,68	1,19	1,02	1,26	1,19	0,84	1,44	1,12	0,96

THIO	Разглашение информации	2,15	2,09	2,07	1,31	1,17	0,98	0,78	1,37	1,17	1,42	1,37	0,81	1,35	1,3	1,17
TH11	Ввод данных из недоверенных источников	1,65	1,73	1,53	1,34	1,20	1,00	0,80	1,40	1,20	1,46	1,40	0,83	1,35	1,28	1,10
TH12	Повреждение оборудования	0,86	0,86	0,77	0,67	0,58	0,48	0,38	0,67	0,58	0,67	0,67	0,40	0,72	0,6	0,55
TH13	Повреждение программного обеспечения	1,14	1,16	1,04	0,91	0,79	0,66	0.53	0,91	0,78	0,91	0,93	0,59	1,01	0,76	0,65
TH14	Эксплуатация уязвимостей через веб-соединения (Drive-by Exploitation)	1,03	1,13	1,00	0,88	0,79	0.65	0,52	1,07	0,82	0,99	0,92	0,63	1,18	0,57	0.49
TH15	Атака повторного воспроизведения, атака «человек посередине»	1,08	1,14	1,01	0,89	0,80	0,67	0,53	1,12	0,80	0,98	0,93	0,67	1,04	0,79	0,68
TH16	Несанкционированная обработка персональных	1,64	1,67	1,48	1,30	1,11	0,93	0,74	1,30	1,13	1,32	1,30	0,86	1,53	1,22	1,05
TH 17	Несанкционированный доступ к объектам	0,48	0,48	0,43	0,37	0,32	0,27	0,21	0,37	0,32	0,37	0,37	0,27	0,64	0,37	0.32
TH18	Несанкционированное использование оборудования	0,82	0,82	0,73	0,64	0,55	0,46	0,37	0,64	0,55	0,64	0,64	0,41	0,75	0,64	0,55
TH19	Неправильная эксплуатация оборудования	1,08	1,08	0,96	0,84	0,72	0,60	0,48	0,84	0,72	0,84	0.84	0,48	0,72	0.84	0,72
TH20	Повреждение оборудования или носителей информации	0,99	0,99	0,88	0,77	0,72	0,60	0,48	0,77	0,66	0,77	0,84	0,60	1,20	0,63	0.54
TH21	Копирование нелицензионного программного обеспечения	1,50	1,50	1,33	1,16	1,00	0,83	0,67	1,16	1.00	1,16	1,16	0,74	1,42	1,04	0.89
TH22	Использование контрафактного или нелицензионного	0,96	0,96	0,85	0,75	0,68	0,57	0,45	0,79	0.68	0,84	0,79	0,51	0,88	0,70	0,60
TH23	Повреждение данных	1,13	1,13	1,00	0,88	0,75	0,63	0,50	0,88	0,75	0,88	0,88	0,54	1,32	0,8	0,75
TH24	Незаконная обработка данных	1,49	1,53	1,36	1,19	1,02	0,85	0,68	1,19	1,02	1,19	1,19	0,72	1,20	1,1	0,96

TH25	Передача или распространение вредоносного программного обеспечения	1,14	1,20	1,07	0,93	0,84	0,70	0,56	1,17	0,84	1,03	0,98	0.64	1,04	0,70	0,60
TH26	Определение местоположения	0,45	0,45	0,40	0,35	0,30	0,25	0.20	0,35	0,36	0,42	0,35	0,24	0.42	0,3	0,30
TC01	Ошибки использования	1,18	1,18	1,05	0,92	0,83	0,69	0,55	0,94	0,81	0,96	0,96	0,60	1,11	0,7	0,68
TC02	Злоупотребление правами или разрешениями	1,49	1,49	1,32	1,16	0,99	0,83	0.66	1,16	0.99	1,16	1,16	0,66	1,08	1,16	0.99
TC03	Подделка прав или	1,20	1,20	1,07	0,93	0,84	0,70	0,56	0,98	0,84	1,03	0,98	0,67	1,04	0,9	0,84
TC04	Отказ от совершённых	1,41	1,41	1,26	1,10	0,94	0,79	0,63	1,10	0,94	1,10	1,10	0,63	1,11	1,5	1,32
TO01	Недостаточность персонала	1,26	1,26	1,12	0,98	0,84	0,70	0,56	0,98	0,84	0,98	0,98	0,56	0,84	0,9	0,84
TO02	Недостаточность ресурсов	1,44	1,44	1,28	1,12	1,08	0,90	0,72	1,40	1,20	1,40	1,40	0,64	1,44	1,4	1,20
TO03	Неплатёжеспособность поставщика услуг	1,26	1,26	1,12	0.98	0,84	0,70	0.56	0,98	0,72	1,12	1,12	0.64	1,32	1,12	0,96
TO04	Нарушение требований законодательства и нормативных правовых актов	1,54	1,54	1,37	1,20	1,08	0,94	0,75	1,32	1,08	1,38	1,26	0,79	1,44	1,26	1,08
TD01	Несанкционированное использование	1,23	1,25	1,11	0,97	0,83	0,70	0,56	0,97	0,85	0,99	0,97	0,64	1,15	0,92	0,79
TD02	Несанкционированный доступ	0,48	0,48	0,43	0,37	0,32	0,27	0,21	0,37	0,32	0,37	0,37	0,27	0,64	0,3	0,32
TD03	Юридическая ответственность за несоблюдение требований законодательства и нормативных документов	1,54	1,54	1,37	1,20	1,08	0,94	0,75	1,32	1,08	1,38	1,26	0,79	1,44	1,26	1,08
TD04	DoS- и DDoS-атаки на системы хранения данных	1,89	1,89	1,68	1,47	1,26	1,05	0,84	1,47	1,26	1,47	1,47	0,84	1,26	1,26	1,08
TD05	Повреждение, изменение и уничтожение данных	1,40	1,40	1,25	1,09	0,96	0.80	0,64	1,12	0,96	1,15	1,12	0,75	1,37	1,09	0.94
TD06	Утечка данных	2,09	2,09	1,50	1,31	1,17	0,98	0,78	1,37	1,17	1,42	1,37	0,81	1,35	1,3	1,17

TD07	Хищение или случайная утрата носителей информации либо средств хранения данных	0,79	0,79	0,70	0,62	0,58	0,48	0,38	0.62	0,53	0,62	0,67	0,48	0,96	0,50	0,43
TD08	Атака вредоносного программного обеспечения или внедрение вредоносного	1,14	1,20	1,07	0,93	0,84	0,70	0,56	1,17	0,84	1,03	0,98	0,64	1,08	0,70	0,60
TD09	Ненадлежащая обработка или утилизация после завершения использования	2,13	2,13	2,04	1,84	1,22	1,02	0,82	1,43	1,22	1,51	1,43	1,01	1,73	1,34	1,15

Таблица 5. Мероприятия по снижению рисков информационной безопасности, а также остаточный риск информационной безопасности после реализации мероприятий

Наименование угрозы	**Оценка риска**	**Объекты защиты**	**Планируемые мероприятия**	**Остаточный риск**
Отказ устройства или системы	3,40	Автоматизированная банковская система (АБС)	1. Контроль и учёт изменений конфигурации, настроек и программного обеспечения.2. Регламентация и выполнение процедур проверки программного обеспечения перед вводом в эксплуатацию, проведение тестирования (тестовой эксплуатации) до внедрения программного обеспечения.	1,5
	3,35	Система дистанционного банковского обслуживания BSS (ДБО BSS)		1,44
	2,98	Системы ELMA, CRM, AGC (ADPMS) и Anorhub (MerchantCabinet)		1,35

Наименование угрозы	Оценка риска	Объекты защиты	Планируемые мероприятия	Остаточный риск
	2,61	Системы BillMaster, EDMS MyAnor, Superset и 1С	3. Определение и внедрение порядка внесения изменений в программное обеспечение.4. Учёт средств установки программного обеспечения.5. Учёт обновлений программного обеспечения и внесённых изменений.6. Наличие планов восстановления после чрезвычайных ситуаций и проведение соответствующего обучения.7. Выполнение плановых работ по техническому обслуживанию.	1,2
	2,58	Корпоративная электронная почта		1,18
	2,22	Система IP-телефонии и Контакт-центр (Call-центр)		0,95
	2,53	Файловый сервер		1,13
Разглашение информации	2,15	Автоматизированная банковская система (АБС)	1. Документирование обязанностей пользователей и администраторов.2. Проведение обучения пользователей по вопросам ответственности.3. Усиление ответственности за нарушения, разработка и применение мер воздействия к нарушителям.4. Установка DLP-агентов на рабочие станции всех сотрудников.	1,7
	2,09	Система дистанционного банковского обслуживания BSS (ДБО BSS)		1,56

Наименование угрозы	Оценка риска	Объекты защиты	Планируемые мероприятия	Остаточный риск
	2,07	Системы ELMA, CRM, AGC (ADPMS) и Anorhub (MerchantCabinet)		1,02
Утечка данных	2,09	Автоматизированная банковская система (АБС)	1. Установка DLP-агентов на рабочие станции всех сотрудников.2. Регламентация порядка предоставления и управления доступом привилегированных пользователей к хранилищам данных.3. Классификация информационных ресурсов в зависимости от уровня защищённости информации.4. Учёт носителей защищаемой информации.	0,98
	2,09	Система дистанционного банковского обслуживания BSS (ДБО BSS)		0,98
Ненадлежащая обработка или утилизация после завершения использования	2,13	Автоматизированная банковская система (АБС)	1. Регламентация и соблюдение порядка списания, уничтожения и утилизации оборудования и носителей информации.2. Назначение ответственных лиц.3. Применение эффективных методов очистки и уничтожения остаточной информации на носителях информации.4. Обеспечение надлежащего хранения носителей информации, подлежащих дальнейшей обработке.5. Контроль соблюдения процедур утилизации.	1,25

Наименование угрозы	Оценка риска	Объекты защиты	Планируемые мероприятия	Остаточный риск
	2,13	Системы интернет-банкинга и мобильного банкинга		1,25
	2,04	BPM-, CRM-системы, шина данных Karaf и Artemis		0,98

6. МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Модель нарушителя информационной безопасности формируется в целях систематизации сведений о возможностях и типах субъектов, целях осуществления несанкционированного воздействия, а также для разработки адекватных и достаточных методов противодействия таким воздействиям.

При разработке модели нарушителя должны учитываться:

- категории нарушителей;
- особенности оценки уровня опасности и значимости нарушителей, а также анализ их технических возможностей;
- ограничительные и противодействующие меры.

6.2. В отношении объектов защиты Банка нарушителями могут являться как сотрудники Банка, имеющие непосредственный (физический и/или логический) доступ к объектам защиты, так и сотрудники, не имеющие такого доступа. Кроме того, нарушителями могут выступать лица, не являющиеся сотрудниками Банка.

6.3. В Банке разрабатывается модель нарушителя информационной безопасности в целях идентификации потенциальных нарушителей и оценки их практических и теоретических возможностей по реализации угроз информационной безопасности в отношении защищаемых объектов Банка.

6.4. Внутренними нарушителями информационной безопасности Банка могут являться:

1) сотрудники Банка, являющиеся зарегистрированными (авторизованными) пользователями информационных систем и сетей (непосредственные пользователи);
2) сотрудники Банка, не являющиеся пользователями информационных систем и сетей (технический персонал по обслуживанию помещений и зданий и др.);
3) сотрудники, обслуживающие технические средства Банка и имеющие возможность физического доступа к ним;
4) администраторы, обслуживающие информационные системы, сети и средства защиты информации, обладающие привилегированным физическим и логическим доступом к объектам защиты;
5) сотрудники Банка, являющиеся разработчиками информационных систем (проектировщики, разработчики программного обеспечения);
6) сотрудники службы безопасности (охраны), имеющие физический доступ в помещения и к иным объектам защиты, и другие лица.

6.5. Внешними нарушителями информационной безопасности Банка могут являться:

1) уволенные сотрудники Банка;
2) посетители, являющиеся клиентами либо представителями сторонних организаций (партнёров, контролирующих органов и др.);
3) представители сторонних организаций, выполняющие работы на договорной основе (подрядчики, поставщики, разработчики и др.), а также организации, оказывающие услуги аутсорсинга;

4) внешние пользователи, имеющие возможность доступа к информационным системам Банка через внешние сети или каналы связи (клиенты, партнёры, учредители и др.);

5) нарушители, осуществляющие действия извне через внешние сети, а также иные лица.

6.6. Потенциальные нарушители могут классифицироваться по следующим критериям:

1) опыт - уровень квалификации в области информационных технологий;

2) наличие возможностей - уровень функциональных возможностей, прав и полномочий в отношении объекта защиты.

6.7. По уровню опыта в области информационных технологий потенциальные нарушители подразделяются на следующие категории:

1) неопытный пользователь (категория А) - не обладает знаниями по использованию стандартных средств организации и представляет угрозу главным образом как источник ошибок, неосторожных или неправильных действий. Такие действия могут привести к нарушениям функционирования или даже отказу системы, а также к нанесению ущерба организации;

2) осведомлённый пользователь (категория В) - владеет навыками использования стандартных средств и может стать источником нарушений функционирования объекта защиты. При этом попытки установки собственного программного обеспечения либо использования внешних ресурсов, включая сеть Интернет, должны пресекаться средствами управления доступом и средствами защиты информации;

3) квалифицированный пользователь (категория С) - обладает высоким уровнем знаний и практического опыта эксплуатации технических средств, навыками программирования, проектирования и эксплуатации информационных систем, а также знаниями структуры, функций и механизмов работы средств защиты информации, включая их сильные и слабые стороны.

6.8. Исходя из потенциальных возможностей действий, нарушитель может быть отнесён к одному из четырёх уровней:

1) первый (низкий) уровень возможностей нарушителя характеризуется возможностью запуска задач из заранее предусмотренного набора функций обработки информации;

2) второй (средний) уровень включает возможности первого уровня, а также способность самостоятельно разрабатывать и запускать собственные программы с дополнительными функциями обработки информации;

3) третий (высокий) уровень предполагает возможность управления функционированием объекта защиты, включая воздействие на базовое программное обеспечение, его состав, конфигурацию и функционирование;

4) четвёртый (очень высокий) уровень характеризуется всеми возможностями лиц, осуществляющих проектирование, внедрение и обслуживание технических средств объектов защиты, вплоть до внедрения в

аппаратно-программную среду и систему защиты программных и технических средств с новыми функциями обработки информации.

6.9. Для каждого потенциального нарушителя модель нарушителя информационной безопасности Банка должна включать:

1) категорию опыта;

2) уровень возможностей по осуществлению действий;

3) характеристики нарушителя - его возможности и предполагаемые действия;

4) методы, способы и средства воздействия, которые могут быть использованы для нарушения информационной безопасности;

5) мотивы действий нарушителя (ошибка, безответственность, самоутверждение либо корыстная заинтересованность);

6) объекты защиты, на которые может быть направлено воздействие;

7) основные ограничительные меры (контрмеры), применяемые в отношении нарушителя.

6.10. Нарушитель может использовать следующие методы и средства:

1) сбор сведений и данных;

2) средства пассивного перехвата информации;

3) использование штатных средств информационной системы или системы защиты информации, а также эксплуатацию их недостатков;

4) применение средств активного воздействия (модификация и подключение дополнительных средств, подключение к каналам передачи данных, внедрение программных закладок, использование специализированных инструментальных, технологических и сервисных программных средств).

Модель потенциальных нарушителей Банка приведена в Таблице 6.

Таблица 6. Модель потенциальных нарушителей информационной безопасности Банка

Показатель модели	**Описание**
1. Сотрудники, являющиеся зарегистрированными (авторизованными) пользователями информационных систем и сетей (непосредственные пользователи)	
Категория опыта	**Категория В (осведомлённый пользователь)**
Уровень возможностей	**Первый (низкий) уровень**
Характеристика	Имеют возможность реализации угроз, связанных преимущественно с попытками расширения собственных полномочий и обхода мер информационной безопасности. Могут являться источником неосторожных либо ошибочных действий в отношении объектов защиты. Также характеризуются возможностью утечки информации и раскрытия защищаемых сведений.
Методы, возможности и средства воздействия	Использование штатных программных и технических средств объекта защиты, средств взаимодействия с ними, а также эксплуатация их недостатков или недостатков системы защиты
Мотивы	Ошибка, халатность либо корыстная заинтересованность
Объекты воздействия	Информационные системы, сети, рабочие станции, программное обеспечение и информация (данные) в электронном виде
Ограничительные и противодействующие меры	Разграничение прав доступа и контроль доступа к объектам защиты; регистрация действий сотрудников в информационных системах; сокращение и контроль каналов утечки информации; соблюдение сотрудниками требований о неразглашении конфиденциальной информации

Показатель модели	Описание
2. Сотрудники, не являющиеся пользователями информационных систем и сетей (технический персонал по обслуживанию зданий и помещений и др.)	
Категория опыта	**Категория А (неопытный пользователь)**
Уровень возможностей	**Первый (низкий) уровень**
Характеристика	Возможности реализации угроз ограничиваются получением несанкционированного физического доступа к объектам защиты либо совершением неосторожных и ошибочных действий, которые могут привести к нарушениям функционирования или отказу системы.
Методы, возможности и средства воздействия	Сбор информации либо использование средств пассивного перехвата
Мотивы	Ошибка или халатность
Объекты воздействия	Любые материальные активы организации, а также информация в материальной или нематериальной форме (знания)
Ограничительные и противодействующие меры	Соблюдение требований по размещению объектов защиты; применение режимных, организационных и технических мер по предотвращению несанкционированного доступа; подбор и расстановка кадров; организация контроля и управления доступом в помещения, где размещены объекты защиты

Показатель модели	Описание
3. Сотрудники, обслуживающие технические средства организации	
Категория опыта	**Категория С (квалифицированный пользователь)**
Уровень возможностей	**Второй (средний) или третий (высокий) уровень**
Характеристика	Имеют возможность физического доступа к техническим и программным средствам объекта защиты, но не являются его зарегистрированными пользователями.

Показатель модели	Описание
3. Сотрудники, обслуживающие технические средства организации	
Методы, возможности и средства воздействия	Сбор информации, средства пассивного перехвата, использование штатных средств либо средств активного воздействия
Мотивы	Ошибка либо самоутверждение
Объекты воздействия	Обслуживаемые технические средства (средства обработки и хранения информации, сетевое оборудование, средства защиты информации), установленное на них программное обеспечение и хранящиеся данные
Ограничительные и противодействующие меры	Ограничение физического доступа в помещения размещения объектов защиты; контроль порядка выполнения работ; предоставление доступа исключительно к обслуживаемому оборудованию; проверка целостности конфигурации оборудования и данных после завершения работ

Показатель модели	Описание
4. Администраторы, обслуживающие сети, информационные системы и средства информационной безопасности	
Категория опыта	**Категория С (квалифицированный пользователь)**
Уровень возможностей	**Третий (высокий) или четвёртый (очень высокий) уровень**
Характеристика	Обладают санкционированным физическим и логическим доступом к объектам защиты, входят в группу привилегированных пользователей и относятся к числу доверенных сотрудников, имеющих широкие возможности воздействия на внутреннее состояние объектов защиты.
Методы, возможности и средства воздействия	Использование штатных средств, эксплуатация их недостатков либо применение средств активного воздействия

Показатель модели	Описание
4. Администраторы, обслуживающие сети, информационные системы и средства информационной безопасности	
Мотивы	Ошибка, самоутверждение либо корыстная заинтересованность
Объекты воздействия	Информационные системы организации, технические средства, программное обеспечение, обрабатываемая и хранимая в системах информация
Ограничительные и противодействующие меры	Учёт и контроль действий администраторов; использование системы управления привилегированным доступом (PAM); регистрация и блокирование попыток обхода правил безопасности; усиление мер ответственности для данной категории сотрудников

Показатель модели	Описание
5. Сотрудники-разработчики информационных систем (проектировщики, разработчики программного обеспечения)	
Категория опыта	**Категория С (квалифицированный пользователь)**
Уровень возможностей	**Третий (высокий) или четвёртый (очень высокий) уровень**
Характеристика	Имеют возможность реализации угроз, связанных с ошибками при разработке прикладного программного обеспечения либо внедрением недекларированных возможностей («закладок»), способных нарушить штатное функционирование системы, обеспечить несанкционированный доступ или утечку информации.
Методы, возможности и средства воздействия	Использование штатных либо активных средств воздействия
Мотивы	Ошибка либо самоутверждение
Объекты воздействия	Программное обеспечение информационных систем и сами информационные системы организации

Показатель модели	Описание
5. Сотрудники-разработчики информационных систем (проектировщики, разработчики программного обеспечения)	
Ограничительные и противодействующие меры	Учёт и контроль действий разработчиков; анализ программного кода средствами статического анализа; тестирование функциональности, входных и выходных данных программ; сертификация программных продуктов на соответствие требованиям информационной безопасности

Показатель модели	Описание
6. Сотрудники службы безопасности (охраны)	
Категория опыта	**Категория А (неопытный пользователь)**
Уровень возможностей	**Четвёртый (очень высокий) уровень**
Характеристика	Имеют санкционированный физический доступ к помещениям и иным объектам защиты.
Методы, возможности и средства воздействия	Использование средств пассивного перехвата либо штатных средств
Мотивы	Халатность либо корыстная заинтересованность
Объекты воздействия	Помещения и материальные ценности организации, находящиеся под физической защитой
Ограничительные и противодействующие меры	Учёт посещений помещений (видеонаблюдение, журналы входа и выхода); усиление мер ответственности; проведение надлежащего отбора персонала

Внешние нарушители

Показатель модели	Описание
1. Бывшие сотрудники организации	
Категория опыта	В зависимости от ранее занимаемой должности
Уровень возможностей	В зависимости от ранее занимаемой должности
Характеристика	Могут использовать полученные в период работы знания о защищаемой информации, технологиях и технических средствах для получения выгоды, нанесения ущерба организации либо совершения иных противоправных действий.
Методы, возможности и средства воздействия	Сбор информации и данных, применение средств активного воздействия
Мотивы	Корыстная заинтересованность
Объекты воздействия	Знания и конфиденциальная информация, полученные в период работы в организации
Ограничительные и противодействующие меры	Соблюдение обязательств о неразглашении конфиденциальной информации после увольнения; блокирование возможности использования прежних учётных данных; обязательная сдача носителей информации, реквизитов доступа и иных сведений при увольнении

Показатель модели	Описание
2. Посетители, являющиеся клиентами или представителями сторонних организаций	
Категория опыта	**Категория А (неопытный пользователь) либо категория В (осведомлённый пользователь)**
Уровень возможностей	**Первый (низкий) уровень**

Показатель модели	Описание
2. Посетители, являющиеся клиентами или представителями сторонних организаций	
Характеристика	Возможности реализации угроз связаны преимущественно с получением несанкционированного физического доступа к объектам защиты.
Методы, возможности и средства воздействия	Средства пассивного перехвата либо штатные средства
Мотивы	Корыстная заинтересованность
Объекты воздействия	Материальные ценности и средства обработки информации, не находящиеся под достаточной физической защитой
Ограничительные и противодействующие меры	Соблюдение требований по размещению объектов защиты; разделение помещений на зоны безопасности; ограничение доступа посетителей в помещения и зоны ограниченного доступа; регистрация и контроль посетителей; сопровождение посетителей; приём посетителей в зонах с низким уровнем безопасности

Показатель модели	Описание
3. Представители сторонних организаций, выполняющие работы по договору (подрядчики, поставщики, разработчики и др.), а также организации-аутсорсеры	
Категория опыта	**Категория B (осведомлённый пользователь) либо категория C (квалифицированный пользователь)**
Уровень возможностей	**Второй (средний) либо третий (высокий) уровень**
Характеристика	Имеют логический и физический доступ к объектам защиты при выполнении работ по внедрению, настройке, сопровождению и обслуживанию оборудования и программного обеспечения. Потенциально способны реализовывать различные сценарии воздействия посредством специальных средств.
Методы, возможности и средства воздействия	Использование средств активного воздействия

Показатель модели	Описание
3. Представители сторонних организаций, выполняющие работы по договору (подрядчики, поставщики, разработчики и др.), а также организации-аутсорсеры	
Мотивы	Корыстная заинтересованность
Объекты воздействия	Аппаратные и программные средства, используемые и обслуживаемые данной категорией лиц
Ограничительные и противодействующие меры	Контроль порядка выполнения работ; присутствие представителя организации при проведении работ; предоставление доступа только к необходимым объектам; соблюдение технических требований при разработке продуктов; проведение тестирования на уязвимости по принципу «белого хакера»; проверка целостности конфигурации и данных после завершения работ

Показатель модели	Описание
4. Внешние пользователи, имеющие доступ к информационным системам организации через внешние сети	
Категория опыта	**Категория B (осведомлённый пользователь)**
Уровень возможностей	**Первый (низкий) уровень**
Характеристика	Являются зарегистрированными пользователями информационных систем организации. Потенциальные угрозы связаны преимущественно с попытками расширения собственных полномочий и обхода мер информационной безопасности с использованием штатных программных и технических средств.
Методы, возможности и средства воздействия	Использование штатных программных и технических средств объекта защиты и средств взаимодействия с ним
Мотивы	Корыстная заинтересованность
Объекты воздействия	Информационные системы, к которым предоставлен доступ

Показатель модели	Описание
4. Внешние пользователи, имеющие доступ к информационным системам организации через внешние сети	
Ограничительные и противодействующие меры	Разграничение прав доступа; контроль доступа к объектам защиты; регистрация действий пользователей в информационных системах

Показатель модели	Описание
5. Нарушители, получившие несанкционированный логический доступ к объектам защиты через внешние сети с обходом системы защиты	
Категория опыта	**Категория С (квалифицированный пользователь)**
Уровень возможностей	**Второй (средний), третий (высокий) либо четвёртый (очень высокий) уровень**
Характеристика	Осуществляют целенаправленные действия с использованием специализированных программно-технических средств либо посредством эксплуатации уязвимостей системы.
Методы, возможности и средства воздействия	Использование средств активного воздействия
Мотивы	Корыстная заинтересованность либо самоутверждение
Объекты воздействия	Локальные и корпоративные сети организации, подключённые информационные ресурсы и информационные системы, а также средства обработки, хранения и передачи информации
Ограничительные и противодействующие меры	Использование комплекса программно-аппаратных средств защиты информации, направленных на предотвращение и пресечение несанкционированных действий; выявление и устранение уязвимостей в сетевой инфраструктуре и программном обеспечении

7. МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1.Для построения СУИБ Банка реализуется комплекс мер по обеспечению информационной безопасности, включающий:

- правовые меры;
- поведенческие и этические (психологические) меры;
- организационные меры;
- технологические меры;
- инженерно-технические меры;
- программно-технические меры;
- меры безопасности при взаимодействии с внешними пользователями.

7.2. Правовые меры (меры по нормативно-документальному обеспечению)

Меры нормативно-правового обеспечения в Банке направлены на формирование базы нормативных документов, которыми Банк руководствуется при управлении информационной безопасностью.

Нормативно-правовая база Банка в области информационной безопасности включает государственные стандарты Республики Узбекистан, указанные в разделе 1.2 настоящей Политики, а также нормативно-правовые и внутренние нормативные документы Банка, регулирующие вопросы обеспечения информационной безопасности.

Нормативно-правовая база Банка в области информационной безопасности формируется и поддерживается Управлением информационной безопасности.

Ведомственные нормативные документы Банка в области информационной безопасности разрабатываются (актуализируются) Управлением информационной безопасности совместно с другими заинтересованными подразделениями Банка (Управлением общей безопасности, Департаментом информационных технологий и др.).

Нормативные документы согласовываются и утверждаются в соответствии с правилами, установленными внутренними нормативными документами Банка.

Документация Банка в области информационной безопасности включает следующие уровни документов:

a) основной документ - Политика информационной безопасности Банка;

b) документы, определяющие и классифицирующие объекты защиты (реестры, перечни, классификаторы);

c) документы, распределяющие функции и ответственность (положения о структурных подразделениях, должностные инструкции);

d) документы, регламентирующие процессы и процедуры управления информационной безопасностью (положения, порядки, правила, регламенты, инструкции, методики);

e) организационно-распорядительные документы, направленные на реализацию мероприятий по обеспечению информационной безопасности (приказы, распоряжения, планы);

f) документы, устанавливающие требования к объектам защиты и средствам защиты (требования, технические задания, проекты);

g) эксплуатационная документация (руководства, инструкции по эксплуатации);

h) документы, используемые для регистрации и подтверждения выполнения процедур и работ по обеспечению информационной безопасности (формы, журналы, отчёты, заявки, протоколы, акты).

Ведомственные документы по информационной безопасности и содержащиеся в них требования доводятся Управлением информационной безопасности до сведения соответствующих работников Банка и являются обязательными для исполнения.

Отдельные виды ведомственных нормативных документов по информационной безопасности приведены в приложениях к настоящей Политике.

7.3. Поведенческие и этические (психологические) меры защиты информации

7.3.1. Поведенческие и этические (психологические) меры защиты информации должны быть направлены на:

- создание здорового морально-психологического климата в коллективе;
- снижение вероятности негативного поведения и нарушений информационной безопасности, связанных с человеческим фактором;
- исключение влияния личностно-психологических факторов при нарушении режима защиты информации;
- соблюдение работниками Банка норм этического поведения.

Поведенческие и этические меры защиты носят профилактический характер и включают:

- проведение разъяснительной работы среди работников Банка;
- применение мер дисциплинарного воздействия к нарушителям;
- поощрение и стимулирование работников.

7.3.2. Разъяснительная работа проводится Управлением информационной безопасности в форме специальных занятий либо индивидуальных бесед.

Для проведения такой работы могут привлекаться сотрудники Управления общей безопасности и Департамента управления персоналом Банка.

Разъяснительная работа проводится в целях:

– информирования работников о существующих угрозах деятельности Банка, возможных последствиях их реализации, а также мерах ответственности, применяемых к нарушителям;

– повышения осведомлённости работников о необходимости соблюдения требований и положений Политики информационной безопасности;

– повышения уровня знаний работников и чувства ответственности в вопросах обеспечения информационной безопасности;

– формирования у работников требуемых норм поведения и этики, способствующих соблюдению правил и требований по обеспечению информационной безопасности;

– укрепления взаимодействия работников при решении задач обеспечения информационной безопасности.

Разъяснительная работа проводится как при приёме работников на работу, так и в процессе их трудовой деятельности.

Разъяснительная работа осуществляется отдельно для следующих категорий работников Банка:

– работников, являющихся пользователями информационных систем;

– работников, обслуживающих клиентов Банка;

– работников, обеспечивающих сопровождение информационных систем и ресурсов, а также технических и технологических средств информационной инфраструктуры Банка;

– технического персонала.

7.3.3. В отношении вновь принимаемых работников Банка проводится инструктаж по вопросам обеспечения информационной безопасности.

Комплекс реализуемых мероприятий направлен на создание условий, при которых работники Банка обязаны соблюдать правила и требования по обеспечению информационной безопасности, включая меры ответственности за их нарушение.

К нарушителям по решению руководства Банка и уполномоченных комитетов в рамках трудовых отношений могут применяться меры дисциплинарного взыскания в соответствии с трудовым законодательством в виде замечания, выговора или штрафных санкций, предусмотренных трудовым договором.

7.3.4. Меры стимулирования должны быть направлены на создание условий, побуждающих работников Банка к надлежащему и ответственному поведению в вопросах обеспечения информационной безопасности.

7.3.5. В целях предупреждения правонарушений, устранения причин и условий, способствующих их совершению, работники Банка обязаны соблюдать: Типовые правила служебной этики государственных служащих, утверждённые постановлением Кабинета Министров Республики Узбекистан от 14 октября 2022 года № 595 «О дополнительных мерах по обеспечению соблюдения государственными служащими правил служебной этики»;

Корпоративный кодекс этики Банка, утверждённый протоколом № 7 Наблюдательного совета Банка от 25 февраля 2021 года.

7.4. Организационные меры

7.4.1. Организационные мероприятия направлены на:

- управление информационными активами;
- обеспечение безопасности персонала, повышение осведомлённости и обучение сотрудников;
- ограничение физического доступа к защищаемым объектам (физическая безопасность);
- защиту конфиденциальной информации;
- создание, функционирование и развитие системы и средств защиты информации;
- реагирование на инциденты информационной безопасности;
- контроль и оценку состояния безопасности.

В целях идентификации информационных активов и определения соответствующей ответственности за их защиту реализуются организационные мероприятия по управлению информационными активами.

7.4.2. Организационные мероприятия по управлению информационными активами включают:

а) регулярную инвентаризацию информационных активов для идентификации информационных ресурсов и связанных с ними средств обработки информации;

б) учёт информационных активов - формирование и актуализацию инвентарного перечня указанных активов;

в) определение владельцев информационных активов - назначение владельцев информационных активов, а также установление их обязанностей и ответственности в отношении соответствующих информационных активов;

г) классификацию информационных активов - классификацию информационных активов в соответствии с требованиями законодательства по степени их значимости, важности и чувствительности для Банка, а также обеспечение соответствующего уровня их защиты;

д) маркировку информационных активов - разработку и внедрение комплекса процедур по маркировке информационных активов в соответствии с принятой в Банке системой классификации;

е) допустимое использование и управление информационными активами - документирование и внедрение правил допустимого использования и управления информационными активами и соответствующими средствами обработки информации.

7.4.3. В Банке инвентаризация, учёт, определение владельцев, классификация, маркировка информационных активов, формирование реестра информационных активов, а также иные процедуры управления ими осуществляются в соответствии с Порядком управления информационными активами, приведённым в Приложении 11 к настоящей Политике.

Инвентаризация в целях идентификации объектов защиты и информационных активов организуется и проводится Управлением

информационной безопасности совместно с Управлением общей безопасности и Департаментом информационных технологий. По результатам инвентаризации при необходимости вносятся изменения и дополнения в перечень объектов защиты, реестр информационных активов (информационных ресурсов) и перечень конфиденциальной информации Банка. Кроме того, по итогам инвентаризации определяется перечень помещений, а также состав размещённых в них технических и программных средств.

Категорирование и классификация защищаемых объектов осуществляются в соответствии с требованиями ГС РУз 2814:2014 «Информационные технологии. Автоматизированные системы. Классификация по уровню защищённости от несанкционированного доступа к информации» и иных нормативных документов. Классификация защищаемых объектов осуществляется Управлением информационной безопасности.

7.4.4. Организационные мероприятия по обеспечению безопасности персонала, повышению его осведомлённости и обучению в Банке включают:

а) при приёме на работу:

- установление квалификационных требований к специалистам, ответственным за обеспечение информационной безопасности, а также к уровню квалификации работников, деятельность которых связана с процессами обработки информации и обеспечения информационной безопасности;
- проверку соответствия уровня знаний и компетенций кандидатов квалификационным требованиям и требованиям к профессиональным навыкам, установленным Банком при приёме на работу;

б) при трудоустройстве:

- определение ответственности в области информационной безопасности в трудовых договорах;
- ознакомление с настоящей Политикой;
- информирование о полномочиях, обязанностях и ответственности в области информационной безопасности, установленных должностными инструкциями, а также о мерах поощрения и дисциплинарного воздействия, применяемых в Банке за несоблюдение требований информационной безопасности;

в) в период трудовой деятельности:

- повышение осведомлённости, обучение и проведение тренингов;
- переподготовку и повышение квалификации сотрудников, ответственных за обеспечение информационной безопасности (получение необходимых компетенций);
- проверку и оценку уровня осведомлённости и квалификации работников Банка;
- информирование сотрудников о положениях и требованиях настоящей Политики, а также о нормативных документах в области информационной безопасности;

– контроль соблюдения сотрудниками процедур и требований информационной безопасности;

– установление и применение мер дисциплинарного взыскания;

г) при увольнении или изменении места работы:

– установление обязательства о неразглашении конфиденциальной информации в течение 5 (пяти) лет после прекращения трудового договора с сотрудником, покинувшим либо сменившим должность;

– изъятие у увольняемых сотрудников либо сотрудников, переведённых на другую должность, конфиденциальной информации, а также средств обработки, передачи и хранения информации, которыми они пользовались в период трудовой деятельности;

– аннулирование всех прав логического и физического доступа к объектам защиты Банка для сотрудников, увольняемых либо переведённых на другую должность.

Квалификационные требования к специалистам, ответственным за обеспечение информационной безопасности, требования к уровню квалификации работников, деятельность которых связана с процессами обработки информации, а также их функциональные обязанности определяются Управлением информационной безопасности.

Определение обязанностей и ответственности в области информационной безопасности в трудовых договорах, а также доведение соответствующей информации до работников Банка относится к компетенции Департамента управления персоналом.

В Банке на регулярной основе реализуются мероприятия по повышению уровня осведомлённости, обучению и подготовке персонала, а также по оценке уровня осведомлённости и квалификации в области информационной безопасности.

Управление информационной безопасности проводит для работников Банка тренинги и семинары по вопросам информационной безопасности в целях повышения уровня их осведомлённости и понимания своих обязанностей и ответственности.

Проверка и оценка уровня осведомлённости работников осуществляются посредством аттестации, тестирования и анкетирования работников Банка и отдельных специалистов по результатам тренингов, обучающих мероприятий и семинаров, проводимых Управлением информационной безопасности.

7.4.5. Банк применяет меры дисциплинарного взыскания в отношении работников Банка в следующих целях:

– установление дисциплинарной ответственности в отношении лиц, нарушивших Политику информационной безопасности Банка или установленные процедуры;

– предупреждение нарушений требований информационной безопасности со стороны работников Банка;

– привлечение к ответственности лиц, виновных в умышленном нарушении требований информационной безопасности;

– формирование у работников ответственного отношения к вопросам информационной безопасности и стимулирование соблюдения требований информационной безопасности.

7.4.6. Организационные меры по ограничению физического доступа к объектам защиты (физическая безопасность) направлены на предотвращение несанкционированного физического доступа к охраняемым объектам Банка, их повреждения и иных негативных воздействий.

На территории Банка, в зданиях Банка и его структурных подразделений должны быть чётко определены периметры физической безопасности помещений Банка.

Периметры физической защиты здания и помещений Банка подразделяются на следующие зоны безопасности:

1. *зоны низкого уровня безопасности (зона обслуживания 1-го уровня)* - помещения и места для приёма посетителей, а также зоны обслуживания клиентов в Головном офисе и торговых офисах;

2. *зоны среднего уровня безопасности (зона обслуживания 2-го уровня)* - помещения и территории, доступ в которые разрешён только работникам Банка: служебные помещения структурных подразделений, а также прилегающие к ним коридоры Головного офиса, ИТ-офиса и торговых офисов;

3. *зоны высокого уровня безопасности (защищённая зона 3-го уровня)* - помещения и территории, доступ в которые разрешён ограниченному кругу работников Банка: серверное помещение центра обработки данных, хранилище кассы Головного офиса.

7.4.7. Организационные меры по обеспечению физической безопасности в Банке включают:

1) в отношении зданий и помещений:

– обеспечение охраны периметра здания Головного офиса Банка и опорных пунктов обслуживания;

– организацию пропускного режима (контрольно-пропускные пункты для входа/выхода работников, а также въезда/выезда автотранспортных средств на территории Головного офиса);

– размещение критически важных активов объектов информатизации на максимально возможном удалении от границ контролируемой территории в Головном офисе, ИТ-офисе и торговых офисах;

– оформление материальных пропусков на ввоз и вывоз материальных ценностей и имущества в здания Головного офиса и торговых офисов Банка;

– сопровождение посетителей в здании Головного офиса и ИТ-офиса (зона 2) и (или) в служебных помещениях торговых офисов;

– определение перечня лиц, допущенных в защищённые помещения зоны 3;

2) в отношении средств обработки, хранения, передачи и защиты информации:

– размещение средств в защищённых помещениях;

– установку средств в запираемых коммутационных шкафах;

– использование замков на внешних корпусах оборудования, одноразовых пломб, печатей, защитных клейких лент, защитных и голографических наклеек либо иных средств выявления фактов несанкционированного физического доступа;

3) в отношении конфиденциальной информации на бумажных носителях:

– использование сейфов, запираемых металлических шкафов и иных защищённых хранилищ;

– регистрацию таких носителей в соответствующих журналах учёта;

4) в отношении кабелей электропитания и сетевых кабелей применение организационных мер по защите от повреждения и несанкционированного воздействия в целях предотвращения перехвата информации и нанесения ущерба, указанных в разделе 9 настоящей Политики.

Охрана здания Головного офиса и территориальных торговых офисов обеспечивается Национальной гвардией на договорной основе.

Порядок доступа в Банк осуществляется в соответствии с Правилами пропускного режима в Банке, утверждёнными протоколом Правления Банка № 7 от 24 сентября 2020 года.

7.4.8. Организационные меры по защите конфиденциальной информации включают:

1) определение перечня сведений, составляющих конфиденциальную информацию Банка, а также внесение в данный перечень изменений и дополнений при необходимости;

2) определение перечня работников Банка, которым предоставлен доступ к конфиденциальной информации Банка;

3) принятие работниками Банка обязательств по неразглашению конфиденциальной информации Банка;

4) определение в договорах, заключаемых с контрагентами Банка, условий, требований, обязательств и ответственности, связанных с раскрытием либо неразглашением конфиденциальной информации, а также заключение соглашений о неразглашении (NDA);

5) использование грифов конфиденциальности для конфиденциальной информации и её материальных носителей;

6) регистрацию и учёт носителей, содержащих конфиденциальную информацию;

7) установление ограничений либо требований по защите при передаче конфиденциальной информации через локальные, корпоративные и внешние сети, электронную почту, систему электронного документооборота, а также установление ограничений на распространение конфиденциальной информации в интернет-ресурсах, социальных сетях, средствах массовой информации и иных источниках;

8) установление ограничений либо требований по защите при хранении конфиденциальной информации в бумажной и электронной форме

на средствах обработки информации, электронных носителях, мобильных устройствах и иных средствах;

9) определение порядка доступа к конфиденциальной информации и её использования;

10) определение перечня помещений, в которых осуществляется обработка и хранение конфиденциальной информации, а также установление требований по их защите от несанкционированного физического доступа;

11) определение объектов информатизации, используемых для обработки и хранения конфиденциальной информации в электронной форме, а также установление требований по их защите от несанкционированного логического доступа;

12) установление требований по возврату материальных носителей конфиденциальной информации в случае увольнения работников Банка либо их перевода на другую должность;

13) обеспечение контроля за соблюдением требований по защите конфиденциальной информации.

Работа с информацией, подлежащей защите, должна осуществляться в соответствии с Инструкцией о порядке учёта, обращения и хранения документов, файлов и изданий, содержащих информацию ограниченного распространения, не являющуюся конфиденциальной, утверждённой решением заместителя Премьер-министра Республики Узбекистан от 5 декабря 2006 года, а также Инструкцией о порядке учёта, ведения и хранения документов и файлов, содержащих информацию ограниченного распространения (ДСП), утверждённой протоколом Правления Банка № 32 от 2 декабря 2022 года.

При обработке конфиденциальной информации работники Банка обязаны руководствоваться Положением о соблюдении режима коммерческой тайны (конфиденциальности), утверждённым протоколом Правления Банка № 32 от 2 декабря 2022 года, а также Положением о порядке обработки персональных данных работников АО «Anor Bank», утверждённым протоколом Правления Банка № 7-1 от 16 мая 2023 года.

7.4.9. В целях создания, функционирования и развития системы и средств защиты информации реализуются следующие организационные мероприятия:

а) приобретение средств защиты информации в рамках реализации мероприятий по обеспечению информационной безопасности Банка;

б) определение технических требований к приобретаемым средствам защиты информации;

в) реализация организационных мероприятий по подготовке к внедрению и сопровождению системы и средств защиты информации, включая выделение помещений, разработку эксплуатационных инструкций, назначение ответственных работников и их обучение эксплуатации соответствующих систем и средств;

г) проведение опытной эксплуатации, а также приёмо-сдаточных испытаний при внедрении средств защиты информации;

д) управление системой защиты информации, включая контроль конфигурации и настроек, восстановление работоспособности, установку обновлений программного обеспечения, актуализацию эксплуатационной документации, мониторинг инцидентов информационной безопасности, проведение контрольных процедур и документирование результатов контроля;

е) подготовка и внесение предложений по совершенствованию системы защиты информации в случае выявления недостатков в её функционировании либо необходимости повышения уровня защищённости.

Указанные в настоящем пункте организационные мероприятия по созданию, эксплуатации и развитию системы и средств защиты информации в Банке осуществляются Управлением информационной безопасности во взаимодействии с Департаментом информационных технологий.

7.4.10. Банк реализует организационные мероприятия по реагированию на инциденты информационной безопасности, предусмотренные разделом 8 настоящей Политики.

Организационные мероприятия по контролю и оценке состояния безопасности применяются в следующих целях:

- выявление уязвимостей и недостатков системы менеджмента информационной безопасности;
- объективная оценка состояния защищённости объектов защиты от угроз информационной безопасности;
- определение соответствия системы менеджмента информационной безопасности и применяемых в её рамках методов и средств защиты информации требованиям настоящей Политики и нормативных документов;
- оценка эффективности применяемых мер и средств защиты информации;
- оценка достижения Банком целей в области информационной безопасности и другие цели.

Для контроля и оценки состояния безопасности осуществляются следующие организационные мероприятия:

1) проведение внутренних и внешних аудитов в целях оценки уровня защищённости объектов защиты, а также оценки актуальности и эффективности настоящей Политики;

2) оценка эффективности реализованных организационных, технических и иных мер защиты, а также устранение недостатков, выявленных по результатам аудита.

Внутренний аудит проводится не реже одного раза в год, внешний аудит - не реже одного раза в три года.

Внутренний аудит проводится Управлением информационной безопасности с привлечением, при необходимости, специалистов Управления общей безопасности и Департамента информационных технологий.

Для проведения внешнего аудита информационной безопасности привлекаются сторонние организации, уполномоченные на проведение такого аудита.

Результаты проверок подлежат документированию. В соответствующих документах должны быть отражены:

- выявленные уязвимости, недостатки и несоответствия;
- причины выявленных несоответствий;
- необходимость принятия мер для достижения соответствия и перечень таких мер;
- оценка эффективности мер и средств защиты информации и иные результаты проверки.

По результатам аудита и иных проверок Управление информационной безопасности должно разрабатывать и реализовывать мероприятия по устранению выявленных уязвимостей, недостатков и несоответствий, а также по повышению эффективности защиты информации.

7.5. Технологические (технические) меры

7.5.1. Технологические (технические) меры по обеспечению информационной безопасности Банка направлены на:

- обеспечение безопасности хранения данных, их защиту от утечки и утраты, кражи или потери носителей информации и устройств хранения данных, а также от повреждения данных;
- обеспечение надёжного, устойчивого и безопасного функционирования объектов защиты;
- защиту объектов защиты от нарушений непрерывности их функционирования;
- обеспечение защищённости объектов защиты от воздействия внешней среды, стихийных бедствий и чрезвычайных ситуаций;
- оперативное восстановление функционирования объектов защиты в аварийных ситуациях.

7.5.2. Банк должен принимать меры по обеспечению безопасного хранения данных, их защите от утечки и утраты, кражи или потери носителей и устройств хранения данных, а также от повреждения данных в соответствии с требованиями DSt ISO/IEC 27040:2018 «Информационные технологии. Методы обеспечения безопасности. Безопасность хранения данных».

К мерам информационной безопасности относятся:

- защита объектов хранения и носителей информации от несанкционированного доступа;
- надлежащее и контролируемое уничтожение носителей информации и устройств хранения данных;
- обеспечение физической защиты устройств хранения данных;
- использование средств аутентификации и мониторинга доступа к устройствам хранения данных;
- регулярное резервное копирование данных, размещённых на устройствах хранения.

Для обеспечения надёжной защиты данных Банк обязан реализовывать следующие технические (технологические) меры:

- распределение критически важных ресурсов хранения данных;
- резервное копирование данных;
- удалённое отказоустойчивое онлайн-зеркалирование данных критически важных информационных систем;
- кластеризацию отказоустойчивых приложений и связанных с ними систем вокруг единой копии данных;
- долгосрочное хранение корпоративной конфиденциальной информации;
- распределение баз данных и файловых систем;
- обеспечение хранения данных для оперативного восстановления (из резервных копий) и архивирования.

В рамках стратегии обеспечения устойчивости данных необходимо:

- предусматривать меры по восстановлению данных в планах восстановления после чрезвычайных ситуаций;
- хранить резервные копии данных в хранилищах, географически удалённых от мест хранения основных данных.

Технологические (технические) меры защиты информации, связанные с эксплуатацией, администрированием, техническим обслуживанием, настройкой и уничтожением данных, включают:

- выполнение операций, направленных на обеспечение непрерывного функционирования объектов хранения данных;
- деятельность администраторов по мониторингу и распределению ресурсов инфраструктуры хранения данных, а также выполнение всех мероприятий, необходимых для управления системами хранения данных;
- проведение технического обслуживания, связанного с ремонтом и модернизацией оборудования и систем;
- установку специализированных профилей программного обеспечения и подготовку систем к эксплуатации;
- реализацию мер по уничтожению данных, направленных на сохранение конфиденциальности информации в случаях вывода носителей информации из эксплуатации либо изменения носителей таким образом, чтобы доступ к содержащейся на них информации был невозможен.

7.5.3. Защите подлежат следующие данные:

- база данных АБС;
- базы данных информационных систем RBS BSS, ELMA, Wings, BillMaster, AGC (ADPMS), AnorHub, Qlik Sense, Confluence, GitLab, Jira, Keycloak, MerchantCabinet, ServiceDesk, Verifix, WEBIM, Superset, IC и других информационных систем;
- базы данных систем обмена информацией: корпоративной электронной почты, корпоративного мессенджера, системы электронного документооборота;
- база данных официального веб-сайта Банка;
- настройки и базы данных сервера контроллера домена;

– настройки и базы данных средств информационной безопасности - межсетевых экранов, средств предотвращения вторжений (IPS), DLP-систем, средств оперативного мониторинга, антивирусных средств и иных средств защиты информации;

– настройки сетевого оборудования.

Указанные данные хранятся в серверных хранилищах, а их резервные копии - в системе хранения данных, на резервных серверах баз данных и на ленточных носителях (электронном архиве).

7.5.4. Для хранения резервных копий данных и средств информационных систем, указанных в пункте 7.5.3 настоящей Политики, используется система хранения данных, подключённая к сети хранения данных SAN (Storage Area Network).

Для обеспечения надёжности и сохранности данных информационных систем при хранении баз данных на серверах и в системе хранения данных используется технология RAID.

7.5.5. В целях обеспечения физической защиты данных все серверы и системы хранения данных, а также ленточные накопители размещаются в физически защищённых серверных помещениях основного и резервного центров обработки данных Банка, доступ к которым ограничен для неуполномоченных лиц.

Автоматизированная банковская система (АБС) обеспечивает удалённое отказоустойчивое онлайн-зеркалирование серверов приложений и баз данных.

Основные серверы АБС размещаются в основном центре обработки данных (Головной офис Банка), а резервные серверы АБС - в географически удалённом резервном центре обработки данных (ЦОД АО «Узбектелеком», АТС-233, г. Ташкент).

База данных основного сервера АБС непрерывно реплицируется на резервный сервер базы данных АБС, расположенный в резервном центре обработки данных.

Базы данных АБС основного и резервного центров обработки данных соединены посредством волоконно-оптической линии связи (ВОЛС), организованной непосредственно между указанными центрами обработки данных.

7.5.6. Сеть хранения данных SAN построена на базе технологии Fibre Channel (FC), к которой могут подключаться все основные серверы баз данных и других информационных систем, системы хранения данных, ленточные накопители, а также системы резервного копирования и восстановления данных.

Сеть SAN организована в серверном помещении основного центра обработки данных на базе двух SAN-коммутаторов.

Кроме того, в основном центре обработки данных организована демилитаризованная зона (DMZ) в виде отдельного VLAN-сегмента, в котором размещаются серверы информационных систем и информационных ресурсов, а также серверы систем обмена информацией, подключённых к

внешней сети Интернет, включая: корпоративную электронную почту; официальный веб-сайт Банка; ресурсы интернет-банкинга; систему мобильного банкинга.

7.5.7. Для долгосрочного хранения резервных копий критически важных информационных систем Банк использует ленточные носители данных (ленточную библиотеку). С использованием ленточных носителей формируется электронный архив серверов и баз данных критически важных информационных систем. Срок хранения электронного архива составляет не менее 1 (одного) года.

7.5.8. Работники Банка подключаются к информационным системам через локальную проводную сеть Головного офиса. Работники удалённого ИТ-офиса и торговых офисов подключаются к информационным системам Банка через корпоративную сеть с использованием защищённых VPN-каналов IPSec, организованных для соединения ИТ-офиса и торговых офисов с Головным офисом.

При доступе к информационным системам пользователи проходят авторизацию на сервере контроллера домена, а также в соответствующих информационных системах с использованием логина и пароля.

Подключение пользователей к информационным системам Банка осуществляется через защищённые соединения HTTPS.

7.5.9. За каждой информационной системой Банка закрепляются администраторы информационной системы, а также администратор базы данных, являющиеся работниками Департамента информационных технологий.

Назначенные администраторы обеспечивают:

- настройку и администрирование серверов информационных систем, серверных систем хранения и систем хранения данных, а также просмотр и изменение всех их параметров;
- изменение правил создания и управления учётными записями, создание и назначение ролей/полномочий пользователям информационной системы;
- проверку параметров и конфигураций серверных систем хранения и систем хранения данных, а также журналов их функционирования и сбоев;
- выполнение резервного копирования и восстановления данных серверов информационных систем;
- проверку целостности данных, хранящихся в системах хранения, с использованием средств контроля целостности базы данных.

Управление информационной безопасности должно выполнять функции аудитора безопасности хранилищ данных информационных систем, включая проведение анализа безопасности, позволяющего:

- анализировать права доступа и полномочия пользователей;
- проверять параметры и конфигурации безопасности;
- осуществлять проверку журналов аудита.

7.5.10. Администраторы, указанные в пункте 7.5.8 настоящей Политики, осуществляют удалённый доступ к информационным системам

через локальную сеть или корпоративную сеть с использованием защищённых VPN SSL-соединений, организованных посредством VPN-шлюза. Подключение администраторов осуществляется через защищённые соединения, организованные с использованием протокола SSH.

При доступе к информационным системам администраторы проходят аутентификацию посредством протокола SSH, а также с использованием логина и пароля непосредственно в информационной системе, операционной системе сервера либо в системе управления базами данных.

Кроме того, при доступе к информационным системам администраторы проходят аутентификацию в системе управления привилегированными учётными записями (PAM). Через систему PAM осуществляется контроль доступа администраторов к серверам и базам данных информационных систем, а также мониторинг их действий.

7.5.11. В отношении хранилищ данных информационных систем должны осуществляться аудит, учёт и мониторинг безопасности, включая:

- регистрацию всех значимых событий в системе хранения данных;
- хранение данных регистрации событий;
- архивирование и хранение данных регистрации событий в соответствии с политикой хранения данных;
- синхронизацию времени устройств с надёжным внешним источником времени.

Для регистрации и учёта событий в хранилищах данных используется стандартный протокол Syslog (стандартный механизм передачи и регистрации сообщений о событиях, происходящих в системе).

Аудит, учёт и мониторинг безопасности хранилищ данных осуществляются Управлением информационной безопасности, в том числе посредством системы мониторинга функционирования серверов и системы мониторинга событий безопасности SIEM.

Выявленные нарушения политики безопасного хранения данных подлежат регистрации в журнале инцидентов информационной безопасности.

7.5.12. Уничтожение данных на носителях информации и устройствах хранения данных осуществляется в соответствии с Правилами безопасности при работе с носителями информации, мобильными устройствами и устройствами хранения данных, приведёнными в Приложении 7 к настоящей Политике.

7.5.13. В целях усиления защиты данных информационных систем на серверах и в системах хранения данных администраторы информационных систем дополнительно обязаны принимать следующие меры:

- удаление ненужного и неиспользуемого программного обеспечения;
- удаление неиспользуемых учётных записей;
- переименование, удаление либо изменение паролей встроенных и стандартных учётных записей;
- открытие только необходимых для эксплуатации сетевых портов;

– установка актуальных обновлений безопасности (патчей), полученных из доверенных источников;

– обновление микропрограммного обеспечения (прошивок), полученного из доверенных источников;

– внедрение и поддержание средств защиты от вредоносного программного обеспечения.

7.5.14. Для обеспечения устойчивого и непрерывного функционирования объектов защиты реализуются следующие мероприятия:

1) проведение соответствующего технического обслуживания (функциональный мониторинг, профилактическое обслуживание, ремонт) в целях обеспечения постоянной доступности и целостности оборудования;

2) документирование практических процессов, связанных с открытием оборудования, ремонтом, вводом в эксплуатацию, резервным копированием, изменением конфигурации и другими аналогичными действиями;

3) ведение и анализ системных журналов оборудования и информационных систем;

4) надлежащее управление изменениями в средствах и системах обработки информации, отказ которых может привести к сбоям, неисправностям или нарушениям безопасности;

5) управление производительностью и ёмкостью ресурсов - планирование и прогнозирование будущих потребностей, мониторинг использования ресурсов, резервирование ресурсов и дополнительных мощностей;

6) разделение сред разработки, тестирования и эксплуатации - работы по разработке и тестированию должны выполняться на оборудовании, изолированном от эксплуатируемых производственных систем;

7) обеспечение резервирования средств обработки, хранения, передачи и защиты информации;

8) резервное копирование данных и программного обеспечения;

9) управление программным обеспечением, включая его установку, изменение, настройку и обновление;

10) установление правил, запрещающих приём пищи, употребление напитков и курение в непосредственной близости от объектов обработки информации.

7.5.15. Резервированию подлежат следующие технические средства:

– серверы АБС и других информационных систем (серверы баз данных и серверы приложений);

– ядро основных коммутаторов, используемых для организации корпоративной сети;

– межсетевые экраны и шлюзы безопасности, используемые на границах подключения основного и резервного центров обработки данных к корпоративной сети, внешней сети Интернет и БТТ Центрального банка.

Требования к резервированию средств обработки, хранения, передачи и защиты информации, а также каналов связи устанавливаются Порядком

обеспечения непрерывности деятельности и восстановления функционирования в чрезвычайных и аварийных ситуациях, приведённым в Приложении 14 к настоящей Политике.

Резервному копированию подлежат базы данных и журналы аудита (лог-файлы), программное обеспечение информационных систем Банка, а также конфигурационные параметры (настройки) сетевого оборудования и средств защиты информации.

В Банке резервное копирование и восстановление данных, а также обновление системного и прикладного программного обеспечения осуществляются в соответствии с Положением о резервном копировании и восстановлении данных, приведённым в Приложении 4 к настоящей Политике.

Для обеспечения резервного копирования данных применяются системы резервного копирования и восстановления данных, указанные в Приложении 18 к настоящей Политике.

7.5.16. Для обеспечения бесперебойного электроснабжения должны реализовываться следующие меры:

1) в здании Головного офиса (основного центра обработки данных), а также в пунктах обслуживания используются дизельные генераторы и источники бесперебойного питания;

2) для основных информационных систем, систем обмена информацией, сетевого оборудования и средств защиты информации, размещённых в резервном центре обработки данных (ЦОД АО «Узбектелеком», АТС-233), предусматриваются меры по обеспечению непрерывного функционирования с использованием дизельных генераторов и источников бесперебойного питания.

Каналы связи, используемые для подключения корпоративной сети Банка к внешней сети Интернет и БТТ Центрального банка, должны быть резервированными.

Основное телекоммуникационное оборудование, базы данных, серверы информационных систем и средства обеспечения информационной безопасности должны размещаться как в основном, так и в резервном центрах обработки данных.

Центр обработки данных АО «Узбектелеком» (АТС-233), используемый для организации резервного центра, а также серверное помещение основного центра в здании Головного офиса должны соответствовать требованиям O‘zDSt 2875:2014 «Требования к центрам обработки данных», включая:

- обеспечение бесперебойного электроснабжения;
- поддержание требуемых климатических условий (системы кондиционирования воздуха);
- обеспечение пожарной безопасности.

7.5.17. Мероприятия по восстановлению включают:

1) разработку, обучение и тестирование планов восстановления;

2) ввод в эксплуатацию резервного оборудования, каналов связи, линий связи или источников электропитания в случае возникновения аварийной ситуации;

3) восстановление программного обеспечения и данных из резервных копий;

4) ремонт либо замену оборудования;

5) перезапуск или переустановку программного обеспечения и иные аналогичные мероприятия.

Порядок реализации мероприятий по восстановлению регулируется Планом обеспечения непрерывности деятельности и восстановления в чрезвычайных и аварийных ситуациях, приведённым в Приложении 14 к настоящей Политике.

7.6. Инженерно-технические меры

7.6.1. Инженерно-технические меры направлены на предотвращение физического доступа неуполномоченных лиц к объектам защиты либо создание физических препятствий для такого доступа и включают следующие мероприятия:

1) определение границ доступа в зоны и служебные помещения Головного офиса посредством дверей и иных инженерно-технических средств;

2) использование идентификационных пластиковых карт работников либо средств идентификации личности (Face ID), а также кодовых замков для доступа в здание и на территорию Головного офиса, оборудованные системой контроля и управления доступом (СКУД), включая отдельные служебные помещения и коридоры, ведущие к таким помещениям;

3) использование металлических дверей на входах в помещения зоны 3;

4) использование электронных замков на входах в служебные помещения зоны 2;

5) использование датчиков системы мониторинга и технической сигнализации (СМТ) на дверях и окнах Головного офиса;

6) оснащение окон Головного офиса, ИТ-офиса и пунктов обслуживания средствами защиты от визуального наблюдения (шторы, жалюзи);

7) использование системы видеонаблюдения для контроля территории здания Головного офиса, ИТ-офиса, а также коридоров и помещений пунктов обслуживания;

8) установка охранной сигнализации и датчиков в защищённых помещениях для фиксации фактов несанкционированного физического доступа;

9) использование запираемых металлических несгораемых шкафов для хранения документированной конфиденциальной информации.

7.7. Аппаратно-программные меры

7.7.1. Аппаратно-программные меры по обеспечению информационной безопасности направлены на:

- организацию технической защиты информации;
- организацию криптографической защиты информации.

7.7.2. Аппаратно-программные меры основываются на использовании аппаратных, программных и технических средств защиты информации, предназначенных для обеспечения:

- информационной безопасности на уровне сетевой инфраструктуры (сетевой безопасности);
- разграничения и управления логическим доступом к объектам защиты;
- антивирусной защиты;
- защиты конфиденциальной информации от утечки;
- контроля и анализа безопасности;
- мониторинга и управления инцидентами информационной безопасности и иных функций обеспечения информационной безопасности.

7.7.3. Меры по обеспечению сетевой безопасности включают:

1) определение безопасной архитектуры сетевой инфраструктуры Банка;
2) физическую и виртуальную сегментацию сети Банка;
3) использование средств сетевой безопасности (межсетевые экраны, системы обнаружения и предотвращения вторжений IDS/IPS, средства VPN, межсетевые экраны веб-приложений WAF);
4) организацию защищённых каналов связи и сетевых соединений.

7.7.4. Безопасная архитектура корпоративной сети, принципы её построения, а также порядок организации защищённых каналов связи и сетевых соединений определяются Положением об организации корпоративной сети и защищённых сетевых соединений, приведённым в Приложении 1 к настоящей Политике.

7.7.5. Обеспечение безопасности сетевой инфраструктуры и использование межсетевых экранов осуществляются в соответствии с Положением об обеспечении информационной безопасности на уровне сетевой инфраструктуры и межсетевых экранов, приведённым в Приложении 2 к настоящей Политике.

7.7.6. С учётом рисков информационной безопасности, связанных с сетевыми атаками и угрозами, Банк должен использовать аппаратно-программные сетевые средства IDPS (системы обнаружения и предотвращения вторжений), обладающие следующими требованиями и функциональными возможностями:

- поддержка технологий SD-WAN и VPN для распределённых сетей и удалённых пользователей;
- глубокий анализ пакетов сетевого трафика (Deep Packet Inspection) по всем протоколам, включая протоколы прикладного уровня;
- наличие производительности, обеспечивающей обработку и передачу всего внешнего сетевого трафика с применением глубокого анализа пакетов;

– поддержка сигнатурного метода выявления сетевых вторжений в сетевом трафике;

– возможность обновления базы сигнатур от производителя;

– поддержка поведенческого метода выявления сетевых вторжений на основе аномалий сетевого трафика и отклонений в работе сетевых протоколов;

– блокирование и фильтрация подозрительного трафика;

– обеспечение защиты от веб-угроз, включая угрозы на основе DNS и вредоносные URL-адреса;

– контроль приложений;

– обнаружение и предотвращение атак типа DoS и DDoS;

– выявление и фильтрация сетевого трафика, содержащего вредоносный код;

– наличие функций контроля целостности защищаемого сетевого объекта IDPS;

– поддержка протокола простого сетевого управления (SNMP);

– формирование уведомлений о выявленных и предотвращённых атаках.

Сетевое средство IDPS должно обеспечивать защиту локальных сетей от угроз со стороны внешних и корпоративных сетей.

Банк использует сетевые средства IDPS, встроенные в межсетевые экраны, - аппаратно-программные межсетевые экраны с функциями IDPS.

Межсетевые экраны с функциями IDPS используются для:

– внешней защиты локальной сети Головного офиса при подключении к внешней сети, а также локальных сетей резервного центра обработки данных и ИТ-офиса при их подключении к внешней сети;

– внешней защиты локальной сети Головного офиса при подключении к корпоративной сети, а также локальных сетей резервного центра обработки данных и ИТ-офиса при их подключении к корпоративной сети;

– внутренней защиты DMZ-зоны основного центра обработки данных, серверных сегментов основного и резервного центров обработки данных, а также процессингового центра основного центра обработки данных при их подключении к локальным сетям.

7.7.7. Банк должен устанавливать на рабочих станциях и критически важных серверах средства HDPS (Host-based Detection and Prevention System), обладающие следующими функциями:

– выявление вредоносной активности путём мониторинга процессов, приложений, файлов и реестра операционной системы;

– контроль входящего и исходящего сетевого трафика;

– настройка параметров для отдельных портов, приложений и IP-адресов;

– защита от сетевых атак и анализ подозрительной сетевой активности;

– поддержка мультиплатформенных сред и обеспечение защиты файловых серверов, функционирующих под управлением Linux и Windows, включая кластерные серверы;

– защита от атак с использованием вредоносного программного обеспечения;

– поиск и выявление уязвимостей.

В качестве HDPS Банк использует систему антивирусной защиты, обладающую дополнительными функциями HDPS.

Для обеспечения функционирования HDPS антивирусное программное обеспечение должно быть соответствующим образом настроено на рабочих станциях и серверах.

7.7.8. В целях разграничения доступа к информационным ресурсам и информационным системам Банка разработана матрица доступа, сформированная в соответствии с Правилами разработки матрицы доступа к информационным ресурсам, приведёнными в Приложении 8 к настоящей Политике.

7.7.9. В Банке аутентификация пользователей при доступе к объектам защиты осуществляется с использованием паролей и иных идентификаторов в соответствии с Инструкцией по парольной защите и аутентификации пользователей в информационных системах, приведённой в Приложении 5 к настоящей Политике.

7.7.10. В Банке для обеспечения антивирусной защиты применяются следующие меры и средства антивирусной защиты:

1) использование средств защиты от вредоносного программного обеспечения (антивирусного программного обеспечения) на средствах обработки информации, включая мобильные устройства, обеспечивающих обнаружение, блокирование и восстановление после воздействия вредоносного программного обеспечения, а также информирование пользователей о выявленных угрозах;

2) принятие Политики антивирусной защиты, устанавливающей требования по защите от вредоносного программного обеспечения, обязательные для исполнения работниками Банка;

3) выявление и устранение уязвимостей, которые могут быть использованы вредоносным программным обеспечением;

4) блокирование использования USB-портов на средствах обработки информации.

7.7.11. Процессы организации и обеспечения антивирусной защиты, а также порядок установления и соблюдения работниками требований по защите от вредоносного программного обеспечения определяются Инструкцией по антивирусной защите, приведённой в Приложении 6 к настоящей Политике.

7.7.12. В Банке используются следующие технические средства защиты информации:

– в качестве средства контроля и анализа безопасности используются система управления уязвимостями и сканеры безопасности корпоративной инфраструктуры Банка;

– в качестве средства защиты конфиденциальной информации от утечки используется DLP-система;

– для мониторинга и управления инцидентами информационной безопасности используется система SIEM;

– для контроля действий привилегированных пользователей (администраторов) Банк использует систему PAM;

– криптографическая защита информации организуется с использованием средств криптографической защиты информации (далее - СКЗИ).

Применяемые методы и средства технической защиты информации определяются Правилами организации технической защиты информации, приведёнными в Приложении 23 к настоящей Политике.

7.7.13. В Банке средства криптографической защиты информации используются при предоставлении цифровых банковских услуг клиентам Банка - юридическим лицам через систему интернет-банкинга BSS DBO для формирования и проверки электронной цифровой подписи (ЭЦП), а также работниками Банка при использовании системы электронного документооборота MyAnor.uz.

Для использования ЭЦП в системе BSS DBO корпоративными клиентами цифровых банковских услуг Банка применяются личные ключи ЭЦП и сертификаты открытых ключей ЭЦП, выданные Регистрационным центром ключей электронной цифровой подписи Государственного налогового комитета Республики Узбекистан.

В системе электронного документооборота MyAnor.uz работники Банка также используют личные ключи ЭЦП и сертификаты открытых ключей ЭЦП, выданные Регистрационным центром ключей электронной цифровой подписи Государственного налогового комитета Республики Узбекистан.

Средства криптографической защиты информации применяются в защищённой системе электронной почты, к которой подключены работники Управления секретариата Банка.

Средства криптографической защиты информации дополнительно используются для организации защищённых сетевых соединений в корпоративной сети Банка и при взаимодействии с информационными системами третьих лиц.

Банк обязан использовать только те средства криптографической защиты информации, которые сертифицированы органом по сертификации средств криптографической защиты информации в соответствии с Постановлением Президента Республики Узбекистан № ПП-614 от 3 апреля 2007 года.

Применение методов и средств криптографической защиты информации в Банке осуществляется в соответствии с Инструкцией по

организации криптографической защиты информации, приведённой в Приложении 13 к настоящей Политике.

7.7.14. Перечень используемых в Банке аппаратных, программных и средств информационной безопасности, а также сетевого и серверного оборудования и программного обеспечения приведён в Приложении 18 к настоящей Политике.

7.8. Меры безопасности при взаимодействии с внешними пользователями

7.8.1. В целях защиты информационных активов Банка должны применяться меры по обеспечению информационной безопасности при взаимодействии с организациями третьих лиц и при работе с клиентами, которым предоставляется доступ либо возможность получения доступа к информационным активам Банка.

При этом организации третьих лиц могут иметь как физический, так и логический доступ к информационным активам Банка, тогда как клиенты Банка могут получать доступ к информационным активам Банка исключительно на логическом уровне.

Банк осознаёт, что предоставление такого доступа либо возможности его получения может привести к нарушению или снижению уровня информационной безопасности.

7.8.2. Меры информационной безопасности рассматриваются в следующих случаях взаимодействия с третьими лицами:

1) при оказании услуг или выполнении работ третьими лицами (подрядчиками, поставщиками и иными организациями);

2) при взаимодействии информационной системы Банка с информационной системой сторонней организации;

3) при приёме представителей внешних организаций и проведении встреч с ними.

7.8.3. Меры информационной безопасности также определяются при работе с клиентами, использующими цифровые банковские услуги (онлайн-сервисы).

7.8.4. При взаимодействии со сторонними организациями, оказывающими услуги или выполняющими работы, Банк принимает следующие меры по обеспечению информационной безопасности:

1) до заключения договора определяет требования к сторонней организации и её специалистам, которым будет предоставлен доступ к объектам защиты Банка и возможность работы с ними;

2) включает требования информационной безопасности в условия договоров, заключаемых со сторонними организациями;

3) заключает со сторонними организациями дополнительные соглашения о конфиденциальности либо включает соответствующие условия в договоры;

4) определяет перечень информации и объектов защиты, к которым сторонняя организация получает доступ при оказании услуг или выполнении

работ, а также перечень сотрудников сторонней организации, которым предоставляется такой доступ;

5) устанавливает процедуры предоставления доступа третьим лицам с указанием видов доступа и порядка его предоставления;

6) доводит требования информационной безопасности Банка до специалистов сторонней организации до начала выполнения работ;

7) до предоставления доступа к информации и объектам защиты обеспечивает внедрение соответствующих мер защиты и средств контроля и управления доступом (физического и/или логического);

8) обеспечивает физическое разделение средств обработки информации, находящихся под управлением Банка, и средств обработки информации, находящихся под управлением сторонней организации;

9) осуществляет контроль, мониторинг и управление доступом сторонней организации к объектам обработки, передачи и защиты информации;

10) обеспечивает постоянное присутствие работника Банка при выполнении работ сторонней организацией на объектах защиты;

11) предоставляет сторонней организации уникальные идентификаторы доступа, исключающие использование привилегированных прав доступа, известных работнику Банка;

12) после завершения работ сторонней организацией аннулирует предоставленные права доступа, осуществляет проверку целостности данных и контроль настроек оборудования;

13) согласовывает использование и размещение технических средств, принадлежащих сторонней организации.

Указанные меры, порядок их реализации, а также иные требования Банка в области информационной безопасности должны быть определены в договоре, заключаемом со сторонней организацией.

Соглашение о неразглашении конфиденциальной информации (NDA), заключаемое со сторонней организацией, должно устанавливать обязательства по неразглашению конфиденциальной информации и ответственность сторонней организации в случае раскрытия такой информации по её вине, включая возмещение ущерба, причинённого Банку вследствие такого раскрытия.

Требования NDA подлежат соблюдению в течение всего срока действия договора и не менее 5 (пяти) лет после его прекращения.

7.8.5. При взаимодействии информационной системы Банка с информационной системой сторонней организации либо при предоставлении работникам сторонней организации доступа к информационной системе Банка применяются следующие меры обеспечения информационной безопасности:

1) установление требований информационной безопасности при подключении информационной системы либо сотрудников сторонней организации;

2) принятие Банком мер и использование средств защиты, исключающих несанкционированный логический доступ сторонней организации к информационной системе Банка;

3) организация защищённых соединений для обмена информацией и иные необходимые меры безопасности.

Указанные меры должны быть закреплены в двусторонних соглашениях между сторонами.

Организация защищённых соединений осуществляется в соответствии с требованиями Положения об организации корпоративной сети и защищённых сетевых соединений, приведённого в Приложении 1 к настоящей Политике.

При подключении сторонних организаций и их информационных систем к информационным системам Банка должны применяться меры межсетевого экранирования в соответствии с Положением об обеспечении информационной безопасности на уровне сетевой инфраструктуры и межсетевых экранов, приведённым в Приложении 2 к настоящей Политике.

7.8.6. При взаимодействии АБС с информационными системами сторонних организаций применяются следующие меры:

а) подключение АБС к информационным системам сторонних организаций осуществляется через БТТ Центрального банка;

б) подключение АБС к внешним каналам связи для взаимодействия с информационными системами сторонних организаций осуществляется через межсетевые экраны и средства IDS/IPS;

в) при подключении АБС к внешним информационным системам организуются защищённые VPN-каналы IPSec.

7.8.7. В случае приёма и проведения встреч с представителями сторонних организаций Банк обязан принимать следующие меры, направленные на исключение несанкционированного физического доступа к объектам защиты Банка:

а) проведение встреч с представителями сторонних организаций в приёмных помещениях (переговорных комнатах Банка) либо в специально выделенных помещениях, расположенных на удалении от защищённых зон Банка и имеющих повышенный уровень безопасности;

б) сопровождение представителей сторонних организаций работниками Банка при их нахождении в здании Банка;

в) установление ограничений на предоставление представителям сторонних организаций права работы на рабочих станциях, подключённых к локальной или корпоративной сети Банка либо к информационным системам Банка, а также ограничений на подключение их устройств к сети и информационным системам Банка.

7.8.8. При работе с клиентами применяются следующие меры информационной безопасности:

– установление и реализация требований информационной безопасности, обязательных для клиентов при использовании цифровых банковских услуг;

– разграничение ответственности между Банком и клиентами при использовании цифровых банковских услуг;

– предоставление пользователям разрешённых способов доступа, а также организация управления и использования уникальных идентификаторов пользователей и паролей;

– аннулирование права доступа в случае нарушения пользователем требований информационной безопасности;

– ознакомление пользователей с рисками, возникающими при нарушении требований информационной безопасности при использовании цифровых банковских услуг.

Указанные требования безопасности, а также риски, связанные с их несоблюдением, должны быть отражены в договорах, заключаемых с клиентами.

7.8.9. Требования к обеспечению мер информационной безопасности при взаимодействии со сторонними организациями и работе с клиентами устанавливаются Управлением информационной безопасности.

Управление информационной безопасности также осуществляет контроль за соблюдением указанных требований структурными подразделениями и работниками Банка.

8. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. Одним из ключевых процессов интегрированной системы менеджмента информационной безопасности Банка является процесс управления инцидентами информационной безопасности.

Банк должен применять последовательный, эффективный и системный подход к управлению инцидентами информационной безопасности.

Целями управления инцидентами информационной безопасности в Банке являются:

– минимизация потерь и ущерба, причинённых Банку в результате инцидентов информационной безопасности;

– принятие оперативных и эффективных мер по локализации инцидентов, предотвращению угроз и устранению их последствий в максимально короткие сроки;

– извлечение уроков из произошедших инцидентов, снижение риска их повторения либо предотвращение подобных инцидентов в будущем;

– минимизация негативных последствий инцидентов для Банка и его деятельности;

– обеспечение взаимосвязи процесса реагирования на инциденты с соответствующими элементами кризисного управления и управления непрерывностью деятельности, включая процессы взаимодействия с внешними организациями;

– выявление и оценка уязвимостей информационной безопасности, а также их своевременное устранение в целях предотвращения либо снижения количества инцидентов, связанных с такими уязвимостями.

Установленные цели управления инцидентами информационной безопасности должны быть доведены до сведения работников, ответственных за управление инцидентами информационной безопасности, и использоваться в качестве приоритетов при реагировании на инциденты.

8.2. Банк должен применять следующие процедуры управления инцидентами информационной безопасности:

а) мониторинг и выявление инцидентов;

б) анализ, оценка и подготовка отчётности по инцидентам;

в) учёт и регистрация инцидентов;

г) уведомление и информирование об инцидентах;

д) локализация угрозы либо прекращение действия угрозы, приведшей к инциденту;

е) оценка последствий инцидента;

ж) восстановление после инцидента и устранение его последствий;

з) анализ инцидента и установление причин его возникновения;

и) разработка и реализация мер по предотвращению повторного возникновения инцидентов;

к) сбор, анализ и хранение доказательств, а также проведение расследований;

л) привлечение к ответственности лиц, виновных в возникновении инцидента и его последствиях.

8.3. Мониторингу подлежат все объекты защиты, определённые в разделе 4 настоящей Политики.

Мониторинг осуществляется в целях выявления инцидентов информационной безопасности и проводится в круглосуточном режиме.

Источниками информации об инцидентах информационной безопасности на объектах защиты являются:

– данные системы мониторинга и управления инцидентами информационной безопасности (далее - система SIEM);

– данные системных журналов (журналов аудита, лог-файлов) информационных систем, оборудования и программного обеспечения;

– данные, получаемые от средств защиты информации;

– результаты визуального контроля состояния функционирования оборудования и средств корпоративной сети Банка, информационных ресурсов и информационных систем;

– результаты внутреннего и внешнего аудита информационной безопасности;

– сведения и сообщения, поступающие от работников Банка;

– обращения и жалобы клиентов Банка, а также сторонних организаций, взаимодействующих с Банком;

– выявленные факты хищения, атак, утечки информации, несанкционированного доступа и иных нарушений информационной безопасности.

Мониторинг осуществляется работниками Управления информационной безопасности, Управления общей безопасности и Департамента информационных технологий Банка.

Для мониторинга и выявления инцидентов информационной безопасности Банк использует систему SIEM, указанную в Приложении 18 к настоящей Политике.

8.4. Анализ и оценка инцидента информационной безопасности проводятся в целях принятия решения о необходимости классификации соответствующего события как инцидента информационной безопасности.

В Банке к инцидентам информационной безопасности относятся следующие события:

1) чрезвычайные и аварийные ситуации (техногенные угрозы, стихийные бедствия, массовые беспорядки и иные аналогичные события);

2) сбои в функционировании и работе информационных систем Банка, включая отказы серверного и сетевого оборудования, а также сбои программного обеспечения;

3) нарушение конфиденциальности, целостности и доступности конфиденциальной информации Банка, а также нарушение требований по защите информации;

4) хищение, атаки, утечка информации и иные несанкционированные действия, повлёкшие материальный ущерб, включая факты утраты или хищения материальных ценностей, денежных средств, носителей информации и конфиденциальной информации;

5) нарушение связи с внешними сетями, сбои в корпоративной сети Банка и локальных сетях, технические неисправности сетевого оборудования, повреждение кабельных линий связи и иные аналогичные события;

6) отказ средств защиты информации по любым причинам, включая технические неисправности и ошибки, обусловленные человеческим фактором;

7) несанкционированный физический или логический доступ третьих лиц к информационным системам и информационным ресурсам Банка;

8) атаки типа DoS (Denial of Service) и DDoS (Distributed Denial of Service);

9) сетевые атаки, выявленные средствами защиты информации;

10) обнаружение опасных компьютерных вирусов и вредоносного программного обеспечения;

11) несанкционированное подключение устройств и сетевых узлов к локальным и корпоративным сетям;

12) несанкционированное проникновение посторонних лиц в защищённые помещения;

13) выявление незаконных действий по сбору, копированию, извлечению либо выведению информации.

Управление информационной безопасности несёт ответственность за анализ и оценку инцидентов информационной безопасности, их классификацию в качестве инцидентов информационной безопасности и определение уровня их критичности.

8.5. Все инциденты информационной безопасности, произошедшие в основном и резервном центрах обработки данных, а также в Головном офисе, ИТ-офисе и торговых офисах Банка, подлежат обязательному учёту.

Учёт выявленных инцидентов информационной безопасности осуществляется системой SIEM.

Для учёта инцидентов информационной безопасности, не выявленных системой SIEM, ведётся отдельная электронная база данных инцидентов информационной безопасности.

Управление информационной безопасности несёт ответственность за учёт выявленных инцидентов информационной безопасности, а также за ведение электронной базы данных инцидентов информационной безопасности Банка.

Форма электронной базы данных инцидентов информационной безопасности приведена в Регламенте реагирования на инциденты информационной безопасности, содержащемся в Приложении 15 к настоящей Политике.

Учёт инцидентов информационной безопасности необходим для установления причин их возникновения, анализа инцидентов и проведения оценки рисков информационной безопасности Банка.

Инциденты информационной безопасности с уровнем критичности «Высокий» подлежат отдельной регистрации.

Для регистрации таких инцидентов сведения о них вносятся в Реестр чрезвычайных ситуаций безопасности Банка, форма которого определена Регламентом реагирования на инциденты информационной безопасности, приведённым в Приложении 15 к настоящей Политике.

Управление информационной безопасности несёт ответственность за регистрацию инцидентов информационной безопасности с уровнем критичности «Высокий» и ведение Реестра чрезвычайных ситуаций безопасности Банка.

8.6. Об инцидентах информационной безопасности должны быть уведомлены:

- руководство структурных подразделений Банка, ответственных за производственную площадку или технологический процесс, пострадавшие в результате инцидента;
- руководство структурного подразделения либо специалист (администратор), ответственный за сопровождение соответствующего объекта защиты;
- руководство Банка;
- внешние заинтересованные организации.

8.7. Угроза, ставшая причиной возникновения инцидента, должна быть локализована либо нейтрализована в целях минимизации ущерба, перехода к восстановлению деятельности либо обеспечения выполнения иных задач и процессов Банка, не затронутых инцидентом информационной безопасности.

8.8. В ходе оценки последствий инцидента информационной безопасности должны быть определены масштабы причинённого ущерба и объём потерь, понесённых в результате инцидента.

После локализации или нейтрализации угрозы должны быть выполнены следующие мероприятия:

- работы по восстановлению деятельности и устранению последствий инцидента;
- анализ инцидента;
- уточнение источников и причин возникновения инцидента;
- сбор доказательств.

При анализе инцидента информационной безопасности необходимо определить:

- характеристики угроз, приведших к возникновению инцидента, а также частоту возникновения выявленных типов угроз;
- причины инцидента и источники угроз;
- факт использования уязвимостей при реализации инцидента;
- существующие ошибки и недостатки в системе защиты информации и системе управления инцидентами;
- эффективность действий работников, а также процедур и процессов управления инцидентами.

8.9. Результаты анализа инцидентов информационной безопасности и выводы, полученные по итогам их рассмотрения, должны использоваться для разработки и реализации мер, направленных на предотвращение повторного возникновения аналогичных инцидентов либо снижение вероятности их возникновения в будущем.

Указанные меры должны быть направлены на устранение выявленных недостатков, повышение эффективности системы защиты информации, устранение уязвимостей, а также совершенствование методов и средств защиты информации.

8.10. Локализация и нейтрализация воздействия угроз, оценка последствий инцидентов, восстановление деятельности и устранение последствий инцидентов, а также анализ инцидентов информационной безопасности осуществляются Группой реагирования на инциденты информационной безопасности Банка.

Состав Группы реагирования на инциденты информационной безопасности утверждается приказом Банка и подлежит пересмотру при необходимости (в случае перевода работников на другие должности, увольнения ответственных лиц либо приёма новых квалифицированных специалистов).

При необходимости и по согласованию с Председателем Правления Банка к выполнению указанных процедур могут привлекаться работники иных

структурных подразделений Банка либо представители заинтересованных организаций.

8.11. В рамках управления инцидентами информационной безопасности сбор доказательств должен быть направлен на выявление, сбор, изучение и сохранение информации, которая может использоваться в качестве доказательной базы в судебных и иных разбирательствах, а также служить основанием для привлечения виновных лиц к ответственности либо применения дисциплинарных мер воздействия.

Сбор доказательств осуществляется в процессе расследования инцидента.

Для проведения расследования инцидента по решению руководства Банка создаётся специальная комиссия (рабочая группа), состав которой определяется соответствующим распорядительным документом.

8.12. Порядок реализации процедур управления инцидентами информационной безопасности, указанных в пункте 8.2 настоящей Политики, обязанности руководства, ответственных лиц по устранению инцидентов, а также работников Банка в рамках управления инцидентами информационной безопасности определяются Положением о реагировании на инциденты информационной безопасности, приведённым в Приложении 15 к настоящей Политике.

При управлении инцидентами информационной безопасности Банк может взаимодействовать со следующими внешними организациями:

1) Центральным банком Республики Узбекистан - в части информирования о произошедших инцидентах, принятых мерах и ходе их реализации;

2) заинтересованными сторонними организациями, с которыми Банк взаимодействует в процессе своей деятельности (партнёрами, поставщиками услуг, поставщиками оборудования и решений), - в части уведомления об инцидентах, их локализации, устранения последствий и выработки совместных мер по предотвращению повторения аналогичных инцидентов;

3) правоохранительными органами - в части возбуждения и расследования дел, связанных с инцидентами информационной безопасности;

4) органами по чрезвычайным ситуациям - в части информирования о событиях, приведших к чрезвычайной ситуации, участия в ликвидации её последствий и расследовании причин возникновения;

5) клиентами Банка - в части информирования о сбоях, сроках их устранения, устранении недостатков, восстановлении предоставления услуг и иных вопросах, связанных с инцидентами информационной безопасности.

Порядок взаимодействия с организациями третьих лиц при управлении инцидентами информационной безопасности определяется Положением о реагировании на инциденты информационной безопасности, приведённым в Приложении 15 к настоящей Политике.

9. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КАНАЛОВ СВЯЗИ

9.1. В Банке электрические и сетевые кабели, используемые для передачи данных, должны быть защищены от повреждения в целях предотвращения перехвата информации и нарушения её целостности.

Для снижения указанных рисков в Банке применяются следующие меры защиты:

1) силовые и телекоммуникационные кабели должны по возможности прокладываться под землёй, в кабельной канализации, коллекторах либо внутри зданий, либо должны быть надлежащим образом защищены от несанкционированного физического доступа;

2) сетевые кабели, по возможности, должны прокладываться отдельно от силовых кабелей для исключения взаимного негативного воздействия;

3) маршрут прокладки сетевых кабелей должен выбираться таким образом, чтобы избегать мест общего пользования, а при отсутствии такой технической возможности сетевые кабели должны быть защищены специальными коробами или металлическими каналами;

4) неиспользуемые разъёмы сетевых кабелей должны быть опломбированы либо закрыты специальными защитными заглушками;

5) кроссовое и коммутационное оборудование, к которому подключены сетевые кабели, должно размещаться в защищённых помещениях либо в закрытых коммутационных шкафах;

6) неиспользуемые сетевые порты должны отключаться средствами управления телекоммуникационным и серверным оборудованием;

7) должны проводиться проверки (сканирование сети либо физические проверки) для выявления несанкционированного подключения устройств к кабельной сети.

9.2. В целях обеспечения конфиденциальности информации при её передаче через внешние телекоммуникационные сети и корпоративную сеть применяются следующие меры защиты:

1) использование собственной волоконно-оптической линии связи (ВОЛС) между Головным офисом (основным центром обработки данных) и резервным центром обработки данных, а также организация соединений IPsec VPN между основным и резервным центрами обработки данных;

2) организация соединений IPsec VPN при подключении ИТ-офиса и основных торговых офисов к Головному офису (основному центру обработки данных) через корпоративную сеть Банка;

3) использование соединений IPsec VPN, организованных через БТТ Центрального банка, для обеспечения взаимодействия АБС Банка с информационными системами сторонних организаций, включая банковские системы Центрального банка, процессинговые системы HUMO, UzCard и иные системы;

4) использование защищённых соединений на основе протокола SSL/TLS при предоставлении доступа к веб-ресурсам Банка через корпоративную сеть и сеть Интернет (официальный веб-сайт, веб-ресурсы интернет-банкинга и веб-приложения информационных систем АБС);

5) использование защищённых соединений на основе протокола TLS при подключении мобильных клиентов к системе мобильного банкинга Банка посредством мобильных приложений;

6) использование защищённых соединений SSH при удалённом подключении администраторов с рабочих станций через корпоративную сеть Банка и VPN-шлюз к сетевому и серверному оборудованию, размещённому в основном и резервном центрах обработки данных.

9.3. Требования к организации защищённых сетевых соединений в корпоративной сети определяются Положением об организации корпоративной сети и защищённых сетевых соединений, приведённым в Приложении 1 к настоящей Политике.

9.4. В Банке доступ работников к сети Интернет организуется через интернет-шлюз Банка, установленный на границе подключения Головного офиса (основного центра обработки данных) к внешней сети Интернет.

9.5. В пункте обслуживания Головного офиса организуются гостевые сети Wi-Fi для посетителей Банка с целью предоставления доступа к сети Интернет.

Кроме того, сети Wi-Fi организуются для работников Головного офиса и ИТ-офиса.

Указанные сети Wi-Fi в Банке должны соответствовать следующим требованиям:

- отсутствие физического подключения сетей Wi-Fi к локальным сетям Головного офиса, ИТ-офиса, торговых офисов и корпоративной сети Банка;
- использование отдельного подключения к сети Интернет через локального провайдера для сетей Wi-Fi;
- подключение сетей Wi-Fi к сети Интернет через отдельно выделенный межсетевой экран с обязательной авторизацией пользователей по логину и паролю.
-

10. РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ

10.1. Для создания и поддержания режима информационной безопасности необходимо чётко документировать ответственность за обеспечение информационной безопасности отдельных ресурсов Банка, а также за реализацию соответствующих процедур защиты информации, направленных на обеспечение непрерывности деятельности и восстановление функционирования Банка.

10.2. Ответственность за распределение ресурсов и реализацию процедур информационной безопасности возлагается на руководство Банка и Управление информационной безопасности.

Основными обязанностями руководства Банка в области обеспечения информационной безопасности являются:

1) определение целей и принципов обеспечения информационной безопасности, соответствующих требованиям Банка;

2) определение и изменение организационной структуры управления информационной безопасностью Банка;

3) распределение функций и назначение лиц, ответственных за обеспечение информационной безопасности;

4) распределение и выделение ресурсов, необходимых для обеспечения информационной безопасности Банка;

5) координация и поддержка инициатив структурных подразделений и работников Банка в области обеспечения информационной безопасности;

6) утверждение проектов в области информационной безопасности Банка;

7) обеспечение включения требований информационной безопасности во все проекты Банка;

8) оценка целесообразности и координация реализации конкретных мер по управлению информационной безопасностью для новых систем и сервисов Банка;

9) анализ результатов расследования инцидентов информационной безопасности и принятие решений о привлечении виновных лиц к ответственности;

10) поддержка и стимулирование работников, способствующих повышению эффективности обеспечения информационной безопасности, а также выполнение иных функций в данной области.

10.3. Непосредственная организация и обеспечение эффективного функционирования системы менеджмента информационной безопасности возлагаются на Управление информационной безопасности.

Функции и обязанности Управления информационной безопасности определяются Положением об Управлении информационной безопасности, приведённым в приложении к настоящей Политике.

10.4. В процессах обеспечения информационной безопасности участвуют:

- Управление общей безопасности, ответственное за обеспечение физической безопасности в Банке;
- Департамент информационных технологий, обеспечивающий эксплуатацию, техническое обслуживание программного обеспечения и аппаратно-программных средств объектов информатизации Банка.

10.5. Для обеспечения обслуживания, технической поддержки и непрерывного функционирования объектов информатизации Банка за каждым объектом информатизации закрепляются ответственные работники Департамента информационных технологий, осуществляющие сопровождение и развитие соответствующего программного обеспечения.

10.6. Настоящая Политика устанавливает следующее распределение ответственности за обеспечение информационной безопасности в Банке:

1) начальник Управления информационной безопасности несёт ответственность за организацию и реализацию всех мероприятий по обеспечению информационной безопасности в Банке;

2) начальник Управления общей безопасности несёт ответственность за обеспечение физической защиты зданий, помещений и материальных ценностей Головного офиса и торговых офисов Банка;

3) директор Департамента информационных технологий и работники подразделений Департамента информационных технологий, ответственные за обеспечение непрерывного и штатного функционирования объектов информатизации Банка, включая локальные сети, корпоративную сеть, внешние каналы связи, информационные ресурсы и информационные системы Банка, несут ответственность за обслуживание, техническую поддержку и обеспечение непрерывного функционирования указанных объектов информатизации;

4) работники Банка, а также владельцы информационных активов Банка несут персональную ответственность за нарушение конфиденциальности защищаемой информации в любой форме;

5) работники Банка несут ответственность за действия, совершаемые в информационных системах Банка, в пределах предоставленных им ролей, полномочий и должностных обязанностей;

6) за обеспечение информационной безопасности (включая физическую безопасность) рабочей станции, иных терминальных устройств и носителей информации несёт ответственность работник Банка, которому указанные средства предоставлены для выполнения служебных обязанностей;

7) руководители структурных подразделений Головного офиса Банка, руководители торговых офисов, а также ответственные лица Хозяйственного управления Банка несут ответственность за соблюдение требований пожарной и технической безопасности, а также за сохранность оборудования в пределах соответствующих зданий и помещений.

10.7. В Банке определены следующие ответственные работники:

1) Администратор корпоративной сети Банка, являющийся работником Департамента информационных технологий, в обязанности которого входят:

- обеспечение штатного и непрерывного функционирования сетевого оборудования корпоративной сети;
- организация защищённых сетевых соединений в корпоративной сети;
- управление сетевым трафиком, сетевыми соединениями и доступом к информационным системам и информационным ресурсам из корпоративной и внешних сетей.

2) Системный администратор локальной сети Банка, являющийся работником Департамента информационных технологий, в обязанности которого входят:

- обеспечение функционирования сервера контроллера домена;
- управление учётными записями работников и их доступом к информационным системам и информационным ресурсам Банка.

3) Администраторы информационных систем Банка, являющиеся работниками Департамента информационных технологий, в обязанности которых входят:

– настройка и администрирование серверов информационных систем, контроль их функционирования, просмотр и изменение параметров серверных систем хранения и систем хранения данных;

– настройка системного и прикладного программного обеспечения информационных систем и мониторинг его функционирования;

– проверка параметров и конфигураций серверных систем хранения и систем хранения данных, а также журналов их работы и сбоев;

– выполнение резервного копирования и восстановления серверов информационных систем.

4) Администраторы баз данных Банка, являющиеся работниками Департамента информационных технологий, в обязанности которых входят:

– администрирование систем управления базами данных;

– внесение изменений в структуру баз данных;

– проверка баз данных с использованием средств контроля целостности данных;

– выполнение резервного копирования и восстановления данных информационных систем.

Ответственность, указанная в настоящем пункте, закрепляется в должностных инструкциях работников и иных внутренних нормативных документах Банка.

В случае отсутствия ответственного работника (отпуск, временная нетрудоспособность, служебная командировка и иные причины) его обязанности выполняются работником, назначенным в установленном порядке.

Такому работнику предоставляются соответствующие права доступа, и он несёт ответственность за надлежащее исполнение возложенных на него обязанностей.

10.8. В целях разграничения функций и обязанностей:

1) определяется перечень лиц, имеющих право физического и логического доступа к оборудованию Банка и средствам защиты информации, объектам защиты, включая конфиденциальную информацию, центры обработки данных, серверные помещения и иные помещения с высоким уровнем безопасности (зона 3), локальные и корпоративные сети, АБС, а также другие информационные системы и информационные ресурсы Банка;

2) перечень мобильных устройств, носителей информации и устройств хранения данных закрепляется за работниками Банка соответствующими организационно-распорядительными документами;

3) Управление информационной безопасности Банка осуществляет контроль за выполнением обязанностей, возложенных на лиц, ответственных за обеспечение информационной безопасности.

10.9. Работники Банка обязаны ознакомиться с Политикой информационной безопасности Банка после её утверждения либо пересмотра под подпись в Журнале ознакомления с Политикой информационной безопасности Банка, форма которого приведена в Приложении 16 к настоящей Политике.

Ознакомление работников Банка с требованиями Политики информационной безопасности и их обучение осуществляются в соответствии с пунктом 7.4.4 настоящей Политики.

11. ПОРЯДОК ПЕРЕСМОТРА И АКТУАЛИЗАЦИИ ПОЛИТИКИ

11.1. Управление информационной безопасности осуществляет оценку актуальности и эффективности положений и требований Политики информационной безопасности по следующим направлениям:

- соответствие Политики информационной безопасности действующей организационно-технологической и информационной инфраструктуре Банка, а также перспективам её дальнейшего развития;
- соответствие Политики информационной безопасности требованиям действующих нормативных документов;
- достаточность и обоснованность требований, установленных Политикой информационной безопасности;
- эффективность методов и средств защиты информации, предусмотренных Политикой информационной безопасности.

11.2. Оценка актуальности и эффективности Политики информационной безопасности Банка проводится Управлением информационной безопасности на регулярной основе не реже одного раза в год.

Оценка актуальности и эффективности Политики информационной безопасности Банка может осуществляться путём проведения внутреннего или внешнего аудита на предмет соответствия информационной инфраструктуры Банка требованиям и положениям утверждённой Политики.

По результатам оценки актуальности и эффективности Политики информационной безопасности могут подготавливаться предложения по внесению изменений и дополнений в Политику либо по её пересмотру.

Предложения о внесении изменений и дополнений в настоящую Политику либо о её пересмотре подготавливаются Управлением информационной безопасности, согласовываются с заинтересованными структурными подразделениями Банка и утверждаются Наблюдательным советом Банка.

11.3. Предложения о внесении изменений и дополнений в Политику информационной безопасности Банка либо о её пересмотре должны подготавливаться в следующих случаях:

- при выявлении несоответствий между положениями и требованиями Политики информационной безопасности и организационной, технологической либо информационной инфраструктурой Банка;
- если отдельные положения и требования Политики информационной безопасности противоречат новым либо изменённым законодательным и иным нормативно-правовым актам;

– при выявлении недостаточности или неэффективности требований, методов и средств защиты информации, предусмотренных Политикой информационной безопасности;

– при необходимости совершенствования Политики информационной безопасности и подходов к управлению информационной безопасностью в Банке;

– при проведении реорганизации или реструктуризации Банка;

– при изменении структуры и состава системы менеджмента информационной безопасности;

– при реконструкции и модернизации информационно-коммуникационной инфраструктуры;

– при изменении бизнес-процессов, технологических процессов и в иных аналогичных случаях.

11.4. Внесение изменений и дополнений в Политику информационной безопасности Банка либо её пересмотр осуществляются в целях:

– совершенствования подходов к управлению информационной безопасностью и соответствующими процессами;

– совершенствования мер и средств контроля, управления и обеспечения информационной безопасности, а также целей их применения;

– совершенствования распределения ресурсов и (или) обязанностей, а также повышения уровня ответственности;

– снижения угроз информационной безопасности для Банка.

12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

12.1. В случае если отдельные положения Политики информационной безопасности вступят в противоречие с законодательством и нормативными документами вследствие принятия новых нормативно-правовых актов либо внесения изменений в действующие нормативно-правовые акты, такие положения утрачивают юридическую силу до момента внесения соответствующих изменений и дополнений в настоящую Политику информационной безопасности.

Если вновь принятые или изменённые нормативно-правовые акты противоречат положениям настоящей Политики, до внесения соответствующих изменений Банк руководствуется требованиями действующего законодательства.

Во всех вопросах, не урегулированных настоящей Политикой, Банк руководствуется действующим законодательством Республики Узбекистан.

12.2. С момента утверждения настоящей Политики информационной безопасности АО «ANOR BANK» считать утратившим силу аналогичный документ, утверждённый Наблюдательным советом Банка (Протокол № 5 от 10 февраля 2022 года).

Разработано: Согласовано:	Начальник Управления информационной безопасности	ПОДПИСЬ	А.А.Абдурахманов
	Председатель Правления	ПОДПИСЬ	Ш.С.Акрамов
	Первый заместитель Председателя Правления	ПОДПИСЬ	Э. Наджимитдинов
	Заместитель Председателя Правления	ПОДПИСЬ	Э.Р.Кадиров
	Заместитель Председателя Правления	ПОДПИСЬ	А.Р.Сайдуллаев
	Заместитель Председателя Правления	ПОДПИСЬ	С.Д.Хан
	Заместитель Председателя Правления	ПОДПИСЬ	М.Д.Нуритдинова
	Управляющий директор	ПОДПИСЬ	А.А.Бакиев
	Главный бухгалтер	ПОДПИСЬ	У.М.Бабаев
	Начальник Юридического управления	ПОДПИСЬ	Т.Ф. Занахов
	Директор Департамента риск-менеджмента	ПОДПИСЬ	Д.А.Ибрагимова
	Директор Департамента внутреннего аудита	ПОДПИСЬ	С.А.Усманов
	Директор Департамента внутреннего контроля	ПОДПИСЬ	М.Т Пулатова
	Исполняющий обязанности директора Департамента управления персоналом	ПОДПИСЬ	А.С.Илхомжонов

	Начальник Управления комплаенс-контроля	ПОДПИСЬ	Д.И.Хушназаров
	Начальник Управления общей безопасности	ПОДПИСЬ	М.И.Норкин