Приложение
к Постановлению Совета директоров
№0219/1 от 19.02.2024 г.

Одобрено
Протоколом Правления
№ 0129/8 от 29.01.2024 г.

Политика информационной безопасности АО «Банк ЦентрКредит»

Содержание

1. Общие положения

1. Настоящая Политика информационной безопасности (далее – Политика) является основополагающим документом системы управления информационной безопасности АО «Банк ЦентрКредит» (далее – Банк), определяющим цели, задачи и область действия системы управления информационной безопасностью Банка (далее – СУИБ).

2. СУИБ обеспечивает защиту информационных активов Банка, допускающую минимальный уровень потенциального ущерба для бизнес-процессов Банка.

3. Политика разработана в соответствии с законодательством Республики Казахстан, в том числе нормативными правовыми актами, регулирующими требования к обеспечению информационной безопасности банков второго уровня, а также требованиями международных стандартов в области информационной безопасности.

4. Требования, предъявляемые к процессам системы управления информационной безопасности Банка, изложенные в настоящей Политике, детально описаны во внутренних нормативных документах Банка, разработанных в соответствии с Главой 9 «Требования к процессам системы управления информационной безопасностью» постановления Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 «Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах».

2. Цели, задачи и основные принципы построения системы управления информационной безопасностью

5. Первый руководитель Банка обеспечивает создание, функционирование и улучшение СУИБ, являющейся частью общей системы управления банка, организации, предназначенной для управления процессом обеспечения информационной безопасности

6. Целью СУИБ является повышение эффективности процессов обеспечения информационной безопасности, обеспечение требуемого уровня конфиденциальности, целостности и доступности критичных информационных активов, и как следствие, снижение рисков информационной безопасности и связанного с ними ущерба.

7. К задачам СУИБ относятся:

1) категорирование информационных активов;

2) организация доступа к информационным активам;

3) обеспечение безопасности информационной инфраструктуры;

4) осуществление мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз и уязвимостей, противодействию атакам и расследованию инцидентов информационной безопасности;

5) проведение анализа информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах;

6) определение порядка управления средствами криптографической защиты информации;

7) обеспечение информационной безопасности при доступе третьих лиц к информационным активам;

8) проведение внутренних проверок состояния информационной безопасности.

8. Построение СУИБ и ее функционирование осуществляются в соответствии со следующими основными принципами:

1) законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на информационные активы Банка;

2) ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки основной деятельности, любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий для ведения бизнеса;

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

4) 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. Во всех случаях стоимость мер и технологических решений по обеспечению информационной безопасности не должна превышать стоимость защищаемых информационных активов;

5) адаптивность – определение и применение методов и средств защиты информационных активов в соответствии с их критичностью;

6) необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем информационным активам, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

7) специализация – реализация мер и эксплуатация технологических решений по обеспечению информационной безопасности должны осуществляться профессионально подготовленными специалистами;

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

9) 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;

10) подтверждаемость – свидетельства, подтверждающие исполнение требований по информационной безопасности и эффективности СУИБ должны создаваться и храниться с возможностью оперативного доступа и восстановления.

3. Область действия системы управления информационной безопасностью

9. Областью действия СУИБ являются основные бизнес-процессы Банка, непосредственно ориентированные на предоставление услуг клиентам, представляющие ценность для клиентов и обеспечивающие получение прибыли, определенные процедурой классификации бизнес-процессов, а также процессы, обеспечивающие деятельность Удостоверяющего Центра Банка.

10. Объектами защиты являются критичные информационные активы, необходимые для функционирования основных бизнес-процессов, а также информационные активы, обеспечивающие функционирование Удостоверяющего Центра, к которым могут быть отнесены:

1) индивидуальные устройства обработки информации;
2) носители информации;
3) периферийное компьютерное оборудование;
4) серверы;
5) базы данных;
6) сетевое оборудование;
7) аппаратура телефонии;
8) физические каналы связи;
9) виртуальные каналы связи;
10) системы виртуализации;
11) операционные системы;
12) программное обеспечение аппаратных средств;
13) прикладное программное обеспечение;
14) программное обеспечение телефонии;
15) средства криптографической защиты информации.

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

11. Доступ к информации и информационным системам Банка предоставляется работникам в объеме, необходимом для исполнения их функциональных обязанностей.

12. Предоставление доступа к критичным информационным системам Банка производится путем формирования и внедрения ролей для обеспечения соответствия прав доступа пользователей информационных систем их функциональным обязанностям.

13. Доступ лицам, не являющимся работниками Банка (далее – третьи лица), к информационным активам Банка предоставляется на период и в объеме, необходимых для проведения работ на основании соответствующего соглашения/договора, включающего условия о соблюдении требований к информационной безопасности, за исключением случаев, предусмотренных законодательством Республики Казахстан. В соглашениях/договорах, заключаемых с третьими лицами, содержатся положения о конфиденциальности, условия о возмещении ущерба, возникшего вследствие нарушения информационной безопасности, а также сбоев в работе информационных систем и нарушения их безопасности, вызванных действием или бездействием третьих лиц.

5. Требования к осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности

14. Банк обеспечивает создание структурного подразделения по реагированию на инциденты информационной безопасности – службу реагирования на инциденты информационной безопасности.

15. Банк обеспечивает надлежащий мониторинг деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности.

6. Требования к осуществлению сбора, консолидации и хранения информации об инцидентах информационной безопасности

16. Банк обеспечивает наличие документов, сведений и фактов, подтверждающих реализацию порядка реагирования на инциденты информационной безопасности, а также учет, хранение, консолидацию, систематизацию, целостность и сохранность информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах, о результатах внутреннего расследования инцидентов информационной безопасности и материалов расследования на бумажном носителе и (или) в электронном виде.

7. Требования к проведению анализа информации об инцидентах информационной безопасности

17. Банк обеспечивает:

1) проведение анализа выявленных инцидентов информационной безопасности и нанесенного ими ущерба для рассмотрения коллегиальным органом Банка, с целью оценки рисков информационной безопасности, корректировки методов и средств обеспечения информационной безопасности, изменения бизнес-процессов Банка;

2) оценку эффективности с целью корректировки процесса реагирования на инциденты информационной безопасности с использованием метрик процесса реагирования на инциденты информационной безопасности;

3) пересмотр метрик процесса реагирования на инциденты информационной безопасности с учетом результата оценки эффективности процесса реагирования на инциденты информационной безопасности;

4) пересмотр перечня событий информационной безопасности, подлежащих мониторингу, источников событий, периодичности, порядка и методов мониторинга событий информационной безопасности.

8. Ответственность работников Банка за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей

18. Участниками СУИБ Банка являются:

1) Совет Директоров;

2) Правление;

3) коллегиальный орган, уполномоченный принимать решения по задачам обеспечения информационной безопасности (далее – УКО);

4) подразделение по информационной безопасности;

5) подразделение по информационным технологиям;

6) подразделение по безопасности;

7) подразделение по работе с персоналом;

8) юридическое подразделение;

9) подразделение по комплаенс-контролю;

10) подразделение внутреннего аудита;

11) подразделение по управлению рисками информационных технологий и информационной безопасности;

12) бизнес-владельцы информационных систем и подсистем;

13) руководители структурных подразделений;

14) работники структурных подразделений.

19. Совет директоров утверждает политику информационной безопасности и перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну, и порядок работы с защищаемой информацией. Совет директоров при формировании бюджета учитывает потребности в ресурсах для обеспечения информационной безопасности Банка.

20. Правление утверждает внутренние нормативные документы, регламентирующие процесс управления информационной безопасностью, программу обучения и план проведения тестирования работников на знание требований внутренних нормативных документов по информационной безопасности, порядок и периодичность пересмотра которых определяется внутренними документами Банка.

21. Правление обеспечивает наличие УКО по принятию решений по вопросам обеспечения информационной безопасности, который действует в рамках полномочий, предоставленных Правлением.

22. Подразделение по информационной безопасности в целях обеспечения конфиденциальности, целостности и доступности информации Банка осуществляет следующие функции:

1) организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности подразделений Банка по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

2) разрабатывает политику информационной безопасности Банка;

3) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности Банка;

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

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

6) осуществляет анализ информации об инцидентах информационной безопасности;

7) подготавливает предложения для принятия Комитетом по информационной безопасности решения по вопросам информационной безопасности;

8) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности Банка, а

также предоставление доступа к ним;

9) определяет требования информационной безопасности по использованию привилегированных учетных записей;

10) обеспечивает проведение мероприятий по повышению осведомленности работников Банка в области информационной безопасности;

11) осуществляет мониторинг состояния системы управления информационной безопасностью Банка;

12) осуществляет информирование руководства Банка о состоянии системы управления информационной безопасностью Банка;

13) проводит оценку рисков информационной безопасности;

14) разрабатывает меры по обработке рисков информационной безопасности и предоставляет отчетность по их реализации в подразделение по управлению рисками информационных технологий и информационной безопасности;

15) подготавливает и предоставляет отчетность о реализации существенных рисков информационной безопасности в подразделение по управлению рисками информационных технологий и информационной безопасности, а также об устранении их последствий;

16) разрабатывает план мероприятий по реализации стратегии Банка в части обеспечения информационной безопасности, который раскрывает, но, не ограничиваясь, следующее:

- определение потребностей в ресурсах, в том числе определение бюджета, связанного с реализацией мер, направленных на управление рисками информационной безопасности;
- описание требуемых мероприятий в области информационной безопасности с указанием сроков и ответственных исполнителей за их реализацию.

23. Подразделение по информационным технологиям 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 информационных систем, не относящимися к Подразделению по информационным технологиям;

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

4) 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 внутренними документами Банка;

5) обеспечивает соблюдение требований информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем.

24. Подразделение по безопасности осуществляет следующие функции:

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

2) проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз информационной безопасности при приеме на работу и увольнении работников Банка.

25. Подразделение по управлению персоналом осуществляет следующие функции:

1) обеспечивает подписание работниками Банка, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации;

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

3) уведомляет уполномоченный орган о назначении и увольнении работников подразделения по информационной безопасности.

26. Юридическое подразделение осуществляет правовую экспертизу внутренних нормативных документов Банка по вопросам обеспечения информационной безопасности.

27. Подразделение по комплаенс-контролю совместно с Юридическим подразделением определяет виды информации, подлежащие включению в перечень защищаемой информации, предусмотренной пунктом 19 настоящей Политики.

28. Подразделение внутреннего аудита проводит оценку состояния системы управления информационной безопасностью Банка в соответствии с внутренними нормативными документами Банка, регламентирующими организацию системы внутреннего аудита Банка.

29. Подразделение по управлению рисками информационных технологий и информационной безопасности осуществляет функции, предусмотренные Правилами формирования системы управления рисками и внутреннего контроля для банков второго уровня, утвержденными Постановление Правления Национального Банка Республики Казахстан от 12 ноября 2019 года №188 «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан».

30. Бизнес-владельцы информационных систем или подсистем:

1) отвечают за соблюдение требований к информационной безопасности при создании, внедрении, модификации, эксплуатации информационных систем и предоставлении продуктов и услуг клиентам и подразделениям Банка, а также при интеграции информационных систем с внешними информационными системами, включая информационные системы государственных органов;

2) формируют и поддерживают актуальность матриц доступа к информационным системам.

31. Руководители структурных подразделений Банка:

1) обеспечивают ознакомление работников с внутренними нормативными документами Банка, содержащими требования к информационной безопасности;

2) несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях;

3) обеспечивают заключение соглашений о неразглашении конфиденциальной информации и включение условий об обеспечении информационной безопасности в соглашения, договоры на оказание услуг/выполнение работ в случаях, когда подразделение Банка выступает инициатором заключения таких соглашений, договоров.

32. Работники структурных подразделений Банка:

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

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

3) извещают своего непосредственного руководителя и подразделение по информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными активами.

33. Несоблюдение порядка и правил использования информационных ресурсов и принятых в Банке мер обеспечения информационной безопасности при исполнении работниками возложенных функциональных обязанностей, влечет за собой ответственность в соответствии с действующим законодательством Республики Казахстан и внутренними нормативными документами Банка.

9. Обеспечение информационной безопасности в Дочерних компаниях Банка

34. В целях обеспечения кураторства и построения взаимодействия между подразделением по информационной безопасности и Дочерними компаниями АО «Банк ЦентрКредит» (далее – ДК) в части обеспечения необходимого и достаточного уровня

информационной безопасности в ДК Банка, подразделение по информационной безопасности осуществляет следующие функции координации деятельности ДК:

1) определяет требования по обеспечению информационной безопасности;

2) согласовывает внутренние нормативные документы в части информационной безопасности;

3) рекомендует и согласовывает внедрение организационных мер и программно-технических средств обеспечения информационной безопасности;

4) согласовывает ежегодные планы мероприятий и бюджет ДК в области обеспечения информационной безопасности;

5) оказывает консультационную поддержку в части развития системы управления информационной безопасностью, а также в вопросах обучения и профессионального развития работников ДК, ответственных за обеспечение информационной безопасности;

6) оказывает содействие в прохождении внешних проверок и аудитов в области обеспечения информационной безопасности;

7) проводит проверки состояния информационной безопасности, запрашивает информацию, согласовывает планы мероприятий по устранению выявленных замечаний, требует их исполнения;

8) участвует в профильных комитетах ДК (при наличии).

10. Требования к компетенциям руководителей и работников, ответственных за обеспечение информационной безопасности

35. Руководители и работники, ответственные за обеспечение информационной безопасности, обладают соответствующими компетенциями и опытом работы в сфере защиты информации.

36. Детальные требования к квалификации руководителей и работников, ответственных за обеспечение информационной безопасности, отражены в соответствующих квалификационных требованиях и должностных инструкциях.

37. Руководители и работники, ответственные за обеспечение информационной безопасности повышают квалификацию в соответствии с требованиями Постановления Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 21 сентября 2020 года № 89.

11. Заключительные положения

38. Все вопросы, не урегулированные настоящей Политикой, решаются в соответствии с законодательством Республики Казахстан, внутренними нормативными документами и решениями уполномоченных органов Банка, а также сложившейся практикой деятельности Банка.

39. Политика вступает в силу с даты утверждения Советом Директоров Банка и прекращает свое действие с момента признания ее утратившей силу Советом Директоров Банка.

40. Если в результате изменения законодательства Республики Казахстан отдельные нормы настоящей Политики вступают в противоречие с действующим законодательством Республики Казахстан, то до момента внесения изменений в Политику, необходимо руководствоваться действующим законодательством Республики Казахстан и Политикой в части, не противоречащей законодательству Республики Казахстан.

41. Пересмотр настоящей Политики осуществляется не реже одного раза в год.