# Политика информационной безопасности АО «Халык Банк Грузия»

г. Тбилиси

2025 г.

## Содержание

## 1. Общие положения

АО «Халык Банк Грузия» (далее-Банк) определяет политику информационной безопасности (далее - «Политика»), которая устанавливает основные принципы и требования по защите информации, а также правила/стандарты использования/безопасности информации, информационных технологий и информационных систем, которые должны соблюдать сотрудники Банка и другие пользователи. Регуляторной и юридической основой Политики являются Закон Грузии «О информационной безопасности», Регламент Национального банка Грузии «Об утверждении рамочной программы управления кибербезопасностью для коммерческих банков» и Закон Грузии «О защите персональных данных». Кроме того, настоящая Политика учитывает требования международных стандартов системы управления информационной безопасностью.

## 2. Определения терминов

**Информационная безопасность** - деятельность, направленная на обеспечение защиты доступности, целостности, аутентификации, конфиденциальности и бесперебойной работы информации и информационных систем;

**Информационный актив** - все виды информации и знаний, включая технологические средства для хранения, обработки и передачи информации, сотрудников и их знания по обработке информации, которые имеют ценность для банка.

**Контрольный механизм** - любое действие, устройство, процедура или другая мера, применяемая для снижения рисков и защиты конфиденциальности, целостности и доступности информационных активов (CIA). Это способ управления угрозами и уязвимостями с целью предотвращения инцидентов безопасности или минимизации их воздействия.

**Система управления информационной безопасностью (СУИБ)** - неотъемлемая часть внутренней организационной системы управления банка, основанная на принципах управления рисками, с целью внедрения, функционирования, мониторинга, оценки, поддержки и совершенствования информационной безопасности.

## 3. Цель политики

Настоящая Политика направлена на определение механизмов контроля информационной безопасности в отношении внутренних и внешних угроз. Целью Политики является создание механизмов контроля для защиты информации, находящейся в распоряжении Банка, выполнения функций, возложенных законодательством Грузии и Национальным банком Грузии, а также для защиты репутации Банка. Посредством этих механизмов обеспечивается

конфиденциальность, целостность и доступность информации. Кроме того, целью Политики является:

- защита и сохранение конфиденциальности, целостности и доступности информации и связанных с ней инфраструктурных активов;
- управление рисками нарушений безопасности или компрометации;
- обеспечение безопасной и стабильной среды информационных технологий;
- выявление и реагирование на случаи неправильного использования, утраты и/или несанкционированного раскрытия информационных активов;
- обнаружение возможных признаков компрометации при мониторинге систем;
- обеспечение мониторинга, анализа и постоянного улучшения процесса управления информационной безопасностью Банка;
- повышение осведомлённости и улучшение уровня знаний в области информационной безопасности.

## 4. Сфера распространения политики

Политика распространяется на все типы информационных активов, находящихся в собственности Банка, независимо от их формы или формата. Это включает как электронные, так и физические активы, которые создаются и/или используются в целях поддержки деловой деятельности Банка. Соблюдение требований, установленных Политикой, является обязательным для всех сотрудников Банка, стажёров, подрядчиков и любых третьих лиц, имеющих доступ к информационным активам Банка. Они обязаны в полной мере соблюдать правила и стандарты информационной безопасности для обеспечения защиты данных Банка.

## 5. Лидерство

Руководство высшего звена Банка несёт ответственность за управление Системой управления информационной безопасностью (СУИБ), демонстрирует лидерство и приверженность взятым обязательствам, а также формирует соответствующие подходы путём определения организационных функций, что выражается в следующем:

- формулирование политики информационной безопасности и целей в области информационной безопасности, а также обеспечение их соответствия стратегическим целям Банка;
- обеспечение интеграции требований СУИБ в бизнес-процессы Банка;
- обеспечение доступности ресурсов, необходимых для управления СУИБ;
- обеспечение коммуникации о важности эффективного управления информационной безопасностью и соблюдения требований СУИБ;
- установление и достижение целей, поставленных в рамках СУИБ;
- обеспечение содействия постоянному улучшению СУИБ;
- обеспечение надлежащего управления инцидентами безопасности и использование полученного опыта для совершенствования СУИБ.

Кроме того, поддержку информационной безопасности в Банке обеспечивает каждый сотрудник.
Помимо этого, руководство высшего звена Банка регулярно проводит систематический пересмотр эффективности СУИБ с целью обеспечения достижения поставленных целей в области качества, а также для выявления соответствующих несоответствий посредством аудита и управленческих процессов.

## 6. Рабочая группа по информационной безопасности

В Банке создана рабочая группа по информационной безопасности, основной целью которой является обеспечение эффективного функционирования, соответствия и адекватности Системы управления информационной безопасностью (СУИБ).

Цели, задачи, функции, состав группы, регламент, а также детали организационно-технической поддержки рабочей группы по информационной безопасности подробно изложены в документе — «Положение о рабочей группе по информационной безопасности».

## 7. Управление активами

Банк обеспечивает эффективную идентификацию и классификацию информационных активов с целью их надлежащей защиты на протяжении всего жизненного цикла. В рамках данного процесса:

- осуществляется выявление всех информационных активов и их классификация в соответствии с уровнем чувствительности и критичности;
- чётко определены правила обращения, изменения и уничтожения активов в соответствии с их классификацией;
- для каждого идентифицированного актива назначается ответственное лицо (владелец), которое обеспечивает его надлежащее управление и защиту.

Подробные правила идентификации и классификации информационных активов устанавливаются во внутренних документах Банка.

## 8. Управление рисками

Система управления информационной безопасностью Банка основана на непрерывном процессе управления рисками информационной безопасности, который регулируется «Политикой управления рисками информационных технологий и информационной безопасности». В рамках данного процесса Банк осуществляет следующие ключевые действия:

- выявление, формализация и анализ внутренних и внешних угроз, а также планирование мероприятий по их минимизации;

- установление чётких критериев для идентификации, анализа и оценки рисков информационной безопасности, включая методологию определения уровня риска;
- активное выявление потенциальных рисков информационной безопасности, назначение владельцев (ответственных лиц) за каждый риск, анализ потенциального воздействия на Банк и оценка вероятности наступления риска;
- для снижения выявленных рисков Банк выбирает и внедряет соответствующие контрольные механизмы, а также определяет допустимый уровень риска, чтобы принятые меры были эффективными и соразмерными;
- разработка детального плана управления рисками, включающего конкретные шаги, ресурсы и сроки для устранения выявленных угроз.
- на регулярной основе осуществляется подготовка отчётности по вопросам информационной безопасности и кибер-рисков с последующим представлением уполномоченному органу.

## 9. Управление рисками третьих сторон

Банк обеспечивает безопасность взаимодействия с третьими сторонами с целью защиты информационных активов и снижения связанных с ними рисков. В этих целях Банк реализует следующие мероприятия:

- все поставщики и подрядчики, имеющие доступ к конфиденциальной информации или системам Банка, проходят полную оценку информационной безопасности. Целью этой оценки является проверка уровня их защищённости и соответствие требованиям информационной безопасности Банка;
- Банк обеспечивает включение чётко сформулированных требований по безопасности в каждый контракт с третьими сторонами. Эти требования обязывают поставщиков соблюдать политику безопасности Банка, включая стандарты защиты данных, отчётности об инцидентах и безопасности систем;
- соблюдение мер безопасности со стороны третьих лиц контролируется Банком с установленной периодичностью, что гарантирует постоянное соответствие предоставляемых услуг требованиям Банка;
- в Банке действует документ «Правила взаимодействия с аутсорсинговыми организациями», который регулирует вопросы, связанные с внешними подрядчиками.

## 10. Управление непрерывностью бизнеса

С учётом аспектов информационной безопасности Банк определяет требования к обеспечению непрерывности бизнеса. На этой основе разрабатываются и поддерживаются планы обеспечения непрерывности деятельности в соответствии с требованиями информационной безопасности. Эти планы позволяют Банку в кратчайшие сроки восстановить все критически важные сервисы в случае кризисных ситуаций или катастроф.

В целях реализации системы управления информационной безопасностью Банк определяет и с установленной периодичностью оценивает:

- критерии информационной безопасности и обеспечения непрерывности;
- роли и зоны ответственности в случае возникновения серьёзного инцидента;
- процедуры действий в чрезвычайных ситуациях;
- целевые показатели доступности сервисов;
- В Банке периодически актуализируется стратегия управления информацией. При её обновлении учитываются требования законодательства, внутренних нормативных актов, потребности владельцев бизнес-процессов, а также следующие критерии, применимые к информации: конфиденциальность, целостность, доступность и актуальность.

Для достижения высокого уровня доступности Банк внедряет резервные средства обработки информации и учитывает методы высокой устойчивости при планировании и развитии ИТ-инфраструктуры.

Кроме того, дважды в год в Банке проводится тестирование планов обеспечения непрерывности бизнеса, которое регулируется «Политикой обеспечения непрерывности бизнеса».

## 11. Управление инцидентами информационной безопасности

Банк обеспечивает эффективную и непрерывную реализацию процесса управления инцидентами информационной безопасности. Этот процесс осуществляется специализированной командой, ответственной за своевременное и скоординированное реагирование на инциденты. Все инциденты в области информационной безопасности фиксируются и обрабатываются в соответствии с установленным в Банке порядком. Процесс управления инцидентами включает следующие этапы: выявление инцидента, реагирование, сбор доказательств, устранение, анализ и распространение полученных знаний. Банк также обеспечивает взаимодействие с заинтересованными сторонами в рамках установленного порядка информирования об инцидентах.

## 12. Физическая безопасность

Банк обеспечивает высокий уровень физической безопасности для защиты информационных активов. Ответственные структурные подразделения Банка реализуют следующие меры контроля:

- контролируют защиту материальных активов с целью предотвращения несанкционированного доступа, вмешательства и/или повреждения;
- обеспечивают контроль физического доступа к устройствам, содержащим или обрабатывающим информацию высокой критичности и/или чувствительности. Такие устройства должны размещаться в физически защищённых зонах с ограниченным доступом;
- обеспечивают защиту компьютерных систем и сетей с использованием физических, технических и процедурных механизмов контроля безопасности.

## 13. Безопасность корпоративной сети

Банк обеспечивает высокий уровень сетевой безопасности с целью защиты информационных активов и снижения киберрисков. В этих целях реализуются следующие основные мероприятия:

- критически важные системы (например, основные банковские приложения, базы данных клиентов) сегментированы в изолированные сетевые зоны;
- сотрудники, работающие удалённо или получающие доступ из внешних локаций, используют VPN-соединения с надёжным шифрованием для обеспечения безопасного подключения к внутренней сети Банка;
- уязвимости в сетевых устройствах и системах регулярно сканируются и устраняются, чтобы предотвратить их возможную эксплуатацию злоумышленниками.

Кроме того, дважды в год в Банке проводится тестирование обеспечения непрерывности бизнеса, в рамках которого осуществляется проверка бесперебойной работы внутренней корпоративной сети - как в основной, так и в альтернативной серверной инфраструктуре.

## 14. Аудит и соответствие

Банк регулярно проводит аудит системы управления информационной безопасностью с целью обеспечения полного соответствия требованиям безопасности и постоянного совершенствования. Цели аудита включают:

- проверку соответствия банка требованиям Национального банка Грузии, международным стандартам (например, ISO ISO/IEC 27001, COBIT и др.) и внутренним требованиям банка;
- оценку степени соответствия существующих мер безопасности и процессов установленным требованиям информационной безопасности;
- выявление возможностей для улучшения внедрения и последующей поддержки СУИБ;
- в процессе выбора и проведения аудита банк учитывает требования «Руководства по аудиту управления информационными системами и кибербезопасностью в коммерческих банках».

## 15. Управление уязвимостями (Vulnerability Management)

Банк осуществляет непрерывный и регулярный процесс управления уязвимостями с целью своевременного выявления, оценки, устранения и мониторинга уязвимостей. Процесс управления уязвимостями включает следующие основные этапы:

- сканирование уязвимостей проводится регулярно на всех сетевых устройствах банка, серверах, рабочих станциях и приложениях;

- выполняется аудит конфигураций, обзор безопасности кода и другие технические проверки для выявления известных уязвимостей и ошибок конфигурации;
- постоянно ведется мониторинг информации о внешних угрозах (например, CVE) для своевременного реагирования на недавно обнаруженные уязвимости;
- идентифицированные уязвимости оцениваются по уровню критичности, сложности эксплуатации и потенциальному воздействию на активы банка, операции и репутацию;
- Банк использует риск-ориентированный подход для определения приоритетов устранения, отдавая предпочтение наиболее критичным и высокорисковым уязвимостям;
- Патчи безопасности и обновления операционных систем, приложений и прошивок (firmware) применяются незамедлительно в соответствии с утверждёнными процедурами и приоритетами, основанными на рисках;
- Процесс управления уязвимостями и прогресс устранения постоянно контролируются в банке;
- Регулярные отчёты о статусе уязвимостей, эффективности устранения и общих рисках предоставляются рабочей группе по информационной безопасности.

## 16. Безопасное использование носителей информации

Банк обеспечивает, чтобы все используемые носители информации, содержащие конфиденциальные данные, находились под безопасным управлением на протяжении всего жизненного цикла — от создания до уничтожения. Для этого:

- Все носители информации, содержащие конфиденциальные данные (например, внешние жесткие диски, USB-накопители и другие), учтены и промаркированы в соответствии с установленными правилами;
- Информация, размещённая на носителях, классифицируется согласно внутренней политике банка;
- В банке определены требования по безопасной обработке, хранению и уничтожению информации;
- Носители, содержащие конфиденциальную информацию, хранятся в защищённой среде с жёстким контролем физического доступа, чтобы предотвратить несанкционированный доступ, повреждение или кражу;
- Доступ к носителям информации, содержащим конфиденциальные данные, ограничен принципом минимальных привилегий;
- Любой носитель, предназначенный для резервного копирования или восстановления, должен регулярно тестироваться для обеспечения его исправного функционирования и доступности данных.

## 17. Тестирование на проникновение информационных систем

Банк регулярно проводит тестирование на проникновение информационных систем. Основная цель данного тестирования - выявление неправильных конфигураций, уязвимостей и/или слабых мест в системах банка.

По результатам тестирования банк разрабатывает детальный план действий для устранения всех выявленных уязвимостей и несоответствий, обеспечивает эффективное выполнение, мониторинг и отчётность данного процесса с целью повышения уровня безопасности систем.

## 18. Повышение осведомленности и тренинги

Банк активно заботится о повышении уровня осведомлённости сотрудников в области информационной безопасности. В этой связи:

- Все сотрудники ознакомлены с политиками информационной безопасности и сопутствующей документацией. Особое внимание уделяется их обязанностям и роли в обеспечении эффективности системы управления информационной безопасностью;
- Все сотрудники банка проходят обучение по повышению осведомлённости и соответствующее тестирование дважды в год. Это обеспечивает регулярное обновление знаний о современных угрозах безопасности и лучших практиках;
- Вся необходимая информационная документация постоянно доступна на внутреннем портале банка (интранете), что позволяет сотрудникам в любое время ознакомиться с мерами безопасности и актуализировать свои знания.

## 19. Цикл постоянного совершенствования

Банк активно реализует процесс постоянного совершенствования системы управления информационной безопасностью. В рамках этого процесса используются различные источники, в том числе:

- Результаты аудитов - как внутренних, так и внешних;
- Устранение выявленных недостатков и предотвращение потенциальных рисков;
- Регулярная идентификация и анализ рисков;
- Извлечение уроков из произошедших инцидентов (Lessons learned);
- Непрерывный анализ системных событий;
- Периодические обзоры и оценки со стороны высшего руководства.

На основании этих данных банк формирует детальные планы и цели по совершенствованию. Отчёт о достигнутом прогрессе представляется рабочей группе по информационной безопасности один раз в квартал для рассмотрения и утверждения, что обеспечивает непрерывное развитие и эффективность СУИБ (системы управления информационной безопасностью).

## 20. Нарушение политики

Информация, информационные системы и технологии банка являются критически важными компонентами его деятельности. Соответственно, каждый сотрудник банка обязан обеспечивать безопасность указанных ресурсов с точки зрения конфиденциальности, доступности и целостности. Несоответствие установленным профессиональным практикам и внутренним политикам банка может рассматриваться как серьёзное нарушение, что может

повлечь за собой дисциплинарную ответственность, включая расторжение трудового договора/контракта в соответствии с действующим законодательством.

## 21. План пересмотра политики

Ответственность за пересмотр, обновление, постоянное совершенствование политики и её соответствие стратегическим целям банка возлагается на менеджера по информационной безопасности департамента безопасности банка. Политика подлежит пересмотру не реже одного раза в три года и/или в случае существенных изменений.

В случае внесения изменений в законодательство Грузии и/или нормативные акты регулирующего органа по вопросам, рассмотренным в настоящем документе, приоритет отдается вышеуказанным документам. Документ и/или любые внесённые в него изменения утверждаются Наблюдательным советом банка в соответствии с установленным внутренним порядком.