Утверждено
Общим собранием участников
КБ «Максима» (ООО)
Протокол №145
От «09» января 2017г.

Политика информационной безопасности КБ «Максима» (ООО)

(новая редакция)

Москва, 2017г.

1. Содержание

2. Область применения

Настоящая политика распространяется на все подразделения КБ «Максима» (ООО) и устанавливает основные высокоуровневые положения по обеспечению информационной безопасности в КБ «Максима» (ООО).

Положения настоящей Политики обязательны для исполнения.

3. Нормативное регулирование

3.1. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ;

3.2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ.

3.3. «Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств" СТО БР ИББС-1.3-2016"

3.4. Постановление Правительства РФ от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3.5. "Рекомендации в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности" РС БР ИББС-2.5-2014"

3.6. Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях БС РФ, разработанные совместно Банком России, АРБ и Ассоциацией региональных банков России (Ассоциацией «Россия»);

3.7. «Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0» РС БР ИББС-2.1-2007» (приняты и введены в действие Распоряжением ЦБ РФ от 28.04.2007 № Р-347).

3.8. "Рекомендации в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации" РС БР ИББС-2.9-2016"

4. Термины и определения[1]

4.1. Стандарт - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и

[1] Термины, установленные стандартом, применяются во всех видах документации и во всех видах деятельности по обеспечению ИБ в рамках Комплекса БР ИББС.

характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг[2].

4.2. Рекомендации в области стандартизации - документ, содержащий советы организационно-методического характера, которые касаются проведения работ по стандартизации и способствуют применению основополагающего стандарта.

4.3. Комплекс БР ИББС - взаимоувязанная совокупность документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

4.4. Менеджмент - скоординированная деятельность по руководству и управлению.

4.5. Система - множество (совокупность) материальных объектов (элементов) любой, в том числе различной физической, природы и информационных объектов, взаимодействующих между собой для достижения общей цели, обладающее системным свойством (свойствами)[3].

4.6. Информация - сведения (сообщения, данные) независимо от формы их представления.

4.7. Инфраструктура - комплекс взаимосвязанных обслуживающих структур, составляющих основу для решения проблемы (задачи).

4.8. Информационная инфраструктура - система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия. Включает совокупность информационных центров, банков данных и знаний, систем связи; обеспечивает доступ потребителей к информационным ресурсам.

4.9. Документ - зафиксированная на материальном носителе[4] информация с реквизитами, позволяющими ее идентифицировать.

4.10. Процесс - совокупность взаимосвязанных ресурсов и деятельности, преобразующая входы в выходы.

4.11. Технология - совокупность взаимосвязанных методов, способов, приемов предметной деятельности.

4.12. Технологический процесс - процесс, реализующий некоторую технологию.

4.13. Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

4.14. Авторизация - предоставление прав доступа.

4.15. Идентификация - процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

4.16. Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

4.17. Регистрация - фиксация данных о совершенных действиях (событиях).

4.18. Роль - заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом[5] и объектом[6].

---

[2] Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

[3] Системным свойством (свойствами) является свойство, которое не имеет ни один из элементов и ни одно из подмножеств элементов при любом способе членения. Системное свойство не выводимо непосредственно из свойств элементов и частей.

[4] Под материальным носителем подразумевается изделие (материал), на котором записана информация и которое обеспечивает возможность сохранения этой информации и снятие ее копий, например, бумага, магнитная лента или карта, магнитный или лазерный диск, фотопленка и т.п.

[5] К субъектам относятся лица из числа руководителей организации банковской системы Российской Федерации, ее персонала, клиентов или инициируемые от их имени процессы по выполнению действий над объектами.

4.19. Угроза - опасность, предполагающая возможность потерь (ущерба).

4.20. Риск - мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

4.21. Актив - все, что имеет ценность для КБ «Максима» (ООО) и находится в ее распоряжении. К активам могут относиться:

- работники (персонал), финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.;
- различные виды банковской информации – платежная, финансово-аналитическая, служебная, управляющая, персональные данные и пр.;
- банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы);
- банковские продукты и услуги, предоставляемые клиентам.

4.22. Информационный актив - информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для КБ «Максима» (ООО); находящаяся в распоряжении КБ «Максима» (ООО) и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

4.23. Классификация информационных активов - разделение существующих информационных активов КБ «Максима» (ООО) по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств ИБ.

4.24. Объект среды информационного актива - материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.).

4.25. Ресурс - актив КБ «Максима» (ООО), который используется или потребляется в процессе выполнения некоторой деятельности.

4.26. Банковский технологический процесс - технологический процесс, реализующий операции[7] по изменению и (или) определению состояния активов КБ «Максима» (ООО), используемых при функционировании или необходимых для реализации банковских услуг. В зависимости от вида деятельности выделяют: банковский платежный технологический процесс, банковский информационный технологический процесс и др.

4.27. Банковский платежный технологический процесс - часть банковского технологического процесса, реализующая банковские операции над информационными активами КБ «Максима» (ООО), связанные с перемещением денежных средств с одного счета на другой и (или) контролем данных операций.

4.28. Банковский информационный технологический процесс - часть банковского технологического процесса, реализующая операции по изменению и (или) определению состояния информационных активов, необходимых для функционирования КБ «Максима» (ООО) и не являющихся платежной информацией[8].

4.29. Платежная информация – информация, содержащаяся в документах, на основании которой совершаются операции, связанные с перемещением денежных средств с одного счета на другой.

4.30. Автоматизированная банковская система - автоматизированная система, реализующая технологию выполнения функций КБ «Максима» (ООО).

---

[6] Объектами могут быть аппаратное средство, программное средство, программно-аппаратное средство, информационный ресурс, услуга, процесс, система, над которыми выполняются действия.

[7] Операции над активами организации банковской системы Российской Федерации могут выполняться вручную или быть автоматизированными, например, с помощью автоматизированных банковских систем.

[8] Неплатежная информация, необходимая для функционирования организации банковской системы Российской Федерации, может включать в себя, например, данные статистической отчетности и внутрихозяйственной деятельности, аналитическую, финансовую, справочную информацию.

4.31. Комплекс средств автоматизации автоматизированной банковской системы - совокупность всех компонентов автоматизированной банковской системы КБ «Максима» (ООО), за исключением людей.

4.32. Безопасность - состояние защищенности интересов (целей) КБ «Максима» (ООО).

4.33. Информационная безопасность (ИБ) - безопасность, связанная с угрозами в информационной сфере[9]. Защищенность достигается обеспечением совокупности свойств ИБ – доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств ИБ определяется ценностью указанных активов для интересов (целей) КБ «Максима» (ООО).

4.34. Доступность информационных активов - свойство ИБ КБ «Максима» (ООО), состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

4.35. Целостность информационных активов - свойство ИБ КБ «Максима» (ООО) сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах.

4.36. Конфиденциальность информационных активов - свойство ИБ КБ «Максима» (ООО), состоящее в том, что обработка, хранение и передача информационных активов осуществляются таким образом, что информационные активы доступны только авторизованным пользователям, объектам системы или процессам.

4.37. Система информационной безопасности (СИБ) - совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

4.38. Система менеджмента информационной безопасности (СМИБ) - часть менеджмента КБ «Максима» (ООО), предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

4.39. Система обеспечения информационной безопасности (СОИБ) - совокупность СИБ и СМИБ КБ «Максима» (ООО).

4.40. Область действия СОИБ - совокупность информационных активов и элементов информационной инфраструктуры КБ «Максима» (ООО).

4.41. Осознание необходимости обеспечения ИБ - понимание руководством КБ «Максима» (ООО) необходимости самостоятельно на основе принятых в этой организации ценностей и накопленных знаний формировать и учитывать в рамках основной деятельности (бизнеса) прогноз результатов от деятельности по обеспечению ИБ, а также поддерживать эту деятельность адекватно прогнозу.

4.42. Защитная мера - сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения ИБ КБ «Максима» (ООО).

4.43. Угроза ИБ - угроза нарушения свойств ИБ – доступности, целостности или конфиденциальности информационных активов КБ «Максима» (ООО).

4.44. Уязвимость ИБ - слабое место в инфраструктуре КБ «Максима» (ООО), включая СОИБ, которое может быть использовано для реализации или способствовать реализации угрозы ИБ.

4.45. Ущерб - утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры КБ «Максима» (ООО) или другой вред активам и (или) инфраструктуре

---

[9] Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

КБ «Максима» (ООО), наступивший в результате реализации угроз ИБ через уязвимости ИБ.

4.46. Инцидент ИБ - событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию[10] угрозы ИБ.

4.47. Нарушитель ИБ - субъект, реализующий угрозы ИБ КБ «Максима» (ООО), нарушая предоставленные ему полномочия по доступу к активам КБ «Максима» (ООО) или по распоряжению ими.

4.48. Модель нарушителя ИБ - описание и классификация нарушителей ИБ, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз ИБ со стороны указанных нарушителей.

4.49. Модель угроз ИБ - описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.

4.50. Риск нарушения ИБ - риск, связанный с угрозой ИБ.

4.51. Оценка риска нарушения ИБ - систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения ИБ, связанных с использованием информационных активов КБ «Максима» (ООО) на всех стадиях их жизненного цикла.

4.52. Обработка риска нарушения ИБ - процесс выбора и осуществления защитных мер, снижающих риск нарушения ИБ, или мер по переносу, принятию или уходу от риска.

4.53. Остаточный риск нарушения ИБ - риск, остающийся после обработки риска нарушения ИБ.

4.54. Допустимый риск нарушения ИБ - риск нарушения ИБ, предполагаемый ущерб от которого КБ «Максима» (ООО) в данное время и в данной ситуации готов принять.

4.55. Документация - совокупность взаимосвязанных документов, объединенных общей целевой направленностью.

4.56. План работ по обеспечению ИБ - документ, устанавливающий перечень намеченных к выполнению работ или мероприятий по обеспечению ИБ КБ «Максима» (ООО), их последовательность, объем (в той или иной форме), сроки выполнения, ответственных лиц и конкретных исполнителей.

4.57. Свидетельства выполнения деятельности по обеспечению ИБ - документ или элемент документа, содержащий достигнутые результаты (промежуточные или окончательные), относящиеся к обеспечению ИБ КБ «Максима» (ООО).

4.58. Частная политика ИБ - документация, детализирующая положения настоящей политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности КБ «Максима» (ООО).

4.59. Мониторинг - постоянное наблюдение за объектами и субъектами, влияющими на ИБ КБ «Максима» (ООО), а также сбор, анализ и обобщение результатов наблюдений.

4.60. Аудит ИБ - систематический, независимый и документируемый процесс получения свидетельств деятельности КБ «Максима» (ООО) по обеспечению ИБ, установления степени выполнения в КБ «Максима» (ООО) критериев ИБ, а также допускающий возможность формирования профессионального аудиторского суждения о

[10] Реализация угрозы ИБ – реализация нарушения свойств ИБ информационных активов организации банковской системы Российской Федерации. Нарушение может вызываться источниками угроз ИБ: либо случайными факторами (ошибкой персонала, неправильным функционированием технических средств, природными факторами, например, пожаром или наводнением), либо преднамеренными действиями, приводящими к нарушению доступности, целостности или конфиденциальности информационных активов.

состоянии ИБ КБ «Максима» (ООО). Аудит ИБ выполняется работниками организации, являющейся внешней по отношению к КБ «Максима» (ООО).

4.61. Критерии оценки (аудита) ИБ - совокупность требований в области ИБ, определенных стандартом Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» или его частью.

4.62. Свидетельства оценки соответствия (аудита) ИБ - записи, изложение фактов или другая информация, которые имеют отношение к критериям оценки соответствия (самооценки соответствия, аудита) ИБ и могут быть проверены. Свидетельства оценки соответствия (самооценки соответствия, аудита) ИБ могут быть качественными или количественными.

4.63. Выводы аудита ИБ - результат оценки собранных свидетельств аудита ИБ.

4.64. Заключение по результатам аудита ИБ (аудиторское заключение) - качественная или количественная оценка соответствия установленным критериям аудита ИБ, представленная аудиторской группой после рассмотрения всех выводов аудита ИБ в соответствии с целями аудита ИБ.

5. Обозначения и сокращения

АБС – автоматизированная банковская система;
БС – банковская система;
ЖЦ – жизненный цикл;
ИБ – информационная безопасность;
ИСПДн – информационная система персональных данных;
НСД – несанкционированный доступ;
НРД – нерегламентированные действия в рамках предоставленных полномочий;
ПДн – персональные данные;
РФ – Российская Федерация;
СКЗИ – средство криптографической защиты информации;
СМИБ – система менеджмента информационной безопасности;
СИБ – система информационной безопасности;
СОИБ – система обеспечения информационной безопасности;
ЭВМ – электронная вычислительная машина;
ЭЦП – электронная цифровая подпись.

6. Цели и задачи обеспечения ИБ в КБ «Максима» (ООО)

6.1. Основные цели обеспечения ИБ в КБ «Максима» (ООО):
- развитие и укрепление КБ «Максима» (ООО), поддержание его стабильности;
- повышение доверия к КБ «Максима» (ООО);
- достижение адекватности мер защиты реальным угрозам ИБ;
- предотвращение и (или) снижение ущерба от инцидентов ИБ.

6.2. Основные задачи обеспечения ИБ в КБ «Максима» (ООО):
- установление единых требований по обеспечению ИБ КБ «Максима» (ООО);
- повышение эффективности мероприятий по обеспечению и поддержанию ИБ КБ «Максима» (ООО).

7. Стратегия обеспечения ИБ КБ «Максима» (ООО)

Стратегия обеспечения ИБ КБ «Максима» (ООО) заключается в:

- эффективном использовании по имеющемуся плану заранее разработанных мер по обеспечению ИБ, противостоящих атакам злоумышленников,
- в регулярном пересмотре моделей и политик ИБ, а также корректировке СОИБ.

8. СОИБ КБ «Максима» (ООО)

8.1. Совокупность защитных мер, реализующих обеспечение ИБ КБ «Максима» (ООО), и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение, составляет СИБ КБ «Максима» (ООО).

Совокупность процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов, составляет СМИБ КБ «Максима» (ООО).

Совокупность СИБ и СМИБ составляет СОИБ КБ «Максима» (ООО).

8.2. Процессы эксплуатации защитных мер функционируют в КБ «Максима» (ООО) в реальном времени. Совокупность защитных мер и процессов их эксплуатации обеспечивают текущий, требуемый уровень ИБ в условиях штатного функционирования, а также в условиях реализации угроз, учтенных в принятой Модели угроз и приводящих к возникновению:

- локальных инцидентов ИБ;
- широкомасштабных катастроф и аварий различной природы, последствия которых могут иметь отношение к ИБ КБ «Максима» (ООО).

8.3. Для поддержания системы защиты на должном уровне в качестве оперативной меры используется мониторинг событий и инцидентов в СИБ. Менеджмент событий и инцидентов безопасности, полученных в результате мониторинга, позволяет избежать деградации и обеспечить требуемый уровень безопасности активов.

Для оценки состояния ИБ защищаемого актива и выявления признаков деградации используемых защитных мер проводится оценка (самооценка) соответствия системы требованиям ИБ КБ «Максима» (ООО).

8.4. Для реализации и поддержания ИБ в КБ «Максима» (ООО) реализуются следующие группы процессов:

- планирование СОИБ КБ «Максима» (ООО) («планирование»);
- реализация СОИБ КБ «Максима» (ООО) («реализация»);
- мониторинг и анализ СОИБ КБ «Максима» (ООО) («проверка»);
- поддержка и улучшение СОИБ КБ «Максима» (ООО)(«совершенствование»).

Указанные группы процессов составляют СМИБ КБ «Максима» (ООО).

8.5. Постоянный анализ и изучение инфраструктуры КБ «Максима» (ООО) с целью выявления и устранения уязвимостей ИБ - основа эффективной работы СОИБ.

8.6. Менеджмент ИБ есть часть общего корпоративного менеджмента КБ «Максима» (ООО), которая ориентирована на содействие достижению целей деятельности КБ «Максима» (ООО) через обеспечение защищенности ее информационной сферы.

8.7. Группы процессов СМИБ КБ «Максима» (ООО) организуется в виде циклической модели Деминга «... - планирование - реализация - проверка - совершенствование - планирование -...» (Рисунок 1).

8.8. Основой для построения и корректировки СОИБ КБ «Максима» (ООО) являются требования законодательства Российской Федерации, нормативные акты Банка России, контрактные требования, а также условия ведения бизнеса, выраженные на основе идентификации информационных активов, построения модели нарушителей и угроз.

8.9. Руководство КБ «Максима» (ООО) инициирует, поддерживает и контролирует выполнение процессов СОИБ.

8.10. Для обеспечения ИБ и контроля за качеством обеспечения ИБ в КБ «Максима» (ООО) определяются роли, связанные с деятельностью по обеспечению ИБ.

Председатель Правления КБ «Максима» (ООО) осуществляет координацию своевременности и качества выполнения ролей, связанных с обеспечением ИБ.

Рисунок 1. СОИБ КБ «Максима» (ООО)

9. Область обеспечения ИБ в КБ «Максима» (ООО)

9.1. Область обеспечения ИБ в КБ «Максима» (ООО) включает в себя все ее информационные активы, поименованные в Описи защищаемых активов.

9.2. Опись защищаемых информационных активов составляется в разрезе типов информационных активов и классифицируется в соответствии с тяжестью последствий потери свойств ИБ информационных активов.

9.3. Выделяются следующие типы информационных активов:

9.3.1. Персональные данные:

9.3.1.1. Персональные данные, отнесенные в соответствии с Законом № 152-ФЗ «О персональных данных» к специальным категориям персональных данных;

9.3.1.2. Персональные данные, отнесенные в соответствии с Законом № 152-ФЗ «О персональных данных» к биометрическим персональным данным;

9.3.1.3. Персональные данные, отнесенные в соответствии с Законом № 152-ФЗ «О персональных данных» к общедоступным или обезличенным персональным данным;

9.3.1.4. Прочие персональные данные;

9.3.2. Платежная информация;

9.3.3. Прочие данные (кроме перечисленных выше), составляющие банковскую тайну;

9.3.4. Финансово-аналитическая информация:

9.3.4.1. Условия договоров с контрагентами;

9.3.4.2. Финансовая информация по КБ «Максима» (ООО);

9.3.4.3. Финансовая информация по клиентам КБ «Максима» (ООО);

9.3.4.4. Прочая аналитическая и финансовая информация, не находящаяся в открытом доступе;

9.3.4.5. Прочая аналитическая и финансовая информация, находящаяся в открытом доступе;

9.3.5. Служебная информация;

9.3.6. Управляющая информация:

9.3.6.1. Информация, зафиксированная во внутренних нормативных актах КБ «Максима» (ООО);

9.3.6.2. Решения органов управления, собственников;

9.3.6.3. Данные управленческого учета;

9.3.6.4. Сведения, полученные в ходе проведения проверок деятельности КБ «Максима» (ООО);

9.4. Классификация информационных активов по типам производится в соответствии с тяжестью последствий потери свойств ИБ информационных активов. Выделяются следующие классы информационных активов:

9.4.1. К1 – потеря свойств информационного актива может привести к невыполнению Банком требований законодательства, обязательств по договорам, к потере кредитной организацией деловой репутации и (или) к существенным материальным потерям. Активы существенны для обеспечения непрерывности бизнеса КБ «Максима» (ООО);

9.4.2. К2 – потеря свойств информационного актива приведет к нарушению бизнес-процессов КБ «Максима» (ООО) (восстановление которых потребует длительного времени, существенных материальных затрат и т.п.), но не повлечет нарушения требований законодательства, обязательств КБ «Максима» (ООО) по договорам. Активы существенны для обеспечения непрерывности бизнеса КБ «Максима» (ООО);

9.4.3. К3 – потеря свойств информационного актива не приведет к существенному нарушению бизнес-процессов КБ «Максима» (ООО).

9.5. Процедуры анализа и пересмотра области действия СОИБ, в частности, процедуры пересмотра при изменении перечня информационных активов (типов информационных активов), находящихся в области действия СОИБ, роли по определению и корректировке области действия СОИБ, по составлению и пересмотру области действия СОИБ, ответственные за выполнение указанных ролей определены в «Порядке определения, анализа и пересмотра области действия СОИБ».

10. Модель угроз и нарушителей

10.1. Модель угроз и нарушителей является основным инструментом КБ «Максима» (ООО) при развертывании, поддержании и совершенствовании СОИБ.

10.2. Деятельность банка поддерживается входящей в ее состав информационной инфраструктурой, которая обеспечивает реализацию банковских технологий и может быть представлена в виде иерархии следующих основных уровней:

- физического (линии связи, аппаратные средства и пр.);
- сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и пр.);
- сетевых приложений и сервисов;
- операционных систем (ОС);
- систем управления базами данных (СУБД);
- банковских технологических процессов и приложений;
- бизнес-процессов организации.

10.3. На каждом из уровней угрозы и их источники (в т.ч. злоумышленники), методы и средства защиты и подходы к оценке эффективности являются различными.

10.4. Главной целью злоумышленника является получение контроля над информационными активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов, например путем раскрытия конфиденциальной банковской аналитической информации, более эффективно для злоумышленника и опаснее для собственника, чем нападение, осуществляемое через иные уровни, требующее специфических опыта, знаний и ресурсов (в т.ч. временных) и поэтому менее эффективно по соотношению "затраты / получаемый результат".

Другой целью злоумышленника может являться нарушение функционирования бизнес-процессов банка, например, посредством распространения вредоносных программ или нарушения правил эксплуатации ЭВМ или их сетей.

10.5. Основными источниками угроз ИБ являются:

- неблагоприятные события природного, техногенного и социального характера;
- террористы и криминальные элементы;
- зависимость от поставщиков/провайдеров/партнеров/клиентов;
- сбои, отказы, разрушения/повреждения программных и технических средств;
- работники банка, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);
- работники банка, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками организации БС РФ, но осуществляющие попытки НСД и НРД (внешние нарушители ИБ);
- несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

10.6. Наиболее актуальные источники угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений:

- внешние нарушители ИБ: лица, разрабатывающие/распространяющие вирусы и другие вредоносные программные коды; лица, организующие DoS, DDoS и иные виды атак; лица, осуществляющие попытки НСД и НРД;
- внутренние нарушители ИБ: персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы серверов, сетевых приложений и т.п.;
- комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно;
- сбои, отказы, разрушения/повреждения программных и технических средств.

10.7. Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных, банковских технологических процессов:

- внутренние нарушители ИБ: администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.;

- комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие в сговоре.

10.8. Наиболее актуальные источники угроз на уровне бизнес-процессов:

- внутренние нарушители ИБ: авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.;
- комбинированные источники угроз: внешние нарушители ИБ (например, конкуренты) и внутренние, действующие в сговоре;
- несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

10.9. Процедуры анализа и пересмотра действующей Модели угроз, роли по анализу и пересмотру, а также ответственные за исполнение указанных ролей определены в «Порядке анализа и пересмотра Модели угроз и нарушителей КБ «Максима» (ООО)».

11. Риски нарушения ИБ в КБ «Максима» (ООО)

11.1. Риски нарушения ИБ выражаются в возможности потери состояния защищенности интересов (целей) КБ «Максима» (ООО) в информационной сфере и возникновения ущерба ее бизнесу или убытков.

Потеря состояния защищенности интересов (целей) КБ «Максима» (ООО) в информационной сфере заключается в утрате свойств доступности, целостности или конфиденциальности информационных активов, утрате заданных целями бизнеса параметров или доступности сервисов инфраструктуры КБ «Максима» (ООО).

Риски нарушения ИБ согласованы и иерархически связаны с рисками основной (бизнес) деятельности КБ «Максима» (ООО) через возможный ущерб.

11.2. Уязвимость ИБ создает предпосылки к реализации угрозы через нее (инцидент ИБ). Реализация угрозы нарушения ИБ приводит к утрате защищенности интересов (целей) КБ «Максима» (ООО) в информационной сфере, в результате чего КБ «Максима» (ООО) наносится ущерб. Тяжесть ущерба совместно с вероятностью приводящего к нему инцидента ИБ определяют величину риска.

11.3. Анализ и оценка рисков нарушения ИБ в КБ «Максима» (ООО) основывается на идентификации ее активов, на их ценности для целей и задач КБ «Максима» (ООО), на принятой Модели угроз и нарушителей ИБ.

Оценка рисков нарушения ИБ проводится для свойств ИБ всех типов информационных активов области действия СОИБ.

Методика определения риска нарушения ИБ для выделенных типов информационных активов определены в «Методике оценки рисков нарушения ИБ в КБ «Максима» (ООО)».

11.4. Критерий принятия рисков:

- риск нарушения ИБ принимается КБ «Максима» (ООО), если соответствующий уровень риска не превосходит установленный допустимый уровень;
- иначе риск не принимается.

11.5. Уровень допустимого риска в КБ «Максима» (ООО) устанавливается равным.

11.6. Уровень защищенности интересов (целей) КБ «Максима» (ООО) определяется:

- величиной принятых ею остаточных рисков,
- эффективностью работ по поддержанию принятых рисков на допустимом, низком (остаточном) уровне.

11.7. Периодичность проведения оценки рисков нарушения ИБ и порядок их обработки определен в «Порядке обработки рисков нарушения ИБ в КБ «Максима» (ООО)».

12. Правила, требования и руководящие принципы в области ИБ

Настоящая Политика устанавливает высокоуровневые правила и требования в области ИБ, представляющие особую важность для КБ «Максима» (ООО).

Правила и требования, развивающие соответствующие правила и требования настоящей Политики, приводятся в частных политиках ИБ (Политика обеспечения ИБ КБ «Максима» (ООО) при назначении и распределении ролей и обеспечении доверия к персоналу, Политика по обеспечению ИБ при управлении доступом и регистрации, Политика по обеспечению ИБ КБ «Максима» (ООО) средствами антивирусной защиты, Политика обеспечения ИБ КБ «Максима» (ООО) при использовании СКЗИ), соответствующих порядках, положениях, инструкциях и методиках.

12.1. Общие требования по обеспечению ИБ при назначении и распределении ролей и обеспечении доверия к персоналу

12.1.1. В КБ «Максима» (ООО) выделяются и документально определяются роли ее работников.

12.1.2. Формирование ролей осуществляется на основании существующих бизнес-процессов КБ «Максима» (ООО) и проводиться с целью исключения концентрации полномочий и снижения риска инцидентов ИБ, связанных с потерей информационными активами свойств доступности, целостности или конфиденциальности.

Формирование ролей не должно выполняться по принципу фиксации фактически сложившихся прав и полномочий персонала КБ «Максима» (ООО).

12.1.3. Роли персонифицируются с установлением ответственности за их выполнение. Ответственность документально фиксируется в должностных инструкциях.

12.1.4. С целью снижения рисков нарушения ИБ в рамках одной роли не совмещаются следующие функции:

- разработки и сопровождения системы/ПО,
- их разработки и эксплуатации,
- сопровождения и эксплуатации,
- администратора системы и администратора ИБ,
- выполнения операций в системе и контроля их выполнения.

12.1.5. В КБ «Максима» (ООО) документально определяются и выполняются процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющих получить контроль над защищаемым информационным активом КБ «Максима» (ООО).

12.1.6. В КБ «Максима» (ООО) документально определяются процедуры приема на работу, влияющую на обеспечение ИБ, включающие:

- проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов;
- проверку в части профессиональных навыков и оценку профессиональной пригодности.

Указанные процедуры предусматривают документальную фиксацию результатов проводимых проверок.

12.1.7. В КБ «Максима» (ООО) проводятся регулярные проверки (с документальной фиксацией результатов) в части профессиональных навыков и оценки профессиональной пригодности работников, а также внеплановой проверки (с документальной фиксацией результатов) - при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии.

12.1.8. Все работники КБ «Максима» (ООО) дают письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов.

При взаимодействии с внешними организациями и клиентами требования по обеспечению ИБ регламентируются положениями, включаемыми в договоры (соглашения) с ними.

12.1.9. Обязанности персонала по выполнению требований по обеспечению ИБ должны включаются в трудовые контракты (соглашения, договоры) и (или) должностные инструкции.

Невыполнение работниками КБ «Максима» (ООО) требований по обеспечению ИБ приравнивается к невыполнению должностных обязанностей и приводят как минимум к дисциплинарной ответственности.

12.2. Общие требования по обеспечению информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла.

12.2.1. КБ «Максима» (ООО) рассматривает следующие общие стадии модели ЖЦ АБС:

1) разработка технических заданий;
2) проектирование;
3) создание и тестирование;
4) приемка и ввод в действие;
5) эксплуатация;
6) сопровождение и модернизация;
7) снятие с эксплуатации.

В случае разработки АБС в КБ «Максима» (ООО) рассматриваются все стадии ЖЦ АБС, а в случае приобретения готовых АБС - стадии 4 - 7 ЖЦ АБС.

12.2.2. ИБ АБС обеспечивается на всех стадиях ЖЦ АБС, автоматизирующих банковские технологические процессы, с учетом интересов всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений КБ «Максима» (ООО)).

12.2.3. Разработка технических заданий и приемка АБС осуществляются в КБ «Максима» (ООО) по согласованию и при участии сотрудника службы ИБ.

12.2.4. Ввод в действие, эксплуатация и сопровождение (модернизация), снятие с эксплуатации АБС осуществляется под контролем сотрудника службы ИБ.

12.2.5. Привлекаемые для разработки и (или) производства средств и систем защиты АБС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

12.2.6. Разрабатываемые АБС и (или) их компоненты должны быть снабжены документацией, содержащей описание реализованных защитных мер, в том числе в отношении угроз ИБ (источников угроз), описанных в модели угроз КБ «Максима»

(ООО). Приобретаемые КБ «Максима» (ООО) готовые АБС и (или) их компоненты также должны быть снабжены указанной документацией.

Также документация на разрабатываемые АБС или приобретаемые готовые АБС и их компоненты должна содержать описание реализованных защитных мер, предпринятых разработчиком относительно безопасности разработки и безопасности поставки.

Договор (контракт) о разработке АБС или поставке готовых АБС и их компонентов должен включать (если возможно) положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных положений должен быть приобретен полный комплект рабочей конструкторской документации, обеспечивающий возможность сопровождения АБС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, КБ «Максима» (ООО) производит оценку риска нарушения ИБ и его допустимости.

12.2.7. При разработке технических заданий на системы дистанционного банковского обслуживания должно быть учтено, что защита данных должна обеспечиваться в условиях:

- попыток доступа к банковской информации анонимных, неавторизованных злоумышленников при использовании сетей общего пользования;
- возможности ошибок авторизованных пользователей систем;
- возможности ненамеренного или неадекватного использования конфиденциальных данных авторизованными пользователями.

12.2.8. На стадии тестирования должны обеспечиваться анонимность данных и проверка адекватности разграничения доступа.

12.2.9. На стадии эксплуатации АБС осуществляется контроль работоспособности (функционирования, эффективности) реализованных в АБС защитных мер. Результаты выполнения контроля документируются.

12.2.10. На стадии сопровождения (модернизации) осуществляются процедуры контроля, обеспечивающие защиту от:

- умышленного несанкционированного раскрытия, модификации или уничтожения информации;
- неумышленной модификации, раскрытия или уничтожения информации;
- отказа в обслуживании или ухудшения обслуживания.

Результаты выполнения контроля документируются.

12.2.11. На стадии сопровождения (модернизации) при любом внесении изменения в АБС проводятся процедуры проверки функциональности, результаты которой фиксируются документально.

12.2.12. На стадии снятия с эксплуатации осуществляются процедуры, обеспечивающие удаление информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности КБ «Максима» (ООО), и информации, используемой средствами обеспечения ИБ, из постоянной памяти АБС и с внешних носителей, за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами. Результаты выполнения процедур фиксируются документально.

12.3. Общие требования по обеспечению информационной безопасности при управлении доступом и регистрации

12.3.1. Права доступа работников и клиентов КБ «Максима» (ООО) к информационным активам фиксируются документально.

12.3.2. В составе АБС применяются встроенные защитные меры, а также сертифицированные или разрешенные руководством КБ «Максима» (ООО) к применению средства защиты информации от НСД и НРД.

12.3.3. В КБ «Максима» (ООО) выполняются и контролируются установленные процедуры идентификации, аутентификации, авторизации; управления доступом; контроля целостности; регистрации событий и действий.

Результаты контроля процедур документируются.

12.3.4. В КБ «Максима» (ООО) проводятся процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные операции и транзакции. Если возможно, для проведения процедур мониторинга и анализа данных регистрации, действий и операций используются специализированные программные и (или) технические средства. Указанные процедуры мониторинга и анализа применяются на регулярной основе ко всем выполненным операциям и транзакциям.

12.3.5. Доступ работников КБ «Максима» (ООО) в помещения, в которых размещаются объекты среды информационных активов, ограничен. Осуществляется контроль выполнения установленного порядка доступа, результаты которого документируются.

12.3.6. Используемые в КБ «Максима» (ООО) АБС, в том числе системы дистанционного банковского обслуживания, должны обеспечивать среди прочего возможность регистрации:

- операций с данными о клиентских счетах, включая операции открытия, модификации и закрытия клиентских счетов;
- проводимых транзакций, имеющих финансовые последствия;
- операций, связанных с назначением и распределением прав пользователей.

12.3.7. Системы дистанционного банковского обслуживания в КБ «Максима» (ООО) должны реализовывать защитные меры, обеспечивающие невозможность отказа от авторства проводимых клиентами операций и транзакций.

12.3.8. При заключении договоров со сторонними организациями, если возможно, юридически оформляются договоренности, предусматривающие необходимый уровень взаимодействия, в случае выхода инцидента ИБ за рамки отдельной КБ «Максима» (ООО).

12.3.9. В системах дистанционного банковского обслуживания КБ «Максима» (ООО) должны быть реализованы механизмы информирования (регулярного, непрерывного или по требованию) клиентов обо всех операциях, совершаемых от их имен.

12.3.10. В КБ «Максима» (ООО) применяются защитные меры, направленные на обеспечение защиты от НСД и НРД, повреждения или нарушения целостности информации, необходимой для регистрации, идентификации, аутентификации и (или) авторизации клиентов и работников КБ «Максима» (ООО). Все попытки НСД и НРД к такой информации регистрируются.

12.3.11. Работа всех пользователей АБС осуществляется под уникальными учетными записями.

12.4. Общие требования по обеспечению информационной безопасности средствами антивирусной защиты

12.4.1. На всех автоматизированных рабочих местах и серверах АБС КБ «Максима» (ООО), если иное не предусмотрено технологическим процессом, применяются средства антивирусной защиты.

Установка и обновление антивирусных средств контролируются сотрудником службы ИБ.

12.4.2. Инструкции по антивирусной защите должны учитывать особенности банковских технологических процессов в КБ «Максима» (ООО).

12.4.3. В КБ «Максима» (ООО) организуется антивирусная фильтрация всего трафика электронного почтового обмена.

12.4.4. Если возможно, КБ «Максима» (ООО) организует эшелонированную централизованную систему антивирусной защиты, предусматривающую использование средств антивирусной защиты различных производителей и их раздельную установку на рабочих станциях, почтовых серверах и межсетевых экранах.

12.4.5. КБ «Максима» (ООО) проводит предварительную проверку устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов. Результаты установки, изменения программного обеспечения и антивирусной проверки документируются.

12.4.6. В случае обнаружения компьютерных вирусов, сотрудники КБ «Максима» (ООО) действуют строго в соответствии с требованиями Политики по обеспечению ИБ КБ «Максима» (ООО) средствами антивирусной защиты.

12.4.7. В КБ «Максима» (ООО) проводятся процедуры контроля за отключением и обновлением антивирусных средств на всех автоматизированных рабочих местах и серверах АБС. Результаты контроля документируются.

12.5. Общие требования по обеспечению информационной безопасности при использовании ресурсов сети Интернет

12.5.1. При принятии решений об использовании сети Интернет, при формировании документов, регламентирующих порядок использования сети Интернет, а также иных документов, связанных с обеспечением ИБ при использовании сети Интернет, учитывается следующее:

- сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
- существует вероятность НСД, потери и искажения информации, передаваемой посредством сети Интернет;
- существует вероятность атаки злоумышленников на оборудование, программное обеспечение и информационные ресурсы, подключенные/доступные из сети Интернет;
- гарантии по обеспечению ИБ при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются.

12.5.2. Сеть Интернет в банке может использоваться для:

- ведения дистанционного банковского обслуживания;
- получения и распространения информации, связанной с банковской деятельностью (например, путем создания информационных web-сайтов банка);
- информационно-аналитической работы в интересах организации;
- обмена электронными сообщениями между организациями БС РФ и иными субъектами национальной платежной системы;
- обмена электронными сообщениями, например почтовыми.

Использование сети Интернет в неустановленных целях запрещено.

12.5.3. Решение об использовании сети Интернет для производственной и (или) собственной хозяйственной деятельности принимается руководством КБ «Максима» (ООО).

12.5.4. Порядок подключения и использования ресурсов сети Интернет определен в Порядке подключения и использования сети Интернет в КБ «Максима» (ООО).

12.5.5. При осуществлении дистанционного банковского обслуживания применяются защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы. Все попытки таких подмен регистрируются.

12.5.6. Почтовый обмен через сеть Интернет осуществляется с использованием защитных мер.

12.5.7. Электронная почта архивируется. Изменения в архиве не допускаются. Целями создания архивов электронной почты являются:

- контроль информационных потоков, в том числе с целью предотвращение утечек информации;
- использование архивов при проведении разбирательств по фактам утечек информации.

12.5.8. При взаимодействии с сетью Интернет используются защитные меры противодействия атакам хакеров и распространению спама[11].

12.6. Общие требования по обеспечению информационной безопасности при использовании средств криптографической защиты информации

12.6.1. В КБ «Максима» (ООО) применяются СКЗИ в случаях, установленных законодательством РФ.

СКЗИ, применяемые в КБ «Максима» (ООО) для защиты персональных данных, должны иметь класс не ниже КС2.

Работы по обеспечению с помощью СКЗИ безопасности информации проводятся в соответствии с действующими в настоящее время нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России.

12.6.2. Для обеспечения безопасности в КБ «Максима» (ООО) используются СКЗИ, которые:

- допускают встраивание в технологические процессы обработки электронных сообщений, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;
- поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;
- сертифицированы уполномоченным государственным органом либо имеют разрешение ФСБ России.

12.6.3. Установка и ввод в эксплуатацию, а также эксплуатация СКЗИ осуществляются строго в соответствии с эксплуатационной и технической документацией к этим средствам.

12.6.4. При применении СКЗИ должны поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения

[11] Спам - общее наименование не запрошенных пользователями электронных посланий и рекламных писем, рассылаемых в сети Интернет по ставшим известными рассылающей стороне адресам пользователей.

для среды функционирования СКЗИ, представляющую собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

12.6.5. ИБ процессов изготовления криптографических ключей СКЗИ обеспечивается комплексом технологических, организационных, технических и программных мер и средств защиты.

12.6.6. Для повышения уровня безопасности при эксплуатации СКЗИ и их ключевых систем реализуются процедуры мониторинга, регистрирующего все значимые события, состоявшиеся в процессе обмена криптографически защищенными данными, и все инциденты ИБ.

12.6.7. Порядок применения СКЗИ определяется Председателем Правления Банка и включает:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в АБС;
- порядок эксплуатации;
- порядок восстановления работоспособности в аварийных случаях;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой системой;
- порядок обращения с носителями ключевой информации, включая действия при смене и компрометации ключей.

12.6.8. Криптографические ключи могут изготавливаться банком и (или) клиентом банка самостоятельно. Отношения, возникающие между банком и его клиентами, регулируются заключаемыми договорами.

12.7. Общие требования по обеспечению информационной безопасности банковских платежных технологических процессов

12.7.1. В рамках банковских платежных технологических процессов в качестве активов, защищаемых в первую очередь, рассматриваются:

- банковский платежный технологический процесс;
- платежная информация.

12.7.2. СИБ банковского платежного технологического процесса должна соответствовать всем перечисленным выше требованиям.

12.7.3. Банковские платежные технологические процессы осуществляются с использованием специального программного обеспечения. Использование иного программного обеспечения для осуществления указанных процессов не допускается.

Контроль за соответствием используемого программного обеспечения осуществляет служба ИБ КБ «Максима» (ООО). Результаты контроля фиксируются документально.

12.7.4. Порядок обмена платежной информацией фиксируется в договорах между участниками процесса обмена платежной информацией.

12.7.5. Работники КБ «Максима» (ООО), в том числе администраторы АБС и средств защиты информации, не должны обладать полномочиями для бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, а также проведения несанкционированных операций по изменению состояния банковских счетов.

12.7.6. Результаты технологических операций по обработке платежной информации должны контролироваться (проверяться) и удостоверяться лицами/автоматизированными процессами.

Обработку платежной информации и контроль (проверку) результатов обработки осуществляют разные работники/автоматизированные процессы.

12.7.7. Комплекс мер по обеспечению ИБ банковского платежного технологического процесса предусматривает, в том числе:

- защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений;
- доступ работника КБ «Максима» (ООО) только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;
- контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;
- аутентификацию входящих электронных платежных сообщений;
- двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями;
- возможность ввода платежной информации в АБС только для авторизованных пользователей;
- контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т.д.);
- восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
- сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов;
- возможность блокирования приема к исполнению распоряжений клиентов;
- доставку электронных платежных сообщений участникам обмена.

Когда возможно, в КБ «Максима» (ООО) организуется авторизованный ввод платежной информации в АБС двумя работниками с последующей программной сверкой результатов ввода на совпадение (принцип «двойного управления»).

12.7.8. При проектировании, разработке и эксплуатации систем дистанционного банковского обслуживания документально определяются и выполняются процедуры, реализующие в том числе механизмы:

- снижения вероятности выполнения непреднамеренных или случайных операций или транзакций авторизированными клиентами;
- доведение информации о возможных рисках, связанных с выполнением операций или транзакций до клиентов.

Клиенты систем дистанционного банковского обслуживания обеспечиваются детальными инструкциями, описывающими процедуры выполнения операций или транзакций.

12.7.9. В КБ «Максима» (ООО) осуществляется периодический контроль всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ платежной информации.

12.7.10. Восстановление всех реализованных программно-техническими средствами функций по обеспечению ИБ платежной информации осуществляется в соответствии с документацией разработчика к таким программно-техническим средствам. Соответствующие документы согласовываются со службой ИБ.

12.8. Общие требования по обеспечению информационной безопасности банковских информационных технологических процессов

12.8.1. СИБ банковского информационного технологического процесса должна соответствовать всем перечисленным выше требованиям.

12.8.2. Для каждой АБС службой ИБ осуществляется контроль ее функционирования.

12.8.3. Банковские информационные технологические процессы реализуются в рамках, созданных для этих целей АБС. Не входящие в состав данных АБС серверы, офисные ЭВМ и другое оборудование по возможности изолируются от АБС на уровне локальных вычислительных сетей способом, согласованным со службой ИБ.

12.8.4. В КБ «Максима» (ООО) осуществляется процедура периодического контроля всех реализованных программно-техническими средствами и организационными мерами функций (требований) по обеспечению ИБ неплатежной информации.

12.8.5. Восстановление всех реализованных программно-техническими средствами функций по обеспечению ИБ неплатежной информации осуществляется в соответствии с документацией разработчика к таким программно-техническим средствам. Соответствующие документы согласовываются со службой ИБ.

12.9. Требования по защите отдельных типов информации

12.9.1. Общие требования по обработке персональных данных в банке

12.9.1.1. В банке определяются, документально фиксируются и утверждаются руководством цели обработки ПДн.

12.9.1.2. Для каждой цели обработки ПДн определяются:

- объем и содержание ПДн;
- сроки обработки, в том числе сроки хранения ПДн;
- необходимость получения согласия субъектов ПДн.

12.9.1.3. Обработка ПДн осуществляется в КБ «Максима» (ООО) строго в соответствии с требования Закона 152-ФЗ.

12.9.1.4. В КБ «Максима» (ООО) ведется перечень ИСПДн. При этом АБС, реализующие банковские платежные технологические процессы, не относятся к ИСПДн.

12.9.1.5. Для каждого ресурса ПДн должно быть обеспечено:

- установление цели обработки ПДн;
- установление и соблюдение сроков хранения ПДн и условий прекращения их обработки;
- определение перечня и категорий обрабатываемых ПДн (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн);
- выполнение процедур учета количества субъектов ПДн, в том числе субъектов ПДн, не являющихся работниками организации БС РФ;
- выполнение ограничения обработки ПДн достижением цели обработки ПДн;
- соответствие содержания и объема обрабатываемых ПДн установленным целям обработки;
- точность, достаточность и актуальность ПДн, в том числе по отношению к целям обработки ПДн;

- выполнение установленных процедур получения согласия субъектов ПДн (их законных представителей) на обработку их ПДн, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона "О персональных данных";

- выполнение установленных процедур получения согласия субъектов ПДн на передачу обработки их ПДн третьим лицам, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона "О персональных данных";

- прекращение обработки ПДн и уничтожение либо обезличивание ПДн по достижении целей обработки, по требованию субъекта ПДн в случаях, предусмотренных Федеральным законом "О персональных данных", в том числе при отзыве субъектом ПДн согласия на обработку его ПДн.

12.9.1.6. В КБ «Максима» (ООО) ведется перечень (список) работников, осуществляющих обработку ПДн в ИСПДн либо имеющих доступ к ПДн. Работники указываются в перечне (списке) на ролевой основе в соответствии с занимаемой должностью.

Доступ работников КБ «Максима» (ООО) к ПДн и обработка персональных данных работниками КБ «Максима» (ООО) осуществляются только для выполнения их должностных обязанностей.

12.9.1.7. Все ИСПДн банка относятся к специальным.

12.9.2. Общие требования ИБ по защите сведений, составляющих банковскую тайну (кроме ПДн и платежной информации)

12.9.2.1. Обработка сведений, составляющих банковскую тайну, осуществляется сотрудниками КБ «Максима» (ООО) исключительно в рамках их должностных обязанностей. Сотрудники, должностные обязанности которых не предусматривают обработку указанной информации, не имеют к ней доступ.

12.9.2.2. Обработка сведений, составляющих банковскую тайну, осуществляемая без использования средств автоматизации, должна осуществляться в КБ «Максима» (ООО) таким образом, чтобы в отношении каждой категории сведений, составляющих банковскую тайну, можно было определить места их хранения (материальных носителей) и установить перечень лиц, осуществляющих их обработку либо имеющих к ним доступ.

12.9.2.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность сведений, составляющих банковскую тайну и исключающие НСД к ним. Для этого предпринимаются меры, аналогичные мерам в отношении хранения ПДн.

12.9.2.4. Безопасность сведений, составляющих банковскую тайну, при их обработке в информационных системах КБ «Максима» (ООО) обеспечивается с помощью системы защиты, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения НСД, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки таких сведений), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности сведений, составляющих банковскую тайну, при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации,

представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

12.9.2.5. Обмен сведениями, составляющими банковскую тайну, при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

12.9.2.6. При обработке сведений, составляющих банковскую тайну, в информационных системах КБ «Максима» (ООО) обеспечивается:

- проведение мероприятий, направленных на предотвращение НСД к таким сведениям и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов НСД к таким сведениям;
- недопущение воздействия на технические средства автоматизированной обработки сведений, составляющих банковскую тайну, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления сведений, составляющих банковскую тайну, модифицированных или уничтоженных вследствие НСД к ним;
- постоянный контроль за обеспечением уровня защищенности сведений, составляющих банковскую тайну.

12.9.2.7. Запросы пользователей информационной системы на получение сведений, составляющих банковскую тайну, а также факты предоставления указанных сведений по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется уполномоченным сотрудником службы ИБ.

12.9.3. Общие требования ИБ по защите прочих типов информационных активов

12.9.3.1. Обработка защищаемых информационных активов осуществляется сотрудниками КБ «Максима» (ООО) исключительно в рамках их должностных обязанностей. Сотрудники, должностные обязанности которых не предусматривают обработку указанной информации, не имеют к ней доступ.

12.9.3.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность таких информационных активов и исключающие НСД к ним.

12.9.3.3. При обработке защищаемых информационных активов их безопасность обеспечивается использованием системы защиты, включающей организационные меры и средства защиты информации (в том числе средства предотвращения НСД, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки таких сведений), а также используемые в информационной системе информационные технологии.

При работе с материальными носителями ПДн обеспечено:

- обособление ПДн от иной информации, в частности, путем фиксации их на отдельных съемных носителях ПДн, в специальных разделах или на полях форм документов (при обработке ПДн на бумажных носителях);
- учет съемных носителей ПДн;
- установление, выполнение и контроль выполнения порядка хранения съемных, в том числе машинных, носителей ПДн и доступа к ним;
- хранение ПДн, цели обработки которых заведомо несовместимы, на отдельных съемных носителях;

- регистрация и учет мест хранения материальных носителей ПДн с фиксацией категории обрабатываемых персональных данных (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн) включая раздельное хранение ресурсов ПДн, обработка которых осуществляется с различными целями;

- назначение работников, ответственных за организацию хранения материальных носителей ПДн;

- установление и выполнение порядка уничтожения (стирания) информации с машинных носителей ПДн.

Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

Общедоступные источники ПДн создаются и публикуются банком только для цели выполнения требований законодательства РФ.

Поручение обработки ПДн третьему лицу (далее - обработчик) должно осуществляться на основании договора. В указанном договоре должны быть определены перечень действий (операций) с ПДн, которые будут совершаться обработчиком, и цели обработки, должна быть установлена обязанность обработчика обеспечивать безопасность ПДн (в том числе соблюдать конфиденциальность ПДн) при их обработке, не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом, а также должны быть указаны требования по обеспечению безопасности ПДн. При поручении обработки персональных данных обработчику банк должен получить согласие субъекта ПДн, если иное не предусмотрено законодательством РФ.

13. Система менеджмента информационной безопасности организаций банковской системы Российской Федерации

13.1 Внутренние документы, регламентирующие деятельность в области обеспечения ИБ

13.1.1. В целях обеспечения функционирования СИБ КБ «Максима» (ООО) разрабатываются /корректируются внутренние документы, раскрывающие положения настоящей Политики.

13.1.2. Разработка/корректировка внутренних документов, регламентирующих деятельность в области обеспечения ИБ, проводится на основе:

- законодательства Российской Федерации;
- комплекса БР ИББС;
- нормативных актов и предписаний регулирующих и надзорных органов;
- договорных требований КБ «Максима» (ООО) со сторонними организациями;
- результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов).

13.1.3. Разработку/корректировку внутренних документов, регламентирующих деятельность по обеспечению ИБ, осуществляет служба информационной безопасности. Ответственность за своевременное внесение корректив несет Советник Председателя Правления-Руководитель службы информационной безопасности.

13.2. Принятие руководством КБ «Максима» (ООО) решений о реализации и эксплуатации системы обеспечения ИБ

13.2.1. Решения о реализации и эксплуатации СОИБ утверждаются Председателем Правления КБ «Максима» (ООО), в частности:

- об анализе и принятии остаточных рисков нарушения ИБ;
- о планировании этапов внедрения СОИБ;
- о распределении ролей в области обеспечения ИБ КБ «Максима» (ООО);
- о принятии со стороны руководства планов внедрения защитных мер, направленных на снижение рисков ИБ;
- о выделении ресурсов, необходимых для реализации и эксплуатации СОИБ.

13.2.2. Все планы внедрения СОИБ утверждаются Председателем Правления КБ «Максима» (ООО). Указанные планы должны документально фиксировать:

- последовательность выполнения мероприятий в рамках указанных планов;
- сроки начала и окончания запланированных мероприятий;
- должностных лиц (подразделения), ответственных за выполнение каждого указанного мероприятия.

13.2.3. Обязанности (и, соответственно, ответственность) по реализации планов обработки рисков нарушения ИБ и реализацию требуемых защитных мер несут лица, непосредственно поименованные в планах как исполнители.

13.2.4. Решения руководства, связанные с назначением и распределением ролей для всех структурных подразделений в соответствии с положениями внутренних документов, регламентирующих деятельность по обеспечению ИБ документируются.

13.3. Обучение и повышение осведомленности в области ИБ

13.3.1. В КБ «Максима» (ООО) проводится документально оформленная и утвержденная руководством работа с персоналом в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов.

13.3.2. В планах обучения и повышения осведомленности устанавливаются требования к периодичности обучения и повышения осведомленности.

13.3.3. Программы обучения и повышения осведомленности должны включать информацию:

- по существующим политикам ИБ;
- по применяемым в КБ «Максима» (ООО) защитным мерам;
- по правильному использованию защитных мер в соответствии с внутренними документами КБ «Максима» (ООО);
- о значимости и важности деятельности работников для обеспечения ИБ КБ «Максима» (ООО).

13.3.4. Свидетельством выполнения программ обучения и повышения осведомленности в области ИБ в КБ «Максима» (ООО) являются:

- журналы, подтверждающие прохождение руководителями и работниками организации БС РФ обучения в области ИБ;

- документы, содержащие результаты проверок обучения работников КБ «Максима» (ООО);

- документы, содержащие результаты проверок осведомленности в области ИБ в КБ «Максима» (ООО).

13.3.5. Для работника, получившего новую роль, организуется обучение или инструктаж в области ИБ, соответствующее полученной роли.

13.3.6. Обязанность по разработке и реализации планов и программ обучения и повышения осведомленности в области ИБ возлагается на отдел автоматизации.

Ответственность за выполнение указанных функций возлагается начальника отдела автоматизации.

Обязанности по контролю результатов обучения и повышения осведомленности в области ИБ возлагается на службу СВК.

Ответственность за осуществление указанного контроля возлагается на руководителя СВК.

13.4. Обнаружение и реагирование на инциденты ИБ

Обнаружение и реагирование на инциденты ИБ в КБ «Максима» (ООО) осуществляется в соответствии с требованиями, установленными в «Порядке обнаружения и реагирования на инциденты ИБ в КБ «Максима» (ООО)».

13.5 Организация обеспечения непрерывности бизнеса и его восстановления после прерываний

13.5.1. Активы, отнесенные к категориям К1 и К2, являются существенными для обеспечения непрерывности бизнеса КБ «Максима» (ООО).

13.5.2. В КБ «Максима» (ООО) документально определяется план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания («План действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности КБ «Максима» (ООО) в случае возникновения непредвиденных обстоятельств»). Указанный план должен содержать инструкции и порядок действий работников КБ «Максима» (ООО) по восстановлению бизнеса.

13.5.3. Разработка планов обеспечения непрерывности бизнеса и его восстановления после прерывания должна основывается на документально оформленных результатах оценки рисков нарушения ИБ применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания.

13.5.4. В банке документально определяются, реализуются и используются защитные меры обеспечения непрерывности бизнеса применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания («План действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности КБ «Максима» (ООО) в случае возникновения непредвиденных обстоятельств»).

Реализация и использование защитных мер обеспечения непрерывности бизнеса и его восстановления после прерывания основываются на соответствующих требованиях по обеспечению ИБ.

13.5.5. В КБ «Максима» (ООО) выполняется регулярный пересмотр, обновление, периодическое тестирование и, в случае необходимости, корректировка плана обеспечения

непрерывности бизнеса и его восстановления после прерывания в соответствии с требованиями («План действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности КБ «Максима» (ООО) в случае возникновения непредвиденных обстоятельств»). Сценарий тестирования составляется с учетом существующей в КБ «Максима» (ООО) модели угроз и нарушителей, а также результатов оценки рисков.

13.5.6. В КБ «Максима» (ООО) осуществляется обучение и повышение осведомленности работников в области обеспечения непрерывности бизнеса и его восстановления после прерываний в соответствии с разработанной программой.

14. Проверка и оценка ИБ КБ «Максима» (ООО), принятие решений по улучшениям

14.1 Общие положения по проверке и оценке ИБ КБ «Максима» (ООО)

14.1.1. Проверка и оценка ИБ КБ «Максима» (ООО) проводится путем выполнения следующих процессов:

- мониторинга и контроля защитных мер;
- самооценки ИБ;
- аудита ИБ;
- анализа функционирования СОИБ (в том числе со стороны руководства).

Указанные процессы являются частью группы процессов "проверка" СМИБ.

14.1.2. Основными целями мониторинга и контроля защитных мер являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных под заданные цели. Такими целями анализа могут быть:

- контроль за реализацией положений внутренних документов по обеспечению ИБ в организации БС РФ;
- выявление нештатных, в том числе злоумышленных, действий в АБС организации;
- выявление инцидентов ИБ.

Мониторинг и контроль защитных мер проводится сотрудником службы ИБ.

14.1.3. При подготовке к аудиту ИБ проводится самооценка ИБ. Самооценка ИБ проводится собственными силами и по инициативе руководства КБ «Максима» (ООО).

14.1.4. Аудит ИБ, проводимый внешними по отношению к КБ «Максима» (ООО) независимыми проверяющими организациями, является одной из форм проверки и оценки (контроля) выполнения КБ «Максима» (ООО) требований комплекса БР ИББС.

Аудит ИБ проводится как для собственных целей самим КБ «Максима» (ООО) , так и с целью повышения доверия к ней со стороны других организаций.

14.1.5. Анализ функционирования СОИБ проводится сотрудником службы ИБ, а также руководством, в том числе на основании подготовленных для руководства документов (данных).

Основными целями проведения анализа функционирования СОИБ являются:

- оценка эффективности СОИБ;
- оценка соответствия СОИБ требованиям законодательства Российской Федерации и комплекса БР ИББС;
- оценка соответствия СОИБ существующим и возможным угрозам ИБ;
- оценка следования принципам ИБ и выполнения требований по обеспечению ИБ, закрепленным в настоящей Политике, а также в иных внутренних документах КБ «Максима» (ООО).

Результаты, полученные в ходе анализа функционирования СОИБ, являются среди прочего основой для совершенствования СОИБ.

14.2. Мониторинг и контроль защитных мер

14.2.1. В КБ «Максима» (ООО) проводится мониторинг СОИБ и контроль защитных мер, включая контроль параметров конфигурации и настроек средств и механизмов защиты. Указанные процедуры проводятся сотрудником службы ИБ, и охватывают все реализованные и эксплуатируемые защитные меры, входящие в СИБ.

14.2.2. В КБ «Максима» (ООО) осуществляется сбор и хранение информации о действиях работников, событиях и параметрах, имеющих отношение к функционированию защитных мер.

14.2.3. Информация обо всех инцидентах, выявленных в процессе мониторинга СОИБ и контроля защитных мер, включается в базу данных инцидентов ИБ.

14.2.4. Определенные в КБ «Максима» (ООО) процедуры мониторинга СОИБ и контроля защитных мер должны подвергаться регулярным и документально зафиксированным пересмотрам в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ.

14.3. Проведение самооценки ИБ

14.3.1. В КБ «Максима» (ООО) проводится самооценка ИБ в соответствии с Порядком проведения самооценки ИБ КБ «Максима» (ООО) на основе соответствующей методики.

14.3.2. В КБ «Максима» (ООО) разрабатывается, документируется и реализуется программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки.

14.3.3. В КБ «Максима» (ООО) документально определяются:

- порядок формирования, сбора и хранения свидетельств самооценки ИБ;
- периодичность проведения самооценки ИБ;
- порядок хранения и использования результатов самооценки ИБ.

14.3.4. Для каждой проводимой самооценки ИБ документально оформляется план проведения самооценки, определяющий:

- цель самооценки ИБ;
- объекты и деятельность, подвергающиеся самооценке ИБ;
- порядок и сроки выполнения мероприятий самооценки ИБ;
- распределение ролей среди работников КБ «Максима» (ООО), связанных с проведением самооценки ИБ.

14.3.5. По результатам проведения самооценок ИБ подготавливаются отчеты. Результаты самооценок ИБ, а также соответствующие отчеты доводятся до руководства КБ «Максима» (ООО).

14.4. Проведение аудита ИБ

14.4.1. Аудит ИБ банка проводится в соответствии с требованиями стандартов Банка России СТО БР ИББС-1.1 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности" и СТО БР ИББС-1.2 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0".

14.4.2. Программа аудитов ИБ содержит информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки.

Для каждого проводимого аудита ИБ устанавливается план аудита, определяющий:

- цель аудита ИБ;
- критерии аудита ИБ;
- область аудита ИБ;
- дату и продолжительность проведения аудита ИБ;
- состав аудиторской группы;
- описание деятельности и мероприятий по проведению аудита;
- распределение ресурсов при проведении аудита.

В КБ «Максима» (ООО) может проводиться аудит ИБ специализированными организациями на основании заключенных договоров.

14.4.3. При заключении договора на аудит системы ИБ документально определяются:

- порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудита ИБ;
- порядок взаимодействия с организацией, проводящей аудит, в процессе проведения аудита ИБ;
- порядок взаимодействия группы, проводящей аудит, и руководства, позволяющий представителям аудиторской группы при необходимости непосредственно обращаться к руководству;
- порядок организации опроса сотрудников КБ «Максима» (ООО);
- порядок организации наблюдения за деятельностью сотрудников КБ «Максима» (ООО) со стороны представителей организации, проводящей аудит.

14.4.4. Отчеты, подготовленные по результатам проведения аудита. Доводятся до сведения руководства КБ «Максима» (ООО).

14.5. Анализ функционирования СОИБ

14.5.1. В КБ «Максима» (ООО) проводится анализ функционирования СОИБ, использующий в том числе:

- результаты мониторинга СОИБ и контроля защитных мер;
- сведения об инцидентах ИБ;
- результаты проведения аудитов ИБ, самооценок ИБ;
- данные об угрозах, возможных нарушителях и уязвимостях ИБ;
- данные об изменениях внутри КБ «Максима» (ООО), например, данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах КБ «Максима» (ООО);
- данные об изменениях вне КБ «Максима» (ООО), например, данные об изменениях в законодательстве Российской Федерации, изменениях в требованиях комплекса БР ИББС, изменениях в договорных обязательствах КБ «Максима» (ООО).

14.5.2. Анализ функционирования СОИБ включает в том числе:

- анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в КБ «Максима» (ООО), требованиям законодательства Российской Федерации, требованиям стандартов Банка России, контрактным требованиям КБ «Максима» (ООО);
- анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ в КБ «Максима» (ООО), требованиям политик ИБ;
- оценку адекватности модели угроз КБ «Максима» (ООО) существующим угрозам ИБ;
- оценку рисков в области ИБ организации, включая оценку уровня остаточного и допустимого риска;
- проверку адекватности используемых защитных мер требованиям внутренних документов КБ «Максима» (ООО) и результатам оценки рисков;
- анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер.

14.5.3. Результаты анализа функционирования СОИБ документируются.

14.5.4. Обязанности по выполнению процедур анализа СОИБ, поименованных в п. 14.5.2., возлагается на службу ИБ КБ «Максима» (ООО). Ответственность за их выполнение возлагается на руководителя службы ИБ.

14.6. Анализ СОИБ со стороны руководства КБ «Максима» (ООО)

14.6.1. В КБ «Максима» (ООО) определяется и утверждается руководством план выполнения деятельности по контролю и анализу СОИБ. Указанный план должен содержать положения по проведению совещаний на уровне руководства, на которых в том числе производятся поиск и анализ проблем ИБ, влияющих на бизнес КБ «Максима» (ООО).

14.6.2. Руководство КБ «Максима» (ООО) проводит анализ СОИБ на основании документов, включенных в Перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ.

14.6.3. Обязанность по подготовке информации, необходимой для анализа СОИБ руководством, возлагается на службу ИБ.

Ответственность за выполнение указанной функции возлагается на руководителя службы ИБ.

14.7. Принятие решений по тактическим[12] улучшениям СИБ

14.7.1. В целях принятия решений, связанных с тактическими улучшениями СОИБ, рассматриваются среди прочего документально оформленные результаты:

- аудитов ИБ;
- самооценок ИБ;
- мониторинга СОИБ и контроля защитных мер;

[12] К тактическим улучшениям СОИБ следует относить корректирующие или превентивные действия, связанные с пересмотром отдельных процедур выполнения деятельности в рамках СОИБ и не требующие пересмотра политики ИБ и частных политик ИБ. Как правило, тактические улучшения СОИБ не требуют выполнения деятельности в рамках этапа «планирование» СМИБ.

- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых угроз и уязвимостей ИБ;
- оценки рисков;
- анализа перечня защитных мер, возможных для применения;
- стратегических улучшений СОИБ;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций).

14.7.2. Решения по тактическим улучшениям СОИБ документально фиксируются и содержат либо выводы об отсутствии необходимости тактических улучшений СОИБ, либо должны быть указаны направления тактических улучшений СОИБ в виде корректирующих или превентивных действий, например:

- пересмотр процедур выполнения отдельных видов деятельности по обеспечению ИБ;
- пересмотр процедур эксплуатации отдельных видов защитных мер;
- пересмотр процедур обнаружения и обработки инцидентов;
- уточнение описи информационных активов;
- пересмотр программы обучения и повышения осведомленности персонала;
- пересмотр плана обеспечения непрерывности бизнеса и его восстановления после прерывания;
- пересмотр планов обработки рисков;
- вынесение санкций в отношении персонала;
- пересмотр процедур мониторинга СОИБ и контроля защитных мер;
- пересмотр программ аудитов;
- корректировка соответствующих внутренних документов, регламентирующих процедуры выполнения деятельности по обеспечению ИБ и эксплуатации защитных мер;
- ввод новых или замена используемых защитных мер.

14.7.3. Вся деятельность по реализации тактических улучшений документально регистрируется. В частности, результаты выполнения планов реализации тактических улучшений СОИБ фиксируются в отчете о реализации плана тактических улучшений СОИБ, в котором, в том числе, указываются:

- какие мероприятия в рамках плана выполнены;
- какова форма реализации указанных мероприятий;
- выводы и достижении целей плана и необходимости (отсутствии необходимости) проведения дополнительных мероприятий.

14.7.4. Деятельность, связанная с реализацией тактических улучшений СОИБ, должна быть санкционирована и контролироваться сотрудником службы ИБ.

14.7.5. Согласование и информирование заинтересованных сторон о тактических улучшениях СОИБ, в частности, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям ИБ, осуществляется в форме заполнения Подписного листа тактических улучшений СОИБ.

14.7.6. В случаях принятия решений по тактическим улучшениям СОИБ должны быть назначены ответственные за их реализацию.

14.8. Принятие решений по стратегическим[13] улучшениям СОИБ

[13] К стратегическим улучшениям СОИБ следует относить корректирующие или превентивные действия, связанные с пересмотром политики ИБ и частных политик ИБ КБ «Максима» (ООО), с последующим выполнением соответствующих тактических улучшений СОИБ. Стратегические улучшения СОИБ всегда требуют выполнения деятельности в рамках этапа «планирование» СМИБ.

14.8.1. Для принятия решений, связанных со стратегическими улучшениями СОИБ, рассматриваются среди прочего документально оформленные результаты:

- аудитов ИБ;
- самооценок ИБ;
- мониторинга СОИБ и контроля защитных мер;
- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых информационных активов КБ «Максима» (ООО) или их типов;
- выявления новых угроз и уязвимостей ИБ;
- оценки рисков;
- пересмотра основных рисков ИБ;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций);

а также изменения:

- в законодательстве Российской Федерации;
- в нормативных актах Банка России, в частности, требованиях настоящего стандарта;
- интересов, целей и задач бизнеса КБ «Максима» (ООО);
- контрактных обязательств КБ «Максима» (ООО).

14.8.2. Решения по стратегическим улучшениям СОИБ документально фиксируются и должны содержать либо выводы об отсутствии необходимости стратегических улучшений СОИБ, либо указывать направления стратегических улучшений СОИБ в виде корректирующих или превентивных действий, например:

- уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ или частных политик ИБ;
- изменение в области действия СОИБ;
- пересмотр моделей угроз и нарушителей;
- изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ.

14.8.3. Вся деятельность по реализации стратегических улучшений документально регистрируется.

14.8.4. Деятельность, связанная с реализацией стратегических улучшений СОИБ, должна быть санкционирована и контролироваться руководством КБ «Максима» (ООО).

14.8.5. В случае стратегических улучшений СОИБ выполняется деятельность по реализации соответствующих тактических улучшений СОИБ для всех необходимых процедур обеспечения ИБ, используемых защитных мер и соответствующих внутренних документов. В частности, выполняется:

- выработка планов тактических улучшений СОИБ;
- уточнение планов обработки рисков;
- уточнение программы внедрения защитных мер;
- уточнение процедур использования защитных мер.

14.8.6. Согласование и информирование заинтересованных сторон о стратегических улучшениях СОИБ, в частности, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям ИБ, осуществляется в форме заполнения Подписного листа тактических улучшений СОИБ по форме Приложения 12 к настоящей Политике.

14.8.7. В случаях принятия решений по стратегическим улучшениям СОИБ назначаются ответственные за их реализацию.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1. Опись защищаемых информационных активов

_____.

(наименование)

№	Типы информационных активов	Информационные активы, принадлежащие данному типу	Классы информационных активов	Объекты среды информационных активов	Сотрудники (их роли) и клиенты, которым предоставляется доступ
1	2	3	4	5	6

Председатель Правления: _____ / /

«__» _____ 20__ г.

ПРИЛОЖЕНИЕ 2. Порядок контроля функционирования АБС КБ «Максима» (ООО) со стороны службы ИБ

АБС	Порядок контроля функционирования		
	мероприятия контроля	периодичность проведения	ответственный за проведение
«iBank 2»	**1)Проверка целостности структуры базы данных и создание резервной копии данных** **2) Тестовое восстановление резервной копии базы данных**	**3 раза в сутки** **1 раз в сутки**	**Лесников А.Б.**

ПРИЛОЖЕНИЕ 3. Процедуры контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер

1. На стадии эксплуатации АБС определены, выполняются и регистрируются следующие процедуры:

- контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер, в том числе контроль реализации организационных защитных мер, контроль состава и параметров настройки применяемых технических защитных мер;
- контроля отсутствия уязвимостей в оборудовании и программном обеспечении АБС;
- контроля внесения изменений в параметры настройки АБС и применяемых технических защитных мер;
- контроля необходимого обновления программного обеспечения АБС, включая программное обеспечение технических защитных мер;
- контроля состава устанавливаемого и (или) используемого ПО АБС;
- необходимые для обеспечения сохранности носителей защищаемой информации.

2. На стадии сопровождения (модернизации) определены, выполняются и регистрируются процедуры контроля, обеспечивающие защиту от:

- умышленного несанкционированного раскрытия, модификации или уничтожения информации;
- неумышленной модификации, раскрытия или уничтожения информации;
- отказа в обслуживании или ухудшения обслуживания.

3. На стадии снятия с эксплуатации определены, выполняются и регистрируются процедуры, обеспечивающие удаление информации с использованием алгоритмов и (или) методов, обеспечивающих невозможность восстановления удаленной информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, и информации, используемой техническими защитными мерами, из постоянной памяти АБС и с внешних носителей, за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены законодательством РФ, нормативными актами Банка России и (или) договорными документами.

ПРИЛОЖЕНИЕ 4. Применяемые в КБ «Максима» (ООО) на стадии сопровождения (модернизации) АБС процедуры контроля, обеспечивающие защиту от умышленного и неумышленного несанкционированного раскрытия, модификации или уничтожения информации, отказа в обслуживании или ухудшения обслуживания.

- мониторинг, контроль, блокирование использования сервисов электронной почты при передаче информации на внешние адреса электронной почты;
- мониторинг, контроль, блокирование использования беспроводных сетей и сети Интернет с использованием информационной инфраструктуры организации БС РФ;
- мониторинг, контроль, блокирование использования удаленного доступа к информационной инфраструктуре организации БС РФ с использованием сети Интернет;
- мониторинг публикации информации конфиденциального характера в сети Интернет, в том числе социальных сетях и форумах;
- мониторинг, контроль, блокирование копирования информации на переносные носители информации;
- контроль использования средств факсимильной связи;
- контроль (запрет или блокирование) использования личных средств связи (телефоны, смартфоны, планшеты и т.п.);
- мониторинг и контроль печати и (или) копирования информации на бумажных носителях;
- контроль (блокирование) возможности использования и (или) доступа к информации конфиденциального характера на переносных носителях информации за пределами информационной инфраструктуры организации БС РФ;
- блокирование возможности доступа к информации конфиденциального характера на средствах вычислительной техники за пределами информационной инфраструктуры организации БС РФ;
- мониторинг и анализ действий возможных внутренних нарушителей по доступу к информационным активам;
- контроль передачи (выноса) средств вычислительной техники за пределы организации БС РФ;
- контроль физического доступа с целью предотвращения визуального и слухового ознакомления с информацией;
- контроль и (или) запрет размещения на средствах вычислительной техники, используемых для обработки информации конфиденциального характера, и блокирования возможности использования программного обеспечения сервисов мгновенных сообщений (например: ICQ, WhatsUp, Viber, Skype);
- контроль и (или) запрет обработки личной информации с использованием информационной инфраструктуры и средств связи организации БС РФ;
- контроля и (или) запрет самостоятельного использования работниками публичных облачных технологий хранения и обработки информации конфиденциального характера.

ПРИЛОЖЕНИЕ 5. Перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ.

В целях анализа СОИБ КБ «Максима» (ООО) со стороны руководства формируется пакет из следующих документов:

1. Отчеты с результатами мониторинга СОИБ и контроля защитных мер;
2. Отчеты с результатами анализа функционирования СОИБ;
3. Отчеты с результатами самооценок ИБ;
4. Документы, содержащие информацию о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ;
5. Документы, содержащие информацию о новых выявленных уязвимостях и угрозах ИБ;
6. Документы, содержащие информацию о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством;
7. Документы, содержащие информацию об изменениях, которые могли бы повлиять на организацию СОИБ, например, изменения в законодательстве РФ и (или) положениях стандартов Банка России;
8. Документы, содержание информацию по выявленным инцидентам ИБ;
9. Документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например, выполнение планов обработки рисков;
10. Документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания.

ПРИЛОЖЕНИЕ 6. Порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ КБ «Максима» (ООО)

1. Порядок разработки и пересмотра планов по обеспечению ИБ КБ «Максима» (ООО)

1.1. Разработка и пересмотр планов по обеспечению ИБ осуществляется в случаях, установленных требованиями настоящей Политики.

1.2. Разработка планов по обеспечению ИБ осуществляется по решению руководства КБ «Максима» (ООО) специально сформированной комиссией при участии сотрудника службы ИБ.

1.3. При разработке плана по обеспечению ИБ КБ «Максима» (ООО) (далее по тексту Приложения – План) осуществляются следующие мероприятия:

- определение конечных целей разработки Плана;
- выявления объектов воздействия для достижения целей разработки Плана;
- формирование списка возможных мероприятий по достижению целей Плана на основе анализа имеющейся информации о состоянии СОИБ в КБ «Максима» (ООО) в части, касающейся целей Плана, действующей нормативной базы и т.п.;
- анализ совместимости мероприятий, включенных в сформированный список, формирование окончательного списка предполагаемых мероприятий;
- определение последовательности выполнения запланированных мероприятий;
- определение необходимых ресурсов (времени, материальных ресурсов, другое) для выполнения мероприятий, включенных в список;
- анализ возможности выделения кредитной организацией таких ресурсов. В случае невозможности – корректировка плана в части невыполнимых мероприятий;
- для окончательного списка мероприятий определение конкретных сроков, ответственных исполнителей, списка прочих необходимых ресурсов;
- рассмотрение и утверждение плана руководителем службы ИБ;
- утверждение плана руководителем КБ «Максима» (ООО).

1.4. Типовая форма Плана представлена в Приложении 7.

2. Контроль исполнения Плана.

2.1. Контроль за исполнением Плана возлагается на службу ИБ.

2.2. Ответственность за проведение контроля возлагается на руководителя службы ИБ.

2.3. В ходе проведения контроля исполнения Плана сотрудником, проводящим контроль, ставится соответствующая отметка в графу 5 «Статус реализации» Плана о выполнении каждого пункта Плана.

ПРИЛОЖЕНИЕ 7. План по обеспечению ИБ КБ «Максима» (ООО)

Утверждаю
Председатель Правления КБ «Максима» (ООО)
Г.В.Белашов

_____
"__" _____ 20__ г.

№ п/п	Наименование мероприятия	Основание (норматив-ный акт)	Форма реализации	Статус реализации	Срок выпол-нения	Ответст-венное лицо	Примечание
1	2	3	4	5	6	7	8

ПРИЛОЖЕНИЕ 8. Порядок разработки, поддержки, пересмотра и контроля исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ

1. Разработка и пересмотр внутренних документов, регламентирующих деятельность по обеспечению ИБ, осуществляется в соответствии с Планами по обеспечению ИБ КБ «Максима» (ООО) лицами и в сроки, указанные в таких Планах.

2. Разработка и пересмотр внутренних документов, регламентирующих деятельность в области обеспечения ИБ, осуществляется на основе:

- законодательства Российской Федерации;
- комплекса БР ИББС, в частности, требования 7-го и 8-го разделов стандарта СТО БР ИББС-1.0;
- нормативных актов и предписаний регулирующих и надзорных органов;
- договорных требований организации со сторонними организациями;
- результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов).

3. В ходе разработки (пересмотра) внутреннего документа, регламентирующего деятельность по обеспечению ИБ, осуществляются следующие мероприятия:

- изучение и анализ существующей нормативной базы, в том числе в КБ «Максима» (ООО);
- определение (корректировки) целей и задач разрабатываемых (пересматриваемых документов);
- определение положений, позволяющих достигнуть поставленные цели и задачи;
- написание (корректировки) внутреннего документа;
- согласование внутреннего документа (корректировок к нему) с заинтересованными и уполномоченными подразделениями (сотрудниками) КБ «Максима» (ООО);
- утверждение внутреннего документа (корректировок к нему) уполномоченным органом.

4. Обязанности по поддержке внутренних документов, регламентирующих деятельность по ИБ, возлагается на службу ИБ.

Ответственность за выполнение указанной функции возлагается на руководителя подразделения, ответственного в КБ «Максима» (ООО) за ИБ.

5. Контроль за ходом разработки и пересмотра внутренних документов, регламентирующих деятельность по обеспечению ИБ, в том числе соответствие целям разработки (пересмотра) осуществляется сотрудником службы ИБ.

Результаты проведения контроля фиксируются в графе 5 «Статус реализации» Плана.

Ответственность за осуществление контроля при разработке (корректировке) внутренних документов, регламентирующих деятельность по обеспечению ИБ, возлагается на руководителя службы ИБ.

ПРИЛОЖЕНИЕ 9. Журнал обучения и повышения осведомленности сотрудников КБ «Максима» (ООО) в области ИБ

Дата	Основание для проведения обучения	Содержание обучения	Сотрудник (организация), проводивший обучение	Сотрудники, прошедшие обучение	Отметка о выполнении
1	2	3	4	5	6

ПРИЛОЖЕНИЕ 10. Процедуры мониторинга СОИБ и контроля защитных мер

1. В КБ «Максима» (ООО) осуществляется мониторинг СОИБ и контроль применяемых защитных мер, включая контроль параметров конфигурации и настроек средств и механизмов защиты.

2. Мониторинг СОИБ и контроль защитных мер осуществляется на основе информации о действиях работников КБ «Максима» (ООО), событиях и параметрах, имеющих отношение к функционированию защитных мер, документально фиксируемых в соответствии с требованиями Политики ИБ КБ «Максима» (ООО).

3. Сотрудник, осуществляющий мониторинг СОИБ и контроль защитных мер включает информацию обо всех выявленных инцидентах в единую базу данных инцидентов ИБ.

4. Результаты выполнения процедур мониторинга СОИБ и контроля защитных мер фиксируются в журнале Мониторинга СОИБ и контроля защитных мер.

5. Мониторинг СОИБ и контроль применяемых защитных мер осуществляется сотрудником службы ИБ.

6. Ответственность за выполнение указанных функций возлагается на руководителя службы ИБ.

7. Закрепленные настоящим документом процедуры мониторинга СОИБ и контроля защитных мер пересматриваются:

- в связи с изменениями в составе и способах использования защитных мер;
- в связи с выявлением новых угроз и уязвимостей ИБ;
- по результатам расследования инцидента ИБ.

Пересмотр осуществляется в соответствии с порядком, закрепленным «Порядком разработки, поддержки, пересмотра и контроля исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ».

ПРИЛОЖЕНИЕ 11. Журнал мониторинга СОИБ и контроля защитных мер

№ записи	Дата	Процедура мониторинга СОИБ и контроля защитных мер	Исполнитель	Результаты проведения процедуры
1	2	3	4	5

ПРИЛОЖЕНИЕ 12. Подписной листа тактических (стратегических) улучшений СОИБ

№	Тактическое (стратегическое) улучшение СОИБ	Согласовал	Проинформирован	Личная подпись
1	2	3	4	5