Евразийский Банк

Утверждена
Советом директоров
АО «Евразийский банк»
Протокол №15
от «26» февраля 2019 г.

для внутреннего 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) 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 и охватывает все бизнес-процессы, информационные системы и документы, владельцем и пользователем которых является Банк.

2. Целью деятельности по управлению информационной безопасностью в Банке является обеспечение защиты информационных активов Банка и минимизация ущерба от событий, таящих угрозу безопасности информации.

3. Задачами деятельности по управлению информационной безопасностью 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 информационной безопасности и уязвимостей в информационных активах Банка;

– исключение либо минимизация выявленных угроз;

– предотвращение инцидентов информационной безопасности или минимизация их последствий.

4. 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 информационной безопасности;
– 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.

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

Раздел 2. ОСОБЕННЫЕ ПОЛОЖЕНИЯ

5-1. Банк обеспечивают создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления банка, предназначенной для управления процессом обеспечения информационной безопасности.

5-2. Система управления информационной безопасностью обеспечивает защиту информационных активов банка, допускающую минимальный уровень потенциального ущерба для бизнес-процессов банка.

6. Построение системы управления информационной безопасности в Банке и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность – любые действия, предпринимаемые для обеспечения информационной безопасности, 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 информационной безопасности 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 информационной безопасности;

– 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 информационной безопасности должны осуществляться профессионально подготовленными работниками Банка;

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

– взаимодействие и координация – меры информационной безопасности 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 информационной безопасности и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

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

7-1. Участниками системы управления информационной безопасностью банка являются:

1) Совет директоров;

2) Правление;

3) Комитет по информационной безопасности (далее – УКО);

4) подразделение информационной безопасности;

5) подразделение по информационным технологиям;

6) подразделение по безопасности;

7) подразделение по работе с персоналом;

8) подразделение правового сопровождения банковской деятельности и корпоративных вопросов;

9) подразделение комплаенс и внутреннего контроля;

10) подразделение внутреннего аудита;

11) подразделение по управлению рисками ИТ и информационной безопасности.

7-2. 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.

7-3. Правление утверждает внутренние документы, регламентирующие процесс управления информационной безопасностью, порядок и периодичность пересмотра которых определяется Инструкцией по управлению внутренними нормативными документами.

8. Банк создаёт УКО, в состав которого входят представители подразделения по информационной безопасности, подразделения по управлению рисками информационной безопасности, 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 информационной безопасности.

9. УКО осуществляет периодический мониторинг деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности не реже раза в год. Процесс мониторинга деятельности по обеспечению информационной безопасности, 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 информационной безопасности по количеству выявленных угроз, принятых мер и произошедших инцидентов информационной безопасности. Мониторинг мероприятий по расследованию инцидентов информационной безопасности включает в себя оценку последствий инцидентов, указание причин и планов мероприятий по предотвращению, либо уменьшению влияния инцидентов информационной безопасности.

10. Подразделение информационной безопасности проводит мониторинг событий информационной безопасности и управления инцидентами информационной безопасности, в рамках которого определяется перечень событий информационной безопасности, подлежащих мониторингу, источники событий, периодичность, правила мониторинга и их методы.

Подразделение информационной безопасности, осуществляющее мониторинг, вправе вводить дополнительные контроли, частичную или полную остановку бизнес-процесса в случае выявления инцидента информационной безопасности.

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

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

13. Процесс консолидации, систематизации и хранения информации об инцидентах информационной безопасности 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.

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

15. Руководитель подразделения информационной безопасности обеспечивает разработку, внедрение и совершенствование документированных стандартов и процедур в области информационной безопасности.

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

17. 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 информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем.

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

19. 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 информационной безопасности при приеме на работу и увольнении работников Банка.

20. 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 информационной безопасности.

21. Юридическое подразделение осуществляет правовую экспертизу ВНД и внутренних документов Банка по вопросам обеспечения информационной безопасности, в соответствие с Инструкцией по управлению внутренними нормативными документами.

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

23. Подразделение внутреннего аудита проводит оценку состояния системы управления информационной безопасностью Банка при проведении аудиторских проверок.

24. Бизнес-владельцы информационных систем или подсистем отвечают за соблюдение требований к информационной безопасности при создании, внедрении, модификации, предоставлении клиентам продуктов и услуг, а также формируют и поддерживают актуальность матриц доступа к информационным системам.

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

Раздел 3. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

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

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

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

29. Вопросы, не урегулированные Политикой, разрешаются в соответствии с законодательством Республики Казахстан и ВНД.

Директор службы ИТ-безопасности
Рустамов Э.А.

ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

№ п/п	Номер протокола	Дата протокола	Дата вступления в силу	Инициатор изменений
1.	№ 42	11.06.2019	14.06.2019	Служба ИТ безопасности
2.				