Евразийский Банк

Утверждена
Советом директоров
АО «Евразийский банк»
Протокол № 60
от «12» июля 2023 г.

для широкого пользования

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПТ

Политика информационной безопасности (далее – Политика) разработана в соответствии с Постановлением Правления Национального Банка Республики Казахстан (далее – РК) от 27 марта 2018 года № 48 «Об утверждении Требований к обеспечению информационной безопасности банков и организаций, осуществляющих отдельные виды банковских операций» (далее - Постановление №48), Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования», СТ РК ISO/IEC 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации» и внутренними нормативными документами (далее – ВНД) АО «Евразийский банк» (далее – Банк), в том числе Политикой внутреннего нормативного регулирования.

Раздел 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика разработана с целью определения основных принципов и направлений в области информационной безопасности (далее - ИБ) и охватывает все бизнес-процессы, информационные системы (далее - ИС) и документы, владельцем и пользователем которых является Банк.

2. Настоящая Политика определяет:

1) цели, задачи и основные принципы построения системы управления информационной безопасностью (далее – СУИБ);

2) область действия и участников СУИБ;

3) требования к управлению ИБ, в том числе:

– требования к доступу к создаваемой, хранимой и обрабатываемой информации в информационных системах Банка, мониторинг информации и доступа к ней;

– требования к осуществлению мониторинга деятельности по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ;

– требования к осуществлению сбора, консолидации и хранения информации об инцидентах ИБ;

– требования к проведению анализа информации об инцидентах ИБ;

– ответственность работников Банка за обеспечение ИБ при исполнении возложенных на них функциональных обязанностей.

3. Банк обеспечивает создание и функционирование СУИБ, являющейся частью общей системы управления Банка, предназначенной для управления процессом обеспечения ИБ.

4. Целью СУИБ является обеспечение защиты информационных активов Банка, допускающую минимальный уровень потенциального ущерба для бизнес-процессов Банка, минимизация ущерба от событий, таящих угрозу безопасности информации.

5. Основными задачами СУИБ в Банке являются:

– категорирование информационных активов путем разделения их на критичные и некритичные на основании максимального уровня критичности, хранимой и обрабатываемой в них информации;

– своевременное выявление потенциальных угроз ИБ и уязвимостей в информационных активах Банка;

– регулярное проведение оценки рисков ИБ на основании выявленных потенциальных угроз ИБ и уязвимостей информационных активов Банка;

– исключение либо минимизация выявленных рисков;

– применение обоснованных, экономически эффективных организационных и технических мер по обеспечению ИБ;

– предотвращение инцидентов ИБ или минимизация их последствий;

– выявление применимых требований действующего законодательства и регуляторов в области ИБ, достижение соответствия этим требованиям;

– установление ответственности работников по вопросам обеспечения ИБ, обучение и повышение их осведомленности в части ИБ;

– мониторинг эффективности процессов СУИБ.

6. В Политике используются основные понятия, предусмотренные законодательством РК, в том числе Постановлением №48, а также электронным справочником.

Раздел 2. ОСОБЕННЫЕ ПОЛОЖЕНИЯ

Глава 1. Области применения СУИБ

7. Определенная Банком организационная область действия и границы системы менеджмента информационной безопасности (далее - СМИБ) включают в себя:

– все бизнес-процессы Банка, в том числе процессы информационного обмена с клиентами и контрагентами Банка;

– всех работников Банка, а также работников контрагентов при выполнении работ в инфраструктуре Банка, либо при обработке информации, предоставленной Банком;

– всю информацию, собираемую, обрабатываемую и хранимую в результате функционирования бизнес-процессов Банка, в том числе информацию, ответственность по обеспечению безопасности которой передана третьей стороне в рамках информационного обмена с контрагентами.

8. Определенные Банком области действия и границы СМИБ для информационных и коммуникационных технологий включает в себя все информационные активы Банка, необходимые для функционирования бизнес-процессов Банка, включая информационные активы, ответственность по обеспечению безопасности которых передана третьей стороне (размещение серверных мощностей в сторонних центрах обработки данных, использование внешних сервисов обработки и/или хранения данных).

9. Определенные Банком физические области действия и границы СМИБ включает в себя административные помещения Банка и/или его филиалов (отделений) и иные используемые им (ими) помещения различного предназначения, с размещенным в них оборудованием, либо прилегающей территорией (при наличии и/или в пределах установленной зоны ответственности Банка).

10. Политика пересматривается с целью анализа и актуализации изложенной в них информации не реже одного раза в год.

Глава 2. Принципы построения СУИБ

11. Построение СУИБ в Банке и их функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность – любые действия, предпринимаемые для обеспечения ИБ, осуществляются на основе действующего законодательства РК и ВНД Банка, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Банка;

– ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки бизнес-процессов в Банке. Любые меры по обеспечению ИБ не должны повлечь за собой серьезных препятствий деятельности Банка;

– непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Банка должны осуществляться без прерывания или остановки текущих бизнес-процессов Банка;

– комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;

– обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам;

– приоритетность – категорирование (ранжирование) всех информационных ресурсов Банка по степени критичности на основании максимального уровня критичности хранимой и обрабатываемой в них информации, а также потенциальных угроз ИБ;

– необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им функциональных обязанностей в рамках своих полномочий;

– специализация – эксплуатация технических средств и реализация мер ИБ должны осуществляться профессионально подготовленными работниками Банка;

– информированность и персональная ответственность – руководители всех уровней и работники Банка должны быть осведомлены обо всех требованиях ИБ и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер ИБ;

– взаимодействие и координация – меры ИБ осуществляются на основе взаимосвязи соответствующих структурных подразделений Банка, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

– подтверждаемость – критичная документация и все записи – документы, подтверждающие исполнение требований по ИБ и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

Глава 3. Функции участников СУИБ

12. Основными участниками системы управления информационной безопасностью Банка являются:

1) Совет директоров;
2) Правление;
3) Комитет по ИБ (далее – УКО);
4) подразделение ИБ;
5) подразделение по информационным технологиям;
6) подразделение по безопасности;
7) подразделение по работе с персоналом;
8) юридическое подразделение;
9) подразделение комплаенс и внутреннего контроля;
10) подразделение внутреннего аудита;
11) подразделение по управлению рисками ИТ и ИБ.

13. Совет директоров утверждает перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну (далее – защищаемая информация), и порядок работы с защищаемой информацией.

14. Председатель Правления осуществляет стратегическое планирование, координацию деятельности всех подразделений Банка для организации и поддержания соответствующего уровня ИБ.

15. Правление Банка утверждает внутренние документы, регламентирующие процесс управления информационной безопасностью, порядок и периодичность пересмотра которых определяется Инструкцией по управлению внутренними нормативными документами.

16. Банк создаёт УКО, в состав которого входят представители подразделения по ИБ, подразделения по управлению рисками ИБ, подразделения по информационным технологиям, а также при необходимости представители других подразделений Банка. Руководителем УКО назначается Председатель Правления Банка либо заместитель Председателя Правления Банка, курирующий деятельность подразделения по ИБ.

17. УКО осуществляет периодический мониторинг деятельности по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ не реже раза в год. Процесс мониторинга деятельности по обеспечению ИБ, мероприятий по выявлению и анализу угроз, а также противодействию атакам должен включать отчёт по выявлению, анализу угроз и противодействию атакам на основе данных, предоставленных подразделением ИБ по количеству выявленных угроз, принятых мер и произошедших инцидентов ИБ. Мониторинг мероприятий по расследованию инцидентов ИБ включает в себя оценку последствий инцидентов, указание причин и планов мероприятий по предотвращению, либо уменьшению влияния инцидентов ИБ.

18. Руководитель подразделения ИБ обеспечивает разработку, внедрение и совершенствование документированных стандартов и процедур в области ИБ.

19. Подразделение ИБ проводит мониторинг событий ИБ и управления инцидентами ИБ, в рамках которого определяется перечень событий ИБ, подлежащих мониторингу, источники событий, периодичность, правила мониторинга и их методы. Подразделение ИБ, осуществляющее мониторинг,

вправе вводить дополнительные контроли, частичную или полную остановку бизнес-процесса в случае выявления инцидента ИБ.

20. Подразделение ИБ обеспечивает своевременное проведение анализа информации об инцидентах ИБ, который должен включать в себя раскрытие обстоятельств события, при которых стала возможна реализация инцидента ИБ, взаимодействие с подразделением по управлению рисками ИБ, при необходимости, формирование рекомендаций по внедрению защитных мер.

21. Подразделение по информационным технологиям обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности данных информационных систем Банка (включая резервирование и (или) архивирование и резервное копирование информации) в соответствии с ВНД Банка, а также обеспечивает соблюдение требований ИБ при выборе, внедрении, разработке и тестировании ИС.

22. Подразделение по управлению рисками ИБ отвечает за осуществление категорирования информационных активов путем разделения их на критичные и некритичные на основании максимального уровня критичности хранимой и обрабатываемой в них информации.

23. Подразделение по безопасности реализует меры физической и технической безопасности, в том числе организует пропускной и внутриобъектовый режим, а также проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз ИБ при приеме на работу и увольнении работников Банка.

24. Подразделение по работе с персоналом обеспечивает подписание работниками банка, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации, а также участвует в организации процесса повышения осведомленности работников Банка в области ИБ.

25. Юридическое подразделение осуществляет правовую экспертизу ВНД и внутренних документов Банка по вопросам обеспечения ИБ, в соответствии с Инструкцией по управлению внутренними нормативными документами.

26. Подразделение по комплаенс-контролю совместно с юридическим подразделением Банка определяет виды информации, подлежащие включению в перечень защищаемой информации.

27. Подразделение внутреннего аудита проводит оценку состояния СУИБ Банка при проведении аудиторских проверок.

28. Правление Банка осуществляет координацию деятельности всех подразделений Банка для организации и поддержания соответствующего уровня информационной безопасности и несет ответственность за реализацию положений Политики.

29. Правление Банка совместно с подразделением информационных технологий и подразделением информационной безопасности обязано активно реализовывать комплекс мероприятий по поддержанию ИС и электронных информационных ресурсов (далее - ЭИР) Банка посредством дачи ясных указаний, демонстрированных обязательств, чётких постановок задач и осведомлённости работников об обязанностях по обеспечению ИБ.

30. Координация ИБ должна включать взаимосвязь и сотрудничество пользователей, администраторов, разработчиков прикладного программного обеспечения и квалифицированных специалистов в таких областях, как кадровые ресурсы, информационные технологии и управление рисками.

Эта деятельность должна:

1) обеспечивать соответствие выполнения мероприятий по обеспечению ИБ;

2) определять мероприятия по обеспечению ИБ в случае её несоответствия Политике;

3) утверждать методологию и процессы обеспечения ИБ, например, оценку рисков, классификацию информации;

4) идентифицировать все изменения угроз ИБ и степень уязвимости информации и средств обработки информации к угрозам ИБ;

5) оценивать адекватность принимаемых решений и координировать реализацию мер контроля ИБ;

6) повышать уровень подготовки пользователей в области ИБ и осведомлённости о ней;

7) оценивать информацию, полученную от мониторинга и просмотра инцидентов по ИБ и рекомендовать соответствующие мероприятия в ответ на идентифицированные инциденты ИБ.

31. Правление Банка должно обеспечивать чёткое управление и зримую поддержку инициатив по совершенствованию СУИБ.

32. Правление Банка должно обеспечивать координацию мер контроля за ИБ и предоставлять ресурсы для обеспечения ИБ.

33. Правление Банка должно утверждать распределение специфических ролей и обязанностей по ИБ.

34. Правление Банка берет на себя обязательство о соответствии ИС действующим требованиям, связанным с информационной безопасностью, законодательным требованиям, в том числе требованиям по соблюдению прав на интеллектуальную собственность.

35. Требования к обучению и осведомлённости в вопросах ИБ:

1) пользователи, работники подразделения по информационным технологиям, и контрагенты, должны быть ознакомлены с Политикой;

2) ответственный за ИБ Банка должен проводить первичный инструктаж по ИБ;

3) работники подразделения по информационным технологиям, обеспечивающие функционирование ИС и ЭИР должны проходить регулярный инструктаж по соблюдению требований ИБ;

4) ответственный за ИБ по мере необходимости, но не менее 1 (одного) раза в 3 (три) года, проходит курсы по повышению квалификации по информационной безопасности;

36. Банк обеспечивает повышение квалификации работников подразделений по информационной безопасности, по управлению рисками информационной безопасности и внутреннего аудита путем проведения внешнего обучения (посещение курсов, семинаров – не реже 1 (одного) раза в 3 (три) года для каждого работника).

37. В целях обеспечения выполнения содержащихся в Политике требований необходимо обеспечить её соблюдение третьими сторонами. Поэтому, в соответствующих случаях все договоры, заключаемые сторонними юридическими и физическими лицами, должны содержать требование о соблюдении требований Политики и обеспечения ИБ. Вся деятельность, подразумевающая контакт контрагентов с данными, содержащимися в ИС и ЭИР Банка, должна осуществляться в соответствии с изложенными в Политике нормативными требованиями. Данное требование распространяется на всех контрагентов.

Глава 4. Требования по управлению ИБ

38. Основными мерами защиты конфиденциальности, целостности и доступности информационных активов Банка являются:

– управление сетевой безопасностью;
– управление уязвимостями и политиками безопасности;
– управление безопасностью конечных устройств;
– управление идентификацией и доступом;
– управление инцидентами ИБ;
– управление криптографическими средствами защиты;
– управление антивирусными средствами защиты;
– обеспечение физической безопасности информационных активов;
– обеспечение безопасности при взаимодействии с контрагентами;
– обучение и повышение осведомленности персонала в вопросах ИБ;
– обеспечение безопасности интернет-ресурсов.

39. В части организационных мероприятий ИБ Банка требуется:

1) создание и функционирование подразделения по ИБ, ответственного за управление ИБ и разработке мер по обеспечению ИБ;

2) соответствие количества работников и сотрудников, ответственных за ИБ и их квалификации уровню возлагаемых на них задач;

3) утверждение и регулярный пересмотр действующей документации в части ИБ (четырехуровневой системы документированных правил, процедур, практических приемов или руководящих принципов), а также ознакомление с ними работников и сотрудников Банка в части, касающейся их обязанностей, не реже раза в год.

4) планирование мер по обеспечению ИБ на основе оценки рисков ИБ.

40. Задачи обеспечения безопасности информационных ресурсов решаются следующими методами:

– минимизация данных и привилегий на основе принципов минимальной достаточности;

– разделение полномочий и дублирование контроля;
– установление единого порядка хранения и обработки конфиденциальной информации;
– поддержание работоспособности информационных систем, имеющих отношение к ИБ;
– реагирование ответственных лиц на нарушение режима ИБ;
– получение у работников Банка и контрагента обязательства соблюдения требований ИБ и обеспечения сохранности конфиденциальной информации;
– проведение периодического обучения и повышения квалификации работников Банка в области ИБ.

41. Банк разрабатывает внутренние процедуры по созданию, сбору, хранению и обработке информации в ИС Банка. Банк осуществляет мониторинг за процессами создания, хранения и обработки информации и доступа к ней с помощью механизмов ИС и технических средств обеспечения безопасности. Доступ к создаваемой, хранимой и обрабатываемой информации в ИС Банка предоставляется работникам в соответствии с их функциональными обязанностями в соответствии с принципом наименьшего уровня привилегий.

42. Перечень событий ИБ, подлежащих мониторингу, источники событий, периодичность, правила мониторинга и их методы пересматриваются подразделением ИБ не реже одного раза в год с учетом имеющейся статистики и эффективности мониторинга.

43. Порядок управления инцидентами ИБ определяется соответствующими ВНД Банка и содержит в себе положения по консолидации, систематизации и хранению информации об инцидентах ИБ, порядки отнесения события ИБ к инцидентам ИБ, последующего анализа инцидента ИБ и информирования о произошедшем инциденте ИБ.

44. Процесс консолидации, систематизации и хранения информации об инцидентах ИБ должен обеспечивать целостность, доступность и конфиденциальность, а также полноту данных об инциденте, достаточных для осуществления анализа инцидента, проведения служебных проверок и формирования отчетности, предусмотренной Постановлением №48.

45. Бизнес-владельцы ИС отвечают за соблюдение требований к ИБ при создании, внедрении, модификации, предоставлении клиентам продуктов и услуг, а также формируют и поддерживают актуальность матриц доступа к ИС.

46. Руководители структурных подразделений Банка обеспечивают ознакомление работников с ВНД Банка, содержащими требования к ИБ, а также отвечают за обеспечение в подчиненных подразделениях выполнения требований ИБ, внедрение мер защиты при разработке новых продуктов, услуг, бизнес-приложений, бизнес-процессов и технологий.

Раздел 3. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

47. Ответственность за неисполнение/ненадлежащее исполнение требований Политики, а также за обеспечение ИБ при исполнении возложенных на них функциональных обязанностей несут все работники Банка.

48. Контроль за исполнением требований, устанавливаемых Политикой, возлагается на УКО.

49. Политика вступает в силу на следующий рабочий день после внесения в Базу данных ВНД и является общеобязательной к применению и руководству всеми работниками Банка, а также доводится до сведения третьих лиц, имеющих доступ к информационным активам Банка.

50. Вопросы, неурегулированные Политикой, разрешаются в соответствии с законодательством Республики Казахстан и ВНД Банка.

Директор службы ИТ-безопасности
Рустамов Э.А.

ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

№ п/п	Номер протокола	Дата протокола	Дата вступления в силу	Инициатор изменений
1.				
2.				