ВНУТРЕННИЙ ДОКУМЕНТ	
Наименование:	Политика информационной безопасности АО «Фридом Банк Казахстан»
Владелец:	Департамент информационной безопасности
Утвержден:	Решением Совета Директоров Банка (Протокол СД Банка №03-29(з) от 29.03.2024г., рег. №А0-23-04/16/ПТ/29032024 (27.02.2025))
Срок введения в действие:	С даты утверждения
Внесение последних изменений/дополнений	Изменения и дополнения в Политику ИБ АО «Фридом Банк Казахстан», утвержденные решением СД №03-31(з) от 31.03.2025г., СД №07-22(з) от 22.07.2026г.
Отмененные/признанные утратившими силу документы (при наличии):	
Степень конфиденциальности:	***общедоступная***

РЕЕСТР
утвержденных изменений и дополнений в
Политику информационной безопасности

№	Номер документа	Реквизиты решения Органа Банка об утверждении изменений и дополнений	Срок введения в действие утвержденных изменений и дополнений	Основание внесения изменений/дополнений
1	№А0-23-04/16/ПТ/29032024 (27.02.2025)	Решение СД №03-31(з) от 31.03.2025г.	С даты утверждения	В связи с новыми требованиями Комиссии по ценным бумагам и биржам США по кибербезопасности ИБ Холдинга, а также уточнений в части используемых международных стандартов и приведения в соответствие с требованиями Банка по оформлению документа.
2	№А0-23-04/16/ПТ/29032024 (27.02.2025)	Решение СД №07-22(з) от 22.07.2026г.	С даты утверждения	Изменения в целях актуализации нормативной базы в связи с Постановлением Правления АРРФР №53 от 3 апреля 2026г, а таже изменение функций КИБ.
4				
5				
6				

Содержание

Глава 1. Общие положения

1. Политика информационной безопасности (далее – Политика) АО «Фридом Банк Казахстан» (далее – Банк) разработана с целью определения стратегических целей, задач и основных требований к комплексу мер в области информационной безопасности, обеспечению устойчивости функционирования информационных систем и сохранности информации, обеспечению всесторонней защиты интересов Банка от угроз в сфере информационных технологий.

2. Политика определяет основные требования и позицию Банка в сфере сохранности и неразглашении защищаемой информации в Головном офисе и филиалах Банка в любом виде: устно, письменно, на физических носителях информации, а также данных, передаваемых посредством глобальных и локальных сетей.

3. Политика разработана в соответствии с законодательством Республики Казахстан, Постановлением Правления *Агентства Республики Казахстан по регулированию и развитию финансового рынка от 3 апреля 2026 года № 53 «Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций» (далее – Постановление), требованиями законодательства Республики Казахстан в сфере обеспечения кибербезопасности, Политикой информационной безопасности Freedom Holding Corp, международными стандартами ISO/IEC 27001:2022 и PCI DSS (Payment Card Industry Data Security Standard).*

Глава 2. Понятия, используемые в Политике

4. В Политике используются следующие понятия:

1) **Автоматизированная система** – система, представляющая собой организационно упорядоченную совокупность данных (массивов документов), технических и программных средств, реализующих информационные технологические процессы;

2) **Аутентификация** – подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа в системе;

2-1) ***Внутренний документ (далее - ВД) -*** *это документ на электронном (бумажном) носителе, разработанный, утвержденный и зарегистрированный в Банке для организации работы и регламентации/регулирования внутренней(-их) деятельности/процессов Банка, а также устанавливающий, изменяющий и/или прекращающий обязательные для подразделений и работников Банка требования или порядок действий/мероприятий при выполнении функций, взаимодействий, рабочих процессов, в том числе требующих согласованного участия подразделений/работников*;

3) **Департамент информационной безопасности** (далее – ДИБ) – СП Банка, обеспечивающее контроль за состоянием защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

4) **Идентификация** – присвоение или определение соответствия предъявленного для получения доступа в систему и/или к ресурсу системы идентификатора перечню идентификаторов, имеющихся в системе;

5) **Информационная безопасность** (далее – ИБ) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

6) **Информационная система** (далее – ИС) – система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса;

7) **Информационно-коммуникационная инфраструктура** (далее – информационная инфраструктура) – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

8) **Информационные ресурсы** – отдельные документы и отдельные массивы документов, данные и массивы информации в информационных системах (библиотеках, архивах, фондах, базах данных);

9) **Информация** – упорядоченная последовательность знаков, символов, цифр звуковых сигналов, других данных, закрепленных на различных носителях информации и носящих определенный смысл;

10) **Комитет по информационной безопасности** (далее – КИБ) – коллегиальный орган Банка, возглавляемый Председателем Правления и уполномоченный принимать решения по задачам обеспечения ИБ Банка, *состав и функции которого определены Положением о КИБ*;

11) **Несанкционированный доступ** – доступ к защищаемой информации лицами, не имеющими прав на доступ к этой информации;

12) **Подразделения, отвечающие за информационные технологии** (далее – ПИТ**)** – подразделение (-ия) Банка, ответственное (-ые) за функционирование, развитие, разработку и внедрение информационных технологий Банка, а также за своевременное выявление, оценку и управление рисками, как первая линия защиты;

13) **Привилегированная учетная запись** – учетная запись в информационной системе, обладающая привилегиями создания, удаления и изменения прав доступа учетных записей;

14) **Система управления информационной безопасностью** (далее – СУИБ) – часть общей системы управления Банка, которая создает, реализует, использует, осуществляет мониторинг, ревизию, сопровождение и совершенствование информационной безопасности и включает в себя совокупность ВД Банка, организационных мероприятий работников Банка в соответствии с возложенными на них должностными обязанностями, технологических, технических методов и средств, разрабатываемых, внедряемых и действующих по всем направлениям защиты информации;

15) **СП** – структурное подразделение;

16) **ОС** –операционная система;

17) **СУБД** –система управления базами данных.

Глава 3. Цели, задачи и основные принципы построения СУИБ

5. Основной целью СУИБ является обеспечение устойчивого функционирования ИС Банка путем предотвращения реализации угроз безопасности ИС, недопущение разглашения, утраты, утечки, искажения и уничтожения защищаемой информации, а также исключение угрозы негативного воздействия на репутацию Банка.

6. В настоящей Политике раскрываются основные виды угроз ИБ Банка, объекты корпоративной ИС Банка, на которые направлены данные угрозы, а также требования к мерам защиты от угроз.

7. Основные концептуальные задачи по реализации требований настоящей Политики:

1) планирование, реализация и контроль за выполнением комплекса организационных и технических мер по обеспечению ИБ на основе оценки рисков Банка в сфере информационных технологий, направленных на обеспечение:

– непрерывной доступности информационных активов Банка для поддержки его бизнес-процессов;

– целостности информационных активов Банка в целях поддержки высокого качества бизнес-процессов;

– конфиденциальности информации Банка и иных сторон;

– соответствия предпринимаемых мер по ИБ, применяемых в Банке, требованиям законодательства, а также требованиям регулирующих и надзорных органов Республики Казахстан;

2) совершенствование СУИБ как неотъемлемой части общей системы управления Банка, включая:

– совершенствование организационной структуры Банка в соответствии с требованиями регулирующих и надзорных органов Республики Казахстан;

– совершенствование процессов СУИБ, обеспечивающих реализацию выбранного комплекса мер по обеспечению ИБ;

– обеспечение со стороны руководства Банка контроля, оценки результатов и эффективности процессов СУИБ и предпринимаемых в рамках этих процессов мер по обеспечению ИБ, а также их соответствия установленным требованиям настоящей Политики, регулирующих и надзорных органов и действующего законодательства Республики Казахстан;

3) документирование требований по ИБ с учетом выбранного комплекса организационных и технических мер;

4) обеспечение осведомленности работников о политике Банка в области ИБ, предпринимаемых мерах и требованиях по обеспечению ИБ, обязанностях и правилах поведения, возлагаемых на работников, а также обеспечение контроля за их надлежащим выполнением;

5) обеспечение соблюдения требований законодательства Республики Казахстан в ходе деятельности по обеспечению ИБ Банка.

8. В основу настоящей Политики заложены следующие базовые принципы:

1) своевременность обнаружения неблагоприятных факторов, влияющих на цели Банка – СУИБ направлена на быстрое выявление, анализ и прогноз развития угроз в информационных технологиях, способных негативно повлиять на стабильность и надежность работы Банка;

2) оценка влияния неблагоприятных факторов на цели – любые возникающие или прогнозируемые угрозы в информационных технологиях оцениваются в части их влияния на цели и успешность выполнения бизнес-процессов Банка и отражаются в оценке рисков Банка;

3) приоритетность – требования по ИБ имеют приоритет перед любыми иными требованиями, предъявляемыми к ИС и активам Банка;

4) адекватность – меры организационного и технического характера должны соответствовать рискам – затраты на реализацию этих мер должны быть адекватны прогнозируемому ущербу от реализации угроз в информационных технологиях;

5) определенность целей – при планировании мер устанавливаются четкие и достижимые цели. При документировании требований указываются четкие и ясные цели, которые Банк стремится достичь при выполнении этих требований;

6) результативность – любые меры по ИБ должны планироваться с учетом результата,

который Банк стремится достичь при реализации соответствующих мер;

7) использование опыта и лучших практик – деятельность по обеспечению ИБ должна выполняться с учетом накапливаемого и анализируемого опыта, как Банка, так и других организаций, а также с учетом рекомендаций международных стандартов и лучших мировых практик;

8) непрерывность – деятельность по обеспечению ИБ Банка строится на непрерывной основе как постоянно совершенствующийся процесс, в основе которого лежит СУИБ, охватывающая все бизнес-процессы, все уровни управления и всех работников Банка;

9) контролируемость и эффективность мер – любые меры контролируются руководством Банка на предмет их соответствия оцениваемым рискам, полноты и качества реализации. Банком оценивается эффективность мер исходя из степени достижения поставленных целей и результатов;

10) законность – предполагает осуществление защитных мероприятий и разработку СУИБ Банка в соответствии с законодательством Республики Казахстан;

11) системность – системный подход к построению СУИБ и учету всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации;

12) комплексность – комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита строится эшелонировано;

13) мотивация персонала – руководство и работники Банка должны иметь надлежащий уровень мотивации к выполнению установленных требований и достижению целей обеспечения информационной безопасности;

14) риск-ориентированный подход – основные решения в области ИБ принимаются на основании анализа актуальных рисков, их потенциального воздействия на бизнес-процессы, а также в соответствии с допустимыми уровнями риска для Банка;

15) минимизация полномочий – каждому работнику предоставляются только те права и полномочия, которые необходимы для выполнения его должностных обязанностей, с целью предотвращения избыточного доступа к информационным ресурсам;

16) разделение обязанностей – ни одному пользователю не должно быть предоставлено достаточно прав, чтобы он мог скомпрометировать информационную систему или критически важные бизнес-операции самостоятельно;

17) корпоративная ответственность – все работники Банка несут ответственность за обеспечение ИБ в пределах своих должностных обязанностей и прилагают разумные усилия для предотвращения предсказуемых инцидентов и угроз;

18) безопасная архитектура – принципы ИБ учитываются на всех этапах проектирования бизнес-процессов, информационных систем и инфраструктуры, что позволяет минимизировать потенциальные уязвимости еще на этапе их создания;

19) осведомленность и обучение – все участники СУИБ осведомлены о своих обязанностях в области информационной безопасности и проходят регулярное обучение по актуальным угрозам, методам защиты и внутренним регламентам.

Глава 4. Область действия и участники СУИБ

9. Областью действия СУИБ являются все бизнес-процессы Банка по всем клиентским, финансовым услугам по сети Интернет, почте, доступу пользователей к информационным ресурсам Банка.

10. Область действия СУИБ охватывает все СП Банка.

11. В область действия СУИБ входят все информационные активы, включая конфиденциальную и открытую (общедоступную) информацию, принадлежащие и (или) обрабатываемые Банком информационные ресурсы, аппаратно-программные средства, сетевое обеспечение, носители информации, офисы Банка, основные СП Банка, обеспечивающие работу Банка, клирингового обслуживания и предоставления сервисов юридическим и физическим лицам.

12. Основными объектами СУИБ Банка, подлежащими защите, являются:

1) информационные активы, необходимые для работы Банка независимо от формы и вида их представления;

2) элементы ИТ-инфраструктуры, включая технические и программные средства формирования, обработки, передачи, хранения и использования информации, в том числе библиотеки, архивы, базы данных, каналы информационного обмена и телекоммуникации, ИС и средства защиты информации, объекты и помещения, в которых размещены защищаемые элементы ИТ-инфраструктуры Банка;

3) процессы, регламенты и процедуры обработки информации в Банке.

13. Субъектами СУИБ являются работники Банка.

14. Участниками СУИБ Банка являются:

1) Совет директоров Банка;
2) Правление Банка;
3) КИБ;
4) ДИБ;
5) ПИТ;
6) Департамент безопасности;
7) Департамент HR;
8) Юридический департамент;
9) Департамент комплаенс-контроля;
10) Департамент внутреннего аудита;
11) Департамент операционных, ИТ/ИБ рисков и внутреннего контроля;
12) Владельцы бизнес-процессов и ИС.

15. Совет директоров Банка при формировании бюджета учитывает потребности в ресурсах для обеспечения ИБ Банка.

16. Совет директоров Банка утверждает *Политику ИБ Банка*, перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну, и порядок работы с защищаемой информацией.

17. Правление Банка утверждает ВД, регламентирующие процесс управления ИБ.

Глава 5. Распределение ролей и ответственности по обеспечению ИБ

18. Необходимое для реализации целей ИБ качество руководства и управления деятельностью по обеспечению ИБ в Банке обеспечивается эффективной организацией СУИБ и распределением ролей и ответственности за выполнение процессов и мер по обеспечению ИБ или отдельных задач.

19. В рамках СУИБ создается процессно-ориентированная организационная структура, описанная в пункте 14 настоящей Политики, обеспечивающая выполнение всех процессов СУИБ и способствующая:

1) скоординированному участию в решении вопросов, относящихся к области ИБ, всех СП Банка, а также сторонних организаций и лиц, заинтересованных в обеспечении ИБ в Банке;

2) обеспечению требуемой и своевременной информированности руководства Банка по вопросам ИБ, четкой организации процессов принятия, исполнения и контроля связанных с ними решений.

20. В целях эффективного руководства, управления и обеспечения ИБ в Банке определены и оптимальным образом распределены роли и ответственность.

21. При распределении ролей и ответственности исключается возможность существования процессов и мер в рамках СУИБ, не поддерживаемых ни одной ролью и лежащих вне чьей-либо области ответственности.

22. В рамках настоящей Политики определяются ключевые роли в рамках СУИБ в Банке. Детализированное определение ролей и ответственности устанавливается в положениях о СП Банка, должностных инструкциях работников и иных документах Банка.

5.1 КИБ

23. КИБ выполняет следующие функции:

1) обеспечение формирования и развития политики поддержки информационной безопасности Банка и СУИБ Банка при внедрении новых методов обеспечения ИБ;

2) рассмотрение отчетов по результатам внутренних и внешних сканирований с отражением уязвимостей, не устраненных в срок (с указанием причин неустранения);

3) рассмотрение ежегодного отчета о состоянии СУИБ Банка;

4) рассмотрение результатов анализа инцидентов ИБ за прошедший год;

5) рассмотрение других вопросов, относящихся к реализации мер по обеспечению ИБ.

5.2 Председатель Правления Банка

24. Председатель Правления Банка обеспечивает создание, функционирование и улучшение СУИБ, являющейся частью общей системы управления Банка, предназначенной для управления процессом обеспечения ИБ.

5.3 ДИБ

25. ДИБ в целях обеспечения конфиденциальности, целостности и доступности информации Банка осуществляет следующие функции:

1) организует СУИБ, осуществляет координацию и контроль деятельности СП Банка по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ;

2) разрабатывает политику ИБ Банка, в том числе при необходимости вносит изменения *в нее*;

3) обеспечивает методологическую поддержку процесса обеспечения ИБ Банка;

4) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля ИБ Банка в рамках своих полномочий;

5) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах ИБ;

6) осуществляет анализ информации об инцидентах ИБ;

7) подготавливает предложения для принятия *КИБ решений* по вопросам ИБ;

8) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения ИБ Банка, а также предоставление доступа к ним;

9) организация, координация и контроль мероприятий по осуществлению технической защиты информации ограниченного доступа;

10) разрабатывает предложения по совершенствованию системы защиты информации, *включая персональные данные*;

11) анализ результатов внешних проверок, подготовка планов мероприятий по устранению нарушений, выявленных в ходе проверок, контроль их реализации;

12) решение задач по недопущению либо существенному затруднению неправомерных (в том числе преднамеренных) технических, программных и иных воздействий и процессов, направленных на считывание (хищении) информации, на разрушение, искажение или блокирование в процессе ее обработки на объектах информатизации;

13) организует и проводит мероприятия по обеспечению осведомленности работников Банка в вопросах ИБ;

14) осуществляет мониторинг состояния СУИБ Банка;

15) осуществляет информирование руководства Банка о состоянии СУИБ Банка;

16) определяет требования ИБ по использованию привилегированных учетных записей;

17) осуществляет проведение оценки рисков ИБ;

18) разрабатывает меры по обработке рисков ИБ и предоставление отчетности по их реализации в Департамент операционных, ИТ/ИБ рисков и внутреннего контроля;

19) осуществляет подготовку и предоставление отчетности о реализации существенных рисков ИБ в Департамент операционных, ИТ/ИБ рисков и внутреннего контроля, а также об устранении их последствий;

20) разрабатывает план мероприятий по реализации стратегии Банка в части обеспечения ИБ, который раскрывает, но, не ограничиваясь, следующее:

a. определение потребностей в ресурсах, в том числе определение бюджета, связанного с реализацией мер, направленных на управление рисками ИБ;

b. описание требуемых мероприятий в области ИБ с указанием сроков и ответственных исполнителей за их реализацию.

26. Директор ДИБ:

1) организовывает СУИБ в Банке;

2) возглавляет и контролирует все процессы, связанные с обеспечением ИБ Банка;

3) несет ответственность за достижение поставленных руководством Банка целей и задач по обеспечению ИБ;

4) обеспечивает взаимодействие со СП Банка по вопросам обеспечения ИБ Банка;

5) координирует и контролирует СП Банка по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ;

6) разрабатывает планы работ в рамках процессов СУИБ, в том числе архитектуры ИБ Банка;

7) организует процесс выявления возможных каналов утечки информации;

8) организует процесс создания моделей угроз и определения методов защиты по направлению ИБ;

9) информирует руководство Банка о состоянии СУИБ Банка;

10) *организует процесс внедрения и администрирования инструментов ИБ*;

11) ответственен за проведение аудита СП на соответствие требованиям СУИБ.

27. Работники ДИБ отвечают за:

1) организацию и методическое руководство работами по управлению рисками ИБ, классификацию информационных активов, ИС;

2) оценку соответствия разрабатываемых, закупаемых и эксплуатируемых *ИС Банка* требованиям ИБ, разработку предложений по способам реализации требований;

3) контроль выполнения требований по ИБ при проведении изменений систем и их релизов;

4) разработку требований к функциональным возможностям и настройкам сервисов безопасности *ИС* и предложений по способам реализации требований;

5) разработку требований к процессу управления доступом (предоставление, изменение полномочий, лишение) к ИС и ресурсам Банка пользователей, персонала внедрения и поддержки систем;

6) мониторинг состояния ИБ эксплуатируемых приложений, сети, ОС и СУБД;

7) внедрение мер повышения осведомленности по вопросам ИБ;

8) управление и контроль за решением инцидентов по ИБ;

9) мониторинг исполнения требований по ИБ при обеспечении непрерывности критичных бизнес-процессов в условиях чрезвычайных ситуаций;

10) контроль включения в договора с поставщиками ИТ услуг требований по ИБ, мониторинг выполнения требований по ИБ организациями-поставщиками ИТ-услуг по поддержке ИС;

11) защиту критичных информационных активов, *включая персональные данные*;

12) мониторинг и оценку эффективности мер ИБ, определенных законодательством Республики Казахстан;

13) внедрение и контроль исполнения мер и средств обеспечения ИБ;

14) мониторинг исполнения порядка обращения с защищаемой информацией Банка (доступа, передачи, хранения, предоставления уполномоченным органам);

15) внедрение мер и средств *контроля* управления доступом работников Банка, а также работников внешних организаций к местам размещения ИТ и обеспечивающей инфраструктуры;

16) проведение служебных проверок по фактам нарушений установленных требований по ИБ, организация взаимодействия с правоохранительными органами при проведении таких проверок.

28. Следующие ключевые направления ИБ управляются централизованно работниками ДИБ:

1) внедрение средств мониторинга состояния ИБ сети Банка, элементов инфраструктуры (СУБД, ОС), поддерживающих критичные приложения, а также мониторинг и оценку состояния ИБ сети Банка, СУБД, ОС - компонент критичных систем;

2) разработку единых требований по ИБ к разрабатываемым (закупаемым) и эксплуатируемым системам и их компонентам (ОС, СУБД), компонентам информационной инфраструктуры;

3) мониторинг и оценка состояния ИБ при подготовке и проведении релизов обновления систем, определение требований к функциональным возможностям и настройкам сервисов безопасности указанных систем и предложений по способам реализации требований;

4) *исключен решением СД №07-22 (з) от 22.07.2026г*.

29. Работники ДИБ *участвуют в процессе* восстановления ИТ-сервисов Банка при авариях и катастрофах и *взаимодействуют* с другими СП Банка в части оценки угроз ИТ-сервисам, формирования требований по восстановлению ИТ-сервисов и планирования, реализации и поддержки процессов и мер по их восстановлению.

5.4 ПИТ

30. ПИТ осуществляет следующие функции:

1) разрабатывает и поддерживает актуальность схемы информационной инфраструктуры Банка;

2) обеспечивает предоставление доступа пользователям к информационным активам Банка, за исключением специализированных информационных активов, доступ к которым предоставляется ИТ-менеджерами ИС, не относящимися к ПИТ;

3) обеспечивает формирование типовых настроек и конфигурирование системного и прикладного программного обеспечения Банка с учетом требований ИБ;

4) обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности данных ИС Банка (включая резервирование и (или) архивирование и резервное копирование информации) в соответствии с ВД Банка;

5) обеспечивает соблюдение требований ИБ при выборе, внедрении, разработке и тестировании ИС.

31. ПИТ, осуществляющий внедрение и разработку требований к закупке новых и доработке существующих ИС, отвечает за:

1) согласование с ДИБ заданий на разработку (проектирование) ИС, отступлений от установленных в Банке требований по ИБ;

2) разделение продуктивных, тестовых сред и сред разработки;

3) разделение обязанностей персонала разработки и тестирования ИС;

4) устранение выявленных в ходе тестирования уязвимостей по ИБ в ИС.

32. ПИТ, в обязанности которого входит мониторинг и эксплуатация ИС, отвечает за:

1) согласование с ДИБ и контроль выполнения требований к безопасной эксплуатации ИС, настройкам сервисов ИБ (идентификации и аутентификации, управления доступом, протоколирования, шифрования, туннелирования), своевременное устранение выявленных уязвимостей по ИБ;

2) отделение продуктивных сред от тестовых и сред разработки, разделение обязанностей персонала внедрения и поддержки систем (продуктов) и минимизацию полномочий по доступу к системам персонала, осуществляющего их поддержку;

3) внедрение и поддержку средств защиты от вредоносного ПО и спама;

4) управление доступом *пользователей и администраторов* к информационным ресурсам Банка ;

5) доведение до ДИБ, решение инцидентов по *ИТ*/ИБ, устранение причин их возникновения *совместно с ДИБ*;

6) определение в договорах с поставщиками ИТ-услуг, согласованных *в соответствии с ВД* Банка, требований, определяющих необходимые меры ИБ и обязательства сторон по ИБ;

7) выполнение требований по ИБ, определенных законодательством Республики Казахстан и *ВД Банка*;

8) внедрение согласованных с ДИБ мер защиты от прерывания основных бизнес-процессов в условиях чрезвычайных ситуаций, влияющих на критичные объекты информационной и технологической инфраструктуры.

5.5 Департамент безопасности

33. Департамент безопасности осуществляет следующие функции:

1) реализует меры физической и технической безопасности в Банке, в том числе организует пропускной и внутриобъектовый режимы;

2) проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз ИБ при приеме на работу и увольнении работников Банка;

3) контроль и мониторинг обеспечения пожарной безопасности и техники безопасности;

4) прогнозирует, предупреждает, выявляет, пресекает внутренние и внешние угрозы финансовым, информационным и материальным ресурсам Банка, а также причин и условий, способствующих их возникновению;

5) выявляет возможные каналы утечки конфиденциальной информации Банка, составляющую коммерческую, служебную и банковскую тайну.

5.6 Департамент HR

34. Департамент HR осуществляет следующие функции:

1) обеспечивает подписание работниками Банка, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами Обязательства о соблюдении требований ИБ и Соглашения о неразглашении конфиденциальной информации;

2) участвует в организации процесса повышения осведомленности работников Банка в области ИБ;

3) уведомляет уполномоченный орган по регулированию и развитию финансового рынка о назначении и увольнении работников ДИБ в течение трех рабочих дней;

4) проводит совместно с ДИБ обучение и тренинги работников в области ИБ, ежегодную проверку знаний и навыков работников Банка.

5.7 Юридический департамент

35. Юридический департамент:

1) осуществляет правовую экспертизу ВД Банка по вопросам обеспечения ИБ;

2) оказывает юридическую поддержку ДИБ при разбирательствах с инцидентами ИБ;

3) совместно с Департаментом комплаенс-контроля определяет виды информации, подлежащие включению в перечень защищаемой информации.

5.8 Департамент комплаенс-контроля

36. Департамент комплаенс-контроля совместно с Юридическим департаментом определяет виды информации, подлежащие включению в перечень защищаемой информации.

5.9 Департамент внутреннего аудита

37. Департамент внутреннего аудита в соответствии с установленными процедурами при соответствующем поручении и/или одобрении Совета директоров Банка предоставляет достоверную, объективную и независимую оценку соответствия реализуемых процессов и мер по обеспечению ИБ требованиям, отраженным во ВД Банка по ИБ.

38. В задачи Департамента внутреннего аудита входит планирование и проведение оценки состояния СУИБ Банка в соответствии с ВД Банка, регламентирующими организацию системы внутреннего аудита Банка.

5.10 Департамент операционных, ИТ/ИБ рисков и внутреннего контроля

39. Департамент операционных, ИТ/ИБ рисков и внутреннего контроля осуществляет функции по управлению рисками ИБ, предусмотренные ВД Банка, требованиями законодательства РК, и в рамках своей компетенции.

5.11 Владельцы бизнес-процессов и ИС

40. Руководители СП Банка являются владельцами соответствующих бизнес-процессов Банка и в большей степени обладают пониманием степени важности бизнес-процессов и связанных с ними информационных активов в деятельности Банка, пониманием рисков Банка от угроз нарушения бизнес-процессов или нарушения конфиденциальности, целостности или доступности информационных активов и информации.

41. Руководители СП Банка как владельцы бизнес-процессов:

1) участвуют в оценке и классификации бизнес-процессов и информационных активов путем объективной оценки их важности;

2) определяют требования по конфиденциальности, целостности и доступности информационных ресурсов, а также иные требования по ИБ в отношении бизнес-процессов и информационных ресурсов Банка;

3) являются основными участниками процесса управления рисками Банка в информационной сфере;

4) определяют потенциальные негативные факторы, составляющие риски Банка и потенциальный ущерб, которой может быть нанесен;

5) участвуют в переоценке рисков по результатам мониторинга, аудитов и инцидентов ИБ;

6) выступают как владельцы информационных активов Банка, обеспечивающих поддержку их бизнес-процессов. В их задачи входит определение и регулярный пересмотр прав доступа к используемым информационным ресурсам, принятие решения о предоставлении доступа и соответствующих полномочиях;

7) несут ответственность за предоставление полной и объективной информации ДИБ о бизнес-процессах, используемых информационных ресурсах и их оценку;

8) несут ответственность за корректную эксплуатацию ИС и ресурсов Банка в соответствии с требованиями и инструкциями по их эксплуатации;

9) обеспечивают ознакомление работников с ВД Банка, содержащими требования к ИБ;

10) несут персональную ответственность за обеспечение ИБ в возглавляемых ими СП;

11) обеспечивают заключение соглашений о неразглашении конфиденциальной информации и включение условий об обеспечении ИБ в соглашения, договоры на оказание услуг/выполнение работ в случаях, когда СП Банка выступает инициатором заключения таких соглашений, договоров;

42. Бизнес-владельцы ИС или подсистем:

1) отвечают за соблюдение требований к ИБ при создании, внедрении, модификации, эксплуатации ИС и предоставлении продуктов и услуг клиентам и СП Банка, а также при интеграции ИС с внешними ИС, включая ИС государственных органов;

2) формируют и поддерживают актуальность матриц доступа к ИС.

43. Работники СП:

1) отвечают за соблюдение требований к ИБ, принятых в Банке;

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

3) извещают своего непосредственного руководителя и ДИБ обо всех подозрительных ситуациях и нарушениях при работе с информационными активами Банка.

Глава 6. Классификация угроз ИБ Банка

44. Организация СУИБ Банка носит комплексный характер и основывается на анализе возможных негативных последствий, который предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению и способов их предотвращения.

45. Виды угроз ИБ:

1) **Антропогенные** – в качестве антропогенного источника угроз следует рассматривать субъекты, имеющие доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта.

Субъекты антропогенного источника угроз делятся на два вида, действия которых могут привести к нарушению безопасности информации: внешние и внутренние.

Внешние субъекты случайные или преднамеренные имеют разный уровень квалификации. К ним относятся:

- криминальные структуры;
- хакеры;
- недобросовестные партнеры;
- технический персонал поставщиков коммуникационных услуг;
- представители надзорных организаций и аварийных служб;
- любые другие субъекты, имеющие доступ в здание.

Внутренние субъекты представляют собой персонал Банка в области разработки и эксплуатации программного обеспечения и технических средств, а также персонал, выполняющий работу технического и вспомогательного характера. Вышеописанный персонал

имеет возможность использования штатного оборудования, технических средств сети и доступа в помещения их непосредственного расположения. К ним относятся:

- основной персонал (пользователи, администраторы, разработчики);
- вспомогательный персонал (уборщики, охрана);
- технический персонал (жизнеобеспечение, эксплуатация).

2) **Техногенные –** угрозы, вызываемые технократической деятельностью человека и развитием цивилизации.

3) **Стихийные** – угрозы, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех, процесс развития которых не управляем Банком. Такие источники угроз не поддаются прогнозированию и поэтому меры защиты от них применяются всегда.

Стихийные источники потенциальных угроз ИБ как правило являются внешними по отношению к защищаемому объекту, и под ними Банком определены следующие источники:

- пожары;
- землетрясения;
- наводнения;
- ураганы;
- другие аналогичные природные явления.

4) **К техническим средствам**, являющимся источниками потенциальных угроз ИБ, относятся:

внешние:

- средства связи;
- сети инженерных коммуникации (водоснабжения, канализации);

внутренние:

- некачественные технические средства обработки информации;
- некачественные программные средства обработки информации;
- вспомогательные средства (охраны, сигнализации, телефония);
- другие технические средства, применяемые в Банке.

Глава 7. Информационная инфраструктура и объекты защиты Банка

46. Информационная инфраструктура Банка включает в себя информационные ресурсы, автоматизированные системы, средства вычислительной техники, инженерные системы их жизнеобеспечения, а также помещения, в которых функционируют автоматизированные системы и обрабатывается информация. С информационной инфраструктурой неразрывно связан персонал Банка.

47. Информационные ресурсы Банка складываются из исходной информации, баз данных, системного, сетевого, операционного и инструментального программного обеспечения, информации, хранящейся на физических носителях, представленной как в документарной, так и в иной форме.

48. Часть информации Банка обрабатывается на средствах оргтехники, документирования, документальной и речевой связи общего пользования (персональные компьютеры, лазерные и матричные принтеры, факсимильные аппараты, телефоны внутренней и городской автоматических телефонных станций и другое).

49. Отдельные элементы инфраструктуры Банка (системы электропитания, пожарной и охранной сигнализации, проводного радиовещания и другое) в силу соприкосновения с

информационными системами являются вторичными носителями защищаемой информации или каналами ее утечки.

50. Часть информационной инфраструктуры Банка, относящаяся к звену управления и обеспечивающая принятие важных управленческих решений, требует особого внимания в связи с высокой концентрацией на этом уровне наибольшего количества обобщенных, аналитических, статистических и прогнозируемых сведений, подлежащих защите.

51. Защите подлежат следующие объекты информатизации Банка:

1) информационные ресурсы, содержащие сведения ограниченного распространения, составляющие банковскую, коммерческую и другие виды тайн, а также иные сведения, отнесенные ВД Банка к защищаемой информации конфиденциального характера;

2) средства и системы информатизации Банка (автоматизированные системы, вычислительные сети различного уровня и назначения, а также схемы их расположения, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);

3) технические средства и системы защиты информационных ресурсов Банка.

52. Информационные ресурсы, отнесенные законодательством к государственным секретам, в Политике не рассматриваются.

Глава 8. Требования к доступу к создаваемой, хранимой и обрабатываемой информации в информационных системах Банка и мониторинг информации и доступа к ней

53. Доступ к ИС Банка осуществляется путем идентификации и аутентификации пользователей.

54. Идентификация и аутентификация пользователей ИС Банка производится посредством ввода пары «учетная запись (идентификатор) – пароль» или с применением способов двухфакторной аутентификации.

55. В ИС Банка используются только персонализированные пользовательские учетные записи.

56. Использование технологических учетных записей допускается в соответствии с перечнем таких учетных записей для каждой ИС с указанием лиц, персонально ответственных за их использование и актуальность, утверждаемым *руководителем Банка, курирующим ПИТ*.

57. В ИС Банка применяются функции по управлению учетными записями и паролями, определяемые *требованиями по разграничению прав доступа к электронным информационным ресурсам Банка и требованиями парольной защиты Банка*.

58. Работникам Банка предоставляется доступ к защищаемой, конфиденциальной информации в объеме, необходимом для исполнения их функциональных обязанностей.

59. Работники Банка получают доступ к ИС после ознакомления с *Обязательством о соблюдении требований ИБ и Соглашением о неразглашении конфиденциальной информации*.

60. Запрещается предоставлять пользователям на рабочих станциях права локального администратора или аналогичные права за исключением случаев, когда такие права необходимы для функционирования программного обеспечения, автоматизирующего функции, исполняемые пользователем.

61. При изменении функциональных обязанностей работника отключаются все имеющиеся права доступа и присваиваются новые права доступа, соответствующие его новым функциональным обязанностям.

62. При прекращении трудовых отношений с работником отключаются все его права доступа в ИС.

63. При длительном отсутствии работника на рабочем месте его доступ в ИС блокируется в порядке, установленным *требованиями по разграничению прав доступа к электронным информационным ресурсам Банка*.

64. ДИБ производит проверку соответствия прав доступа функциональным обязанностям пользователей ИС, а также контроль отключения прав доступа работникам, с которыми прекращены трудовые отношения, и блокирования доступа длительно отсутствующим работникам.

65. Доступ к ИС Банка внешней стороне/третьим лицам предоставляется в рамках договорных отношений и регламентируется *требованиями по разграничению прав доступа к электронным информационным ресурсам Банка*.

Глава 9. Требования к осуществлению мониторинга деятельности по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ

66. Банком проводится мониторинг деятельности по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ.

67. Банком проводится мониторинг событий ИБ и управление инцидентами ИБ.

68. Банк определяет перечень событий ИБ, подлежащих мониторингу, источники событий, периодичность их появления, правила мониторинга и методы мониторинга.

69. ДИБ при необходимости вводит дополнительный контроль, частично или полностью останавливает бизнес-процесс в случае возникновения инцидента ИБ.

70. Для целей оперативного и постоянного наблюдения объектов мониторинга могут использоваться как специализированные программные средства, так и штатные (входящие в коммерческие продукты и системы) средства регистрации действий пользователей, процессов и т.п.

71. Банком определяется порядок отнесения событий ИБ к инцидентам ИБ.

72. Порядок управления инцидентами ИБ определяется *ВД, регламентирующим вопросы* реагирования на инциденты ИБ Банка.

Глава 10. Требования к осуществлению сбора, консолидации и хранения информации об инцидентах ИБ

73. Банк определяет порядок принятия неотложных мер к устранению инцидента ИБ, его причин и последствий.

74. Банк определяет порядок информирования о произошедшем инциденте ИБ Руководства, *уполномоченного органа* и структурных подразделений Банка.

75. Банк проводит всесторонний анализ причин возникновения инцидента ИБ, его механизма и последствий.

76. Для инцидентов ИБ, вероятность возникновения которых высока и отсутствует возможность ее снизить в ближайшем будущем, создаются отдельные документы, описывающие алгоритм обработки инцидента такого рода, типовых неотложных мер по локализации инцидента и его последствий, методов обработки инцидента.

77. На основании анализа инцидента ИБ подготавливается заключение, в котором отражается вся информация об инциденте, а также предложения по проведению корректирующих мер, в целях снижения вероятности *его повторения*.

78. Банк ведет журнал учета инцидентов ИБ с отражением всей информации об инциденте, принятых мерах и предлагаемых корректирующих мерах.

79. Информация об инцидентах ИБ, полученная в ходе мониторинга деятельности по обеспечению ИБ, подлежит консолидации, систематизации и хранению.

80. Срок хранения информации об инцидентах ИБ составляет не менее 5 (пяти) лет.

81. Процесс *сбора, консолидации и хранения информации об* инцидентах ИБ в Банке *регламентируется ВД, регламентирующим вопросы* реагирования на инциденты ИБ.

Глава 11. Требования к проведению анализа информации об инцидентах ИБ

82. ДИБ по результатам обработки инцидента ИБ проводит всесторонний анализ причин возникновения инцидента, его механизма и последствий. При сборе данных с программно-технических средств, вовлеченных в инцидент, обеспечивается сохранность и неизменность собранных данных.

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

84. Для инцидентов ИБ, вероятность возникновения которых высока и не может быть снижена в короткие сроки, ДИБ разрабатываются отдельные документы, описывающие алгоритм обработки таких инцидентов, типовых неотложных мер по локализации инцидента и его последствий.

85. Результаты анализа инцидентов ИБ, а также рекомендации по минимизации вероятности *их повторного* возникновения ДИБ ежегодно выносятся на рассмотрение Комитета по ИБ и в дальнейшем используются для оценки рисков ИБ, корректировки методов и средств обеспечения ИБ, изменения бизнес-процессов.

Глава 12. Процессы обеспечения ИБ

86. Настоящая Политика регламентирует следующие процессы обеспечения ИБ Банка:

1) Управление уязвимостями – это процесс технического анализа защищенности ИС, который подразумевает сканирование на наличие уязвимостей с использованием специализированного программного обеспечения. ДИБ проводит сканирование на уязвимости не реже одного раза в квартал в соответствии с Правилами управления уязвимостями информационных систем Банка;

2) Управление обновлениями операционных систем и программного обеспечения – это процесс отслеживания выпуска обновлений ИС, их тестирования и установки на конечные устройства, регламентируемый Правилами управления обновлениями операционных систем и программного обеспечения Банка. Обновления безопасности, устраняющие критические уязвимости, устанавливаются не позднее одного месяца со дня их публикации и распространения производителем, за исключением случаев, согласованных с ДИБ;

3) Обеспечение антивирусной защиты – это процесс организации антивирусной защиты информационных ресурсов корпоративной вычислительной сети Банка от разрушающего воздействия компьютерных вирусов и вредоносного программного обеспечения, регламентируемый Правилами антивирусной защиты Банка.

4) Управление сетевой безопасностью – это процесс, определяющий требования ИБ при проектировании, внедрении и эксплуатации сетевой инфраструктуры, регулируемый Политикой сетевой безопасности Банка;

5) Мониторинг и управление инцидентами;

6) Обеспечение осведомленности работников Банка в вопросах ИБ;

7) Предоставления доступа к информационным ресурсам Банка.

Глава 13. Ответственность работников Банка за обеспечение ИБ при исполнении возложенных на них функциональных обязанностей

87. Несоблюдение требований настоящей Политики *работниками Банка* влечет ответственность в соответствии с законодательством Республики Казахстан и *ВД* Банка.

88. Контроль за соблюдением требований настоящей Политики возлагается на Правление Банка и Исполнительных Директоров.

89. СП Банка, являющиеся участниками СУИБ несут ответственность за исполнение требований настоящей Политики в пределах своей компетенции.

90. Исключен решением СД №07-22 (з) от 22.07.2026г.

91. Исключен решением СД №07-22 (з) от 22.07.2026г.

92. Каждый пользователь лично отвечает за свои действия при обращении с информацией и при работе с ИС и ресурсами Банка.

93. Работники Банка обязаны:

1) знать и соблюдать установленные в Банке внутренние требования по обеспечению безопасности ИС;

2) использовать ИС и ресурсы в соответствии с настоящей Политикой, требованиями безопасности к конкретным ИС и приложениям;

3) информировать непосредственного руководителя или работников ДИБ о нарушениях ИБ, иных подозрительных ситуациях и инцидентах;

4) не использовать и не распространять в ИС Банка постороннее программное обеспечение;

5) обеспечивать корректное поведение в информационной сети, не предпринимать каких-либо действий по обходу или блокированию механизмов ИБ, по намеренному изменению, уничтожению, чтению или передаче информации неавторизованным способом;

6) незамедлительно уведомлять администраторов ИС и работников ДИБ о найденных уязвимостях или ошибках в программном обеспечении, а также информировать о неправомерных действиях других пользователей, нарушающих установленные правила ИБ.

94. Работникам Банка запрещается:

1) передавать конфиденциальную информацию Банка посторонним лицам любыми доступными способами;

2) использовать электронную почту в личных целях. Электронная почта предоставляется только для выполнения своих служебных обязанностей;

3) загружать на рабочую станцию информацию, не связанную с деятельностью Банка;

4) использовать и распространять в корпоративной сети Банка постороннее программное обеспечение*;*

5) хранить пароли и иные аутентификационные данные в незашифрованном виде на рабочих компьютерах, мобильных устройствах и электронных носителях информации, а также на бумажных носителях.

95. Банк оставляет за собой право осуществлять наблюдение за входящей/исходящей корреспонденцией работников.

96. Действия каждого пользователя в сети Интернет протоколируются, в случае выявленных нарушений к работнику применяются санкции дисциплинарного взыскания.

Глава 14. Заключительные положения

97. Внесение изменений и дополнений в настоящую Политику осуществляется в соответствии с требованиями *ВД по* разработке, утверждению, изменениям и/или дополнениям и прекращению действия *ВД* Банка.

98. Ответственность за внесение изменений и/или дополнений в Политику несет ДИБ.

99. Пересмотр настоящей Политики и *ВД* по ИБ может быть, как плановый, так и внеплановый – обусловленный изменениями в действующем законодательстве РК или в технологии работы СП Банка, предложениями и замечаниями аудиторов, рекомендациями внешних экспертов. Обязательный пересмотр настоящей Политики и *ВД* по ИБ с целью анализа и актуализации изложенной в ней информации должен осуществляться не реже 1 (одного) раза в два года.

100. Ответственными за информирование внешних заинтересованных сторон (Клиенты Банка, контрагенты и т.д.) об изменениях в Политике в части, их касающейся, являются руководители СП Банка, взаимодействующие с ними. Вопросы общей координации работ по информированию, а также их контроль возлагается на ДИБ.

101. Настоящая Политика обязательна для исполнения и ознакомления всеми работниками Банка.