Приложение
к Распоряжению Управляющего
директора по информационной
безопасности АО «Казахтелеком»
от «__» _____ 2026 года
№ _____

Методика оценки рисков информационной безопасности АО «Казахтелеком»

Алматы, 2026

СОДЕРЖАНИЕ

Глава 1. Общие положения 3
Глава 2. Термины, определения и сокращения 3
Глава 3. Методика управления рисками ИБ 4
§1. Процесс управления рисками ИБ 4
§2. Идентификация рисков ИБ 5
§3. Оценка рисков ИБ 7
§4. Обработка рисков ИБ 8
§5. Мониторинг рисков ИБ 9
§6. Порядок и сроки организации управления рисками ИБ 9
Глава 4. Ответственность и полномочия 11
предоставляет консультационную помощь СИБ по требованиям настоящей Методики. 11
Глава 5. Документация 11
Глава 6. Ссылка 11
Приложение 1 13
Приложение 3 17
Приложение 4 18
Приложение 5 21
Приложение 6 22
Приложение 7 22
Приложение 8 24

Глава 1. Общие положения

1. Настоящая Методика оценки рисков информационной безопасности АО «Казахтелеком» (далее – Методика) определяет состав и порядок выполнения процедур идентификации, анализа, оценки, контроля рисков информационной безопасности, а также мониторинга эффективности применяемых методов управления рисками.

2. Методика разработана в соответствии с законодательством Республики Казахстан, Политикой управления рисками и Политикой информационной безопасности АО «Казахтелеком» (далее – Общество), иными внутренними документами Общества, а также на основе международных практик в области управления рисками и внутреннего контроля.

3. Настоящая Методика разработана в целях оказания практической помощи работникам Общества, осуществляющим идентификацию, анализ, оценку (переоценку), контроль рисков информационной безопасности и мониторинг эффективности методов управления рисками информационной безопасности.

4. Настоящая Методика является, обязательной для соблюдения работниками, занимающими руководящие должности, а также работниками, задействованными в процессе обработки рисков информационной безопасности. Руководители структурных подразделений ответственны за доведение до сведения работников курируемых подразделений настоящей Методики.

Глава 2. Термины, определения и сокращения

5. В настоящей Методике используются следующие термины, определения и сокращения:

доступность - свойство системы (среды, средств и технологий обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ пользователей к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от пользователей запросов всегда, когда в обращении к ним возникает необходимость;

ДУРиВК – Департамент управления рисками и внутренних контролей;

ИБ – информационная безопасность;

идентификация риска - процесс нахождения, составления перечня и описания элементов риска;

информационный актив (далее – ИА) - материальный или нематериальный объект, который является информацией или содержит информацию, или служит для обработки, хранения, передачи информации и имеющий ценность для Общества в интересах достижения целей и непрерывности его деятельности;

инцидент информационной безопасности (далее -ИИБ) – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию

и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;

конфиденциальность – свойство информации, указывающее на необходимость введения ограничений на круг пользователей, имеющих доступ к данной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от пользователей, не имеющих полномочий на доступ к ней;

обработка риска – процесс выбора и реализации защитных мер по изменению рисков;

оценка риска – процесс сравнения результатов анализа риска с установленными критериями риска для определения, является ли риск и/или его величина приемлемыми или допустимыми;

риск информационной безопасности – потенциальная возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящая к угрозе для Общества. Определяется как сочетание вероятности события и его последствий;

риск-менеджер – ответственный работник Департамента управления рисками и внутренних контролей;

СИБ – Служба информационной безопасности АО «Казахтелеком»;

снижение риска – действия, предпринимаемые для уменьшения вероятности событий информационной безопасности и их последствий;

СП – структурное подразделения Центрального аппарата или филиала Общества;

угроза – потенциальная или реальная возможность неправомерного преднамеренного или случайного воздействия на информационный актив, приводящий к потере, разглашению или к несанкционированным изменениям свойств информации (конфиденциальность, доступность, целостность);

управление рисками – скоординированные действия, направленные на руководство и управление организацией с учетом существующих рисков;

уязвимость – недостаток объекта информатизации, использование которого может привести к нарушению целостности и (или) конфиденциальности, и (или) доступности объекта информатизации;

целостность – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Глава 3. Методика управления рисками ИБ
§1. Процесс управления рисками ИБ

8. Управление рисками ИБ представляет собой непрерывный циклический процесс по идентификации, оценке, мониторингу рисков ИБ, принятию и выполнению управленческих решений, направленных на снижение вероятности возникновения неблагоприятного результата и минимизацию возможных потерь в сфере обеспечения ИБ, встроенный в общую систему управления рисками Общества.

9. Основными задачами управления рисками ИБ являются:

1) выявление рисков ИБ, причин их возникновения и способов реализации;

2) анализ вероятности реализации рисков ИБ и степени последствий нарушения ИБ;

3) принятие решений в отношении рисков ИБ, планирование и осуществление мероприятий по их обработке;

4) проведение регулярного и эффективного мониторинга рисков ИБ и усовершенствование процесса управления рисками ИБ;

5) повышение квалификации работников в области управления рисками ИБ.

10. Процесс управления рисками ИБ состоит их следующих основных этапов:

1) идентификация рисков ИБ;

2) оценка рисков ИБ;

3) обработка рисков ИБ;

4) мониторинг рисков ИБ

11. Блок-схема методики управления рисками представлена на рисунке 1.

§2. Идентификация рисков ИБ

12. Целью идентификации рисков ИБ является выявление возможных угроз ИБ, которые могут нанести ущерб деятельности Общества, причин их возникновения и возможных последствий их воздействия.

13. Для идентификации рисков ИБ проводятся следующие процедуры:

1) идентификация и оценка ИА;

2) идентификация угроз ИБ;

3) идентификация уязвимостей;

4) идентификация существующих средств защиты.

14. Идентификация и оценка ИА, а также определение степени их конфиденциальности, целостности и доступности осуществляются СП Общества, являющимися владельцами ИА, совместно с СИБ.

15. Идентификация ИА заключается в определении ИА, находящихся в распоряжении СП, также в определении их пользователей, средств обработки, передачи и хранения данных.

16. Оценка ИА рассматривается с точки зрения качественной оценки возможного ущерба вследствие нарушения их свойств. Ущерб нарушения ИБ оценивается согласно критериям, отраженным в таблице 1 Приложения 1 к настоящей Методике.

17. ИА считается ценным ИА, когда степень последствия нарушения ИБ, наносимого любому из трех свойств ИА (конфиденциальность, целостность, доступность), оценена на высоком и критическом уровне.

18. В случае создания новых бизнес-процессов или при изменении действующих, а также при внедрении новых информационных систем проводится дополнительная идентификация и оценка ИА.

19. Результаты выполнения идентификации и оценки ИА оформляются по форме согласно Приложению 2 к настоящей Методике.

20. СП по запросу СИБ предоставляет сведения о средствах обработки, передачи

и хранения ИА по форме согласно Приложению 2 к настоящей Методике.

21. Идентификация угроз, уязвимостей и существующих средств защиты информационных активов осуществляются СИБ.

22. Идентификация возможных угроз осуществляется с использованием имеющейся информации об ИИБ, ранее проведенных аудиторских проверок и сведений из других источников. Информация о возможных угрозах ИБ может быть также получена от пользователей ИА, руководства Общества и других источников. Примеры типов угроз ИБ и их источники приведены в Приложении 3 к настоящей Методике.

23. Используя результаты прежних идентификаций угроз ИБ, необходимо учитывать, что происходит постоянная смена значимых угроз, особенно если изменяется бизнес-процесс или ИА.

24. Важным элементом процесса идентификации угроз ИБ является определение источников угрозы и механизмов реализации угрозы, на которых будет основана дальнейшая идентификация и оценка рисков, а также способы их обработки.

25. Идентификация уязвимостей проводится с целью определения недостатков и слабых мест в существующих средствах защиты ИА, которые могут быть использованы для реализации угроз ИБ. Для идентификации уязвимостей используются отчеты о предыдущих оценках рисков, замечания внутренних и внешних аудиторов, требования безопасности, результаты тестирования безопасности.

26. Уязвимости могут быть идентифицированы в следующих областях: организация работ, процессы и процедуры, персонал, физическая среда, конфигурация информационных систем, аппаратные средства, программное обеспечение и оборудование сети передачи данных, зависимость от внешних сторон и другие.

27. В качестве методов поиска уязвимостей могут быть использованы следующие методы:

1) проверки системной конфигурации вручную;
2) сетевое сканирование;
3) тестирование на проникновение программного обеспечения и оборудования сети передачи данных;
4) анализ программных кодов и другие.

28. Примеры уязвимостей в различных сферах ИБ, а также примеры угроз, которые могут использовать эти уязвимости, приведены в Приложении 4 к настоящей Методике.

29. Идентификация существующих средств защиты проводится с целью определения степени защищенности информационного актива от угроз, включая их соответствие предъявляемым к ИА требованиям ИБ.

30. Для идентификации средств защиты могут использоваться следующие мероприятия:

1) изучение документов, содержащих информацию о применяемых средствах защиты (документы, регламентирующие бизнес-процессы и работу с рассматриваемым ИА, план реализации мер защиты и другое);

2) осмотр средств защиты, сверка их фактической функциональности с документальным перечнем функций;

3) проверка реализованных средств защиты на предмет их правильной и эффективной работы;

4) анализ результатов внутренних и/или внешних аудиторских проверок ИБ Общества и мер, принятых по результатам устранения выявленных нарушений и замечаний

31. По результатам идентификации существующие методы и средства защиты могут быть определены как неэффективные, недостаточные или необоснованные. Для таких методов и средств защиты важно определить необходимость их удаления и замены на другие, более эффективные.

32. Результаты выполнения идентификации угроз ИБ, уязвимостей и средств защиты информационных активов фиксируются по форме согласно Приложению 5 к настоящей Методике.

§3. Оценка рисков ИБ

33. Оценка рисков ИБ направлена на анализ идентифицированных рисков ИБ и определения их уровня.

При оценке риска ИБ необходимо проанализировать степень его воздействия и вероятность его возникновения для каждого из свойств ИА.

Для анализа рисков ИБ предварительно проводится изучение причин возникновения рисков ИБ, их источников и возможных потерь в случае их реализации, учитывая результаты идентификации, угроз, уязвимостей, средств защиты ИА.

Мероприятия по оценке рисков ИБ проводятся экспертным путем, работниками СИБ и владельцем ИА (далее – эксперты). При необходимости, могут привлекаться в качестве эксперта работники СП, использующие рассматриваемые ИА. Актуализация оценки рисков ИБ проводится не реже одного раза в год, а также дополнительно проводится при изменениях используемых технологий, бизнес-процессов, внутренних документов Общества, также при идентификации новых угроз, уязвимостей, выявленных по результатам аудиторских проверок, расследований нарушений ИБ и других.

34. Для определения уровня риска ИБ необходимо провести оценку вероятности реализации угроз ИБ и степени последствий нарушения ИБ.

35. Для оценки вероятности реализации идентифицированных угроз ИБ проводится анализ следующих факторов:

1) данные о расположении источника угрозы ИБ;

2) информация о мотивации и квалификации источника угрозы ИБ и причинах его возникновения;

3) статистические данные о частоте ранее реализованных угрозах ИБ;

4) информация о способах и механизмах реализации угроз ИБ;

5) информация об уязвимости существующих средств защиты информационных активов.

Вероятность реализации угрозы ИБ оценивается согласно критериям, определенным в таблице 2 Приложения 1 к настоящей Методике.

36. При получении разных оценок экспертов принимается средняя оценка рассматриваемых показателей. При количественной оценке средней оценкой является округленное до целого значения среднее арифметическое оценки экспертов ([сумма оценки экспертов/количество экспертов], здесь [] - округление до целого значения), а средняя качественная оценка равна рассчитанной средней количественной оценке согласно таблицам 1 и 2 Приложения 1 к настоящей Методике.

37. Уровень каждого риска ИБ определяется экспертами на основе оценки вероятности реализации угроз ИБ и оценки степени последствий нарушения ИБ, приведенной согласно таблице 3 Приложения 1 к настоящей Методике.

Результаты проведенной оценки рисков ИБ регистрируются СИБ по форме КТ/Ф-31-05, согласно Приложению 5 к настоящей Методике.

По результатам проведенной оценки рисков ИБ СИБ составляется карта рисков ИБ, которая представляет собой схематичное отображение классификации рисков ИБ по степени их воздействия и вероятности их возникновения.

§4. Обработка рисков ИБ

38. Обработка рисков заключается в принятии решения о дальнейших действиях в отношении рисков ИБ с высокими и критическими уровнями, выявленными в результате проведенной оценки рисков.

39. Выбор мероприятий по обработке рисков ИБ проводится экспертным путем СИБ совместно с владельцем ИА.

40. Существуют следующие варианты обработки рисков или их комбинации:

1) минимизация риска;
2) устранение риска;
3) принятие риска;
4) передача риска.

41. Минимизация риска может быть достигнута путем внедрения новых или обновления существующих средств защиты. Выбор средств защиты должен быть оправданным и учитывать различные ограничения в их выборе, такие как:

1) временные;
2) финансовые;
3) технические;
4) эксплуатационные;
5) юридические;
6) трудовые и другие.

42. Устранение риска может быть наиболее выгодным решением и применяться в тех случаях, когда риски считаются слишком высокими или стоимость осуществления других вариантов обработки риска, превышает выгоду. В таких случаях может быть выполнена корректировка или пересмотр бизнес-процессов таким образом, чтобы исключить рассматриваемый риск.

43. Принятие риска означает отказ от каких-либо действий, направленных на снижение вероятности или влияния риска. Такие риски подлежат обязательному пересмотру, как минимум 1 раз в год.

44. Перенос риска заключается в делегировании риска другой стороне, которая может наиболее эффективно управлять данным видом риска. Перенос риска может быть осуществлен путем страхования потерь от его ущерба, либо путем заключения договора с поставщиком услуг, который будет контролировать риск.

45. Перенос риска может создать новые риски или изменить существующие, поэтому после принятия данной меры, необходима дополнительная переоценка риска.

46. Для реализации принятых решений по обработке рисков ИБ СИБ разрабатывается План по обработке рисков ИБ Общества (далее – План обработки) по форме согласно Приложению 6 к настоящей Методике.

§5. Мониторинг рисков ИБ

47. Мониторинг рисков ИБ проводится владельцем ИА и работниками СИБ, и направлен на анализ следующих факторов:

1) возникновение новых угроз ИБ и определение механизмов их реализации;
2) возникновение новых или усиление имеющихся уязвимостей;
3) изменение вероятности появления рисков ИБ;
4) изменение степени последствий реализации нарушений ИБ;
5) ухудшение эффективности существующих методов и средств защиты;
6) изменение источников реализованных рисков ИБ;
7) другое.

По результатам мониторинга, в случае выявление вышеуказанных факторов, СИБ инициируется переоценка рисков ИБ.

§6. Порядок и сроки организации управления рисками ИБ

48. Ежегодно, не позднее 20 февраля отчетного года, СП Общества направляют в СИБ на согласование результаты проведенной идентификации и оценки ИА по форме КТ/Ф-31-04, согласно Приложению 2 к настоящей Методике.

49. СИБ рассматривает полученные результаты оценки ИА на соответствие Приложению 2 к настоящей Методике и не позднее 10 марта отчетного года направляет на рассмотрение и утверждение Управляющему директору по безопасности перечень ценных ИА.

50. СИБ:

1) в срок до 1 апреля отчетного года идентифицирует риски ИБ для ценных ИА Общества;

2) в срок до 1 мая отчетного года совместно с владельцем ИА, проводит оценку и обработку идентифицированных рисков ИБ;

3) не позднее 20 мая отчетного года разрабатывает План обработки по форме КТ/Ф-31-06 и направляет владельцу ИА для рассмотрения и согласования.

51. В течение 10 (десяти) рабочих дней владелец ИА рассматривает План обработки, при наличии замечаний и предложений направляет их в СИБ либо сообщает об их отсутствии.

52. Согласованный План обработки в течение 10 (десяти) рабочих дней СИБ направляется на утверждение Управляющему директору по безопасности. Не позднее 3 (трех) рабочих дней после утверждения План обработки, СИБ направляет его в соответствующие СП для реализации мероприятий, предусмотренных в Плане обработки.

53. СИБ ежеквартально, не позднее 10-го рабочего дня, следующего за отчетным периодом, направляют ДУРиВК информацию об исполнении Плана обработки, либо изменения по мероприятиям и их срокам по форме КТ/Ф-31-07, согласно Приложению 7 к настоящей Методике.

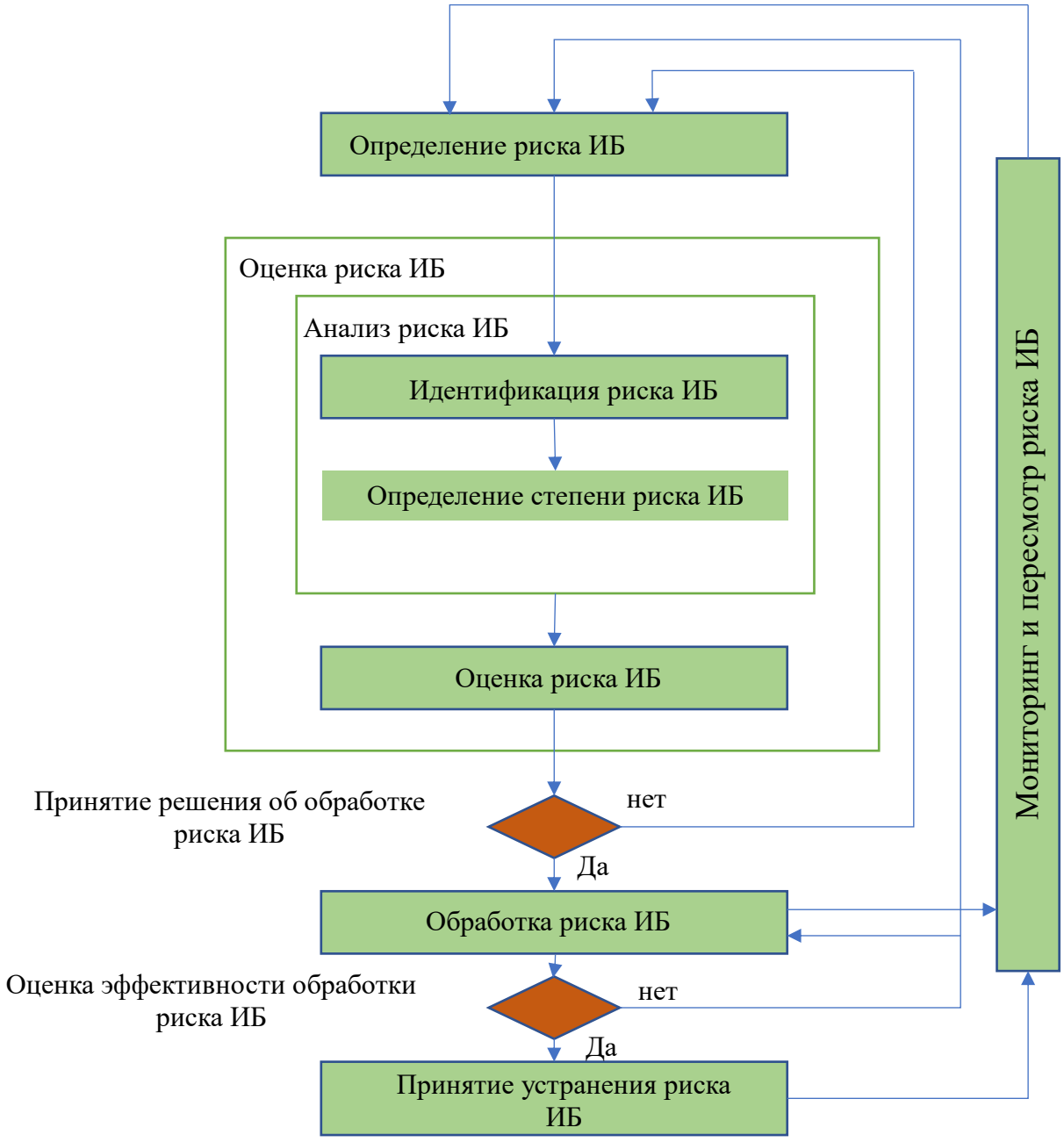

Рисунок 1 – Блок-схема методики управления рисками ИБ

Глава 4. Ответственность и полномочия

54. Управляющий директор по безопасности:
    1) рассматривает и утверждает План обработки;
    2) контролирует реализацию Плана обработки Общества;
    3) рассматривает и утверждает Перечень ценных ИА.
55. СП:
    1) идентифицируют и оценивают ИА в установленные сроки;
    2) обеспечивают и осуществляют мониторинг внутреннего контроля в СП;
    3) своевременно предоставляют в СИБ информацию по выявленным и/или реализованным рискам ИБ осуществляемых бизнес-процессов согласно Приложению 8 к настоящей Методике;
    4) выполняют План обработки в установленные сроки;
    5) подготавливают и своевременно предоставляют в СИБ информацию об исполнении Плана обработки.
56. СИБ:
    1) обеспечивает оперативное управление рисками ИБ Общества;
    2) своевременно идентифицирует риски ИБ;
    3) разрабатывает План обработки, реализует и контролирует его исполнение;
    4) своевременно регистрирует и принимает оперативные меры по реализованным рискам ИБ;
    5) обеспечивает надлежащий уровень ИБ в Обществе;
    6) разрабатывает и совершенствует методологическую базу по управлению рисками ИБ в Обществе;
57. ДУРиВК:
    1) принимает участие в разработке и совершенствовании методологической базы по управлению рисками ИБ в Обществе.
    2) осуществляет мониторинг исполнения СП Плана обработки;
    предоставляет консультационную помощь СИБ по требованиям настоящей Методики.

Глава 5. Документация

КТ/Ф-31-04 – Перечень информационных активов
КТ/Ф-31-05 – Реестр рисков ИБ
КТ/Ф-31-06 – План обработки рисков ИБ
КТ/Ф-31-07 – Отчет об оценке рисков ИБ

Глава 6. Ссылка

ISO 27005-2010 Менеджмент риска информационной безопасности.
СТ РК ИСО/МЭК 31010-2010 Методы оценки риска

ISO 9001:2015 Системы менеджмента качества. Требования.
СТ РК 9001-2016 Системы менеджмента качества. Требования.

Приложение 1
к Методике оценки рисков
информационной безопасности
АО «Казахтелеком»

Таблица 1. Оценка степени последствий нарушений ИБ

Степень последствий нарушения ИБ качественные/количественные шкалы	Описание ущерба вследствие нарушения ИБ		
	Нарушение непрерывности деятельности	*Потеря репутации Финансовые потери*	*Финансовые потери (влияние от размера риск-аппетита)*
Незначительное/1	Последствия от реализации риска незначительные. 1.Непрерывность производственного Процесса/предоставления услуги может остановиться, имеется возможность устранить причины остановки в течение 1 часа 2. Качество управления будет снижено, без угрозы потери управления 3. Качественные и количественные результаты производственного процесса/предоставления услуги ухудшатся, но результат останется приемлемым Фактические сроки достижения поставленных целей могут увеличиться	Краткосрочные негативные статьи ограниченного количества средств массовой информации, а также ограниченное распространение негативной информации в социальных сетях; нет воздействия на рейтинг; незначительное уменьшение поддержки заинтересованных сторон, снижение доверия некоторых взаимодействующих с Обществом сторон (контрагенты), снижение доверия со стороны некоторых лиц среди населения РК	До 15%
Заметное/2	Последствия от реализации риска значительные, но могут быть полностью исправлены 1.Непрерывность производственного процесса/предоставления услуги остановится, имеется возможность устранить причины остановки в течение 12 часов 2. Частичная потеря управления, с сохранением основных функций управления. 3. Ухудшит качественные и количественные результаты производственного	Периодичные негативные репортажи средств массовой информации, распространение негативной информации об Обществе в социальных сетях и блогах; не значительный эффект на рейтинг; уменьшение поддержки заинтересованных сторон. потеря доверия взаимодействующих с Обществом сторон (контрагенты) и населения РК	От 15% до 25%

	процесса/предоставления услуги, результат может оказаться неприемлемым . Фактические сроки достижения поставленных целей увеличатся		
Высокое/3	Последствия от реализации риска очень значительные, но могут быть исправлены до определенной степени 1. Непрерывность производственного процесса/предоставления услуги остановится, устранение причин остановки потребует время свыше 12 часов 2.Частичная потеря управления, с угрозой потери основных функций управления. 3.Неприемлемый результат производственного процесса, не соответствующий предъявляемым требованиям 4.Фактические сроки достижения поставленных целей значительно увеличатся	Постоянные негативные репортажи местных средств массовой информации, тиражирование информации в социальных сетях, блогах; негативный эффект на рейтинг; значительное снижение поддержки заинтересованных сторон. Распространение негативной информации об Обществе через СМИ, форумы и блоги, сети интернет, отказ некоторых взаимодействующих сторон (контрагенты) от сотрудничества с Обществом.	От 25% до 35%
Критическое/4	1. Критические последствия от реализации риска, которые могут быть устранены только частично. . Вызовет полную остановку производственного процесса/предоставления услуги	Постоянные негативные репортажи международных средств массовой информации, сильнейший негативный эффект на рейтинг. Серьезное ухудшение имиджа Общества, потеря доверия со стороны значительной части взаимодействующих с Обществом сторон (контрагенты) и населения РК.	Свыше 35%

Таблица 2. Оценка вероятности реализации угроз ИБ

Уровень вероятности реализации угроз ИБ качественные/количественные шкалы	*Описание*
Редко/1	Маловероятно, что произойдет реализация угроз ИБ. Нет статистики, мотивов и т.п., которые указывали бы на то, что это случится.
Время от времени/2	Существует вероятность, что произойдет реализация угроз ИБ. В прошлом происходили инциденты или существует статистика либо другая информация, указывающая на то, что такие или подобные инциденты прежде происходили или существуют признаки того, что источниками угрозы могут быть определенные причины для реализации таких действий.
Часто/3	Характеризуется наличием большой доли вероятности реализации угроз ИБ. Существует статистика или другая информация, указывающая на то, что произойдет реализация угроз ИБ. Существуют серьезные причины или мотивы у источников угрозы для осуществления действий.
Очень часто/4	Ожидаемая с большой уверенностью, что произойдет реализация угроз ИБ. В прошлом происходили инциденты либо существует статистика или другая информация, указывающая на то, что такие или подобные инциденты постоянно происходили.

Таблица 3. Определение уровня риска ИБ

Уровень риска ИБ		**Степени последствий нарушения ИБ**			
		Незначительное	*Заметное*	*Высокое*	*Критическое*
Уровень вероятности реализации угроз ИБ	*Редко*	Низкий	Низкий	Средний	Средний
	Время от времени	Низкий	Средний	Высокий	Высокий
	Часто	Средний	Высокий	Высокий	Критический
	Очень часто	Средний	Высокий	Критический	Критический

Приложение 2

к Методике оценки рисков
информационной безопасности
АО «Казахтелеком»

КТ/Ф-31-04 – Перечень информационных активов

1	2	3	4	5	6	7	8	9		
№	Наименование информационного актива (ИА)	Наименование бизнес-процессов, в которых используется ИА	Подразделение формирующее ИА	Подразделения-пользователи ИА	Средство обработки и хранения	Средство передачи	Свойства ИА, которые могут быть нарушены	Оценка степени последствия нарушения ИБ		
								Нарушение непрерывности деятельности	Потеря репутации	Финансовые потери
1 (пример)	Персональные данные клиента (физического лица)	Предоставление услуги ID Net	ДРБ	ДРБ	CRM 2.0	Корпоративная сеть передачи данных	Конфиденциальность	Критическое	Критическое	Заметное
							Целостность	Критическое	Высокое	Высокое
							Доступность	*Заметное*	Заметное	Заметное
2										

Приложение 3
к Методике оценки рисков
информационной безопасности
АО «Казахтелеком»

Пример типов угроз и их источники

Угрозы могут быть умышленными (D), случайными (A) или связанными с внешней средой (E).

Источники	Угрозы	Обозначение
Физические повреждения	Огонь	A, D, E
	Повреждение водой	A, D, E
	Загрязнение	A, D, E
	Уничтожение, повреждение оборудования или носителей	A, D, E
	Пыль, коррозия и обледенение	A, D, E
Естественные события	Климатические явления	E
	Сейсмические явления	E
	Метеорологические явления	E
	Наводнение	E
Потеря необходимых сервисов	Отказ кондиционирования или системы водоснабжения	A, D
	Отключение электропитания	A, D, E
	Отказ телекоммуникационного оборудования	A, D
Неисправности вследствие излучения	Электромагнитное излучение	A, D, E
	Тепловое излучение	A, D, E
	Электромагнитный импульс	A, D, E
Компрометация актива	Перехват и отправка компрометированного сигнала	D
	Подслушивание	D
	Кража носителей или документов	D
	Восстановление информации на носителях, отправленных на переработку	D
	Обнаружение (раскрытие) информации	A, D
	Данные из ненадежных источников	A, D
	Вмешательство в аппаратные средства	D
	Вмешательство в программные средства	D
	Угроза нарушения конфиденциальности	A,D
	Угроза нарушения доступности	A,D
	Угроза нарушения целостности	D
	Обнаружение местоположения	D
Технические отказы	Сбой работы оборудования	A
	Насыщение ИС	A, D
	Программный сбой	A
	Нарушение ремонтопригодности ИС	A, D
Несанкционированные действия	Несанкционированное использование оборудования	D
	Мошенническое копирование ПО	D
	Искажение данных	D
	Незаконная обработка данных	D
Компрометация функций	Ошибка в использовании	A
	Злоупотребление правами	A, D
	Фальсификация прав	D
	Отрицание действий	D
	Нарушение работоспособности персонала	A, D, E

Приложение 4
к Методике оценки рисков
информационной безопасности
АО «Казахтелеком»

Примеры уязвимостей в различных сферах ИБ и их угроз

Тип	Примеры уязвимостей	Угрозы
Аппаратные средства	Некачественное обслуживание, инсталляция с повреждённых носителей данных	Нарушение ремонтопригодности информационной системы
	Восприимчивость к влажности, пыли, загрязнению	Пыль, коррозия, обледенение
	Неэффективный контроль за внесением изменений в конфигурации	Ошибка в использовании
	Восприимчивость к изменениям напряжения	Потеря источника питания
	Незащищённое хранение	Кража носителей или документов
	Недостаток в осторожности при уничтожении	Кража носителей или документов
	Неконтролируемое копирование	Кража носителей или документов
Программное обеспечение	Отсутствие или проведение недостаточного программного тестирования	Превышение полномочий пользователя
	Нет 'выхода из системы' при оставлении рабочей станции	Злоупотребление правами
	Передача или многократное использование носителей, данных без надлежащего стирания	Злоупотребление правами
	Недостаточное количество проверок	Злоупотребление правами
	Некорректное распределение прав доступа	Несанкционированная модификация действующих систем
	Широко распространённое программное обеспечение	Искажение данных
	Сложный пользовательский интерфейс	Ошибка в использовании
	Недостатки в документировании	Ошибка в использовании
	Установление неправильных параметров программного обеспечения	Ошибка в использовании
	Отсутствие процедур по резервному копированию	Потеря информации
	Несанкционированное копирование	Кража
	Незащищенные соединения с сетями общего пользования	Несанкционированный доступ
	Некорректные даты	Ошибка в использовании
Сеть	Недостатки идентифицирующих и опознавательных механизмов для пользовательской аутентификации	Подделывание прав
	Незащищённые таблицы паролей	Несанкционированный доступ
	Ненадлежащее управление паролями	Подделывание прав
	Запуск излишних служб	Незаконная обработка данных
	Недоработанное или новое программное обеспечение	Программный сбой
	Неопределенные или неполные спецификации для разработчиков	Программный сбой
	Неэффективный контроль за внесением изменений	Программный сбой
	Неконтролируемая загрузка и использование	Использование вредоносного и

	программного обеспечения	нелицензионного программного обеспечение
	Недостатки в процедуре по резервному копированию	Искажение и утрата данных для восстановления
	Недостатки системы физической защиты (здания, дверей и окон)	Кража носителей или документов
	Нехватка доказательств посылки или получения сообщений	Отрицание действий
	Незащищённые линии связи	Подслушивание
	Незащищённый чувствительный трафик	Перехват данных, несанкционированный доступ
	Плохая совместная проводка	Отказ телекоммуникационного оборудования
	Неправильная сетевая архитектура	Удалённый шпионаж
	Передача паролей в открытом виде	Удалённый шпионаж
	Недостаточный менеджмент сетью (способность системы противостоять ошибкам маршрутизации)	Насыщенность информационной системы
	Незащищённые подключения к общедоступной сети	Несанкционированное использование оборудования
	Отсутствие процедур, гарантирующих возврат ресурсов при увольнении	Несанкционированный доступ
	Недостаточная компетенция персонала в вопросах ИБ	Ошибка в использовании
	Неправильное использование программного обеспечения и оборудования	Ошибка в использовании
	Возможная сложность в определении требований по безопасности	Ошибка в использовании
	Нехватка механизмов мониторинга	Незаконная обработка данных
	Недостаточный контроль за работой внештатных работников и работников, работающих вне рабочего графика	Кража носителей или документов
	Недостаточность определенных инструкции для правильного использования носителей передачи данных и обмена сообщениями	Несанкционированное использование оборудования
Местонахождение организации	Недостаточный физический контроль за доступом к зданию и его помещениям	Уничтожение оборудования или носителей информации
	Наводнение	Потеря источника питания
	Нехватка физической защиты здания, дверей и окон	Кража оборудования
	Недостатки в процедуре пересмотра прав доступа	Злоупотребление правом
	Упущение условий (относительно безопасности) в контрактах с клиентами и/или третьими лицами	Злоупотребление правом
	Недостатки в процедуре контроля над средствами обработки информации	Злоупотребление правом
	Нехватка процедур по выявлению риска и его оценки	Злоупотребление правом
	Полное/частичное отсутствие информации в отчётах о неисправности, в журналах администратора и пользователя	Злоупотребление правом
	Ненадлежащий ответ обслуживающего сервиса	Нарушение ремонтопригодности информационной системы
	Упущение условий (относительно ИБ) в	Нарушение ремонтопригодности

	соглашениях сервисного обслуживания	информационной системы
	Недостатки процедуры контроля за внесением изменений	Нарушение ремонтопригодности
	Недостатки формальной процедуры для менеджмента с документацией системы управления ИБ	Искажение данных
	Недостатки в процедуре предоставления общего доступа к информации	Данные из ненадёжных источников
	Ненадлежащее распределение обязанностей по ИБ	Отрицание действий
Прочее	Недостатки в реализации планов по непрерывности	Отказ оборудования
	Нехватка процедур за обеспечением ввода программного обеспечения в эксплуатируемые системы	Ошибка в использовании
	Нехватка отчётов в файлах регистрации администратора и оператора	Ошибка в использовании
	Нехватка процедур по обработке секретных данных	Ошибка в использовании
	Упущение условий (относительно ИБ) в контрактах с работниками	Незаконная обработка данных
	Нехватка определённого дисциплинарного процесса в случае возникновения нарушения ИБ	Кража оборудования
	Недостаточность определенных правил по использованию мобильной компьютерной техники	Кража оборудования
	Несоблюдение норм «чистого стола и чистого экрана»	Кража носителей или документов
	Нехватка ограничений на средства обработки информации	Кража носителей или документов
	Нехватка установленных контрольных механизмов в случае нарушений правил безопасности	Кража носителей или документов
	Нехватка регулярных пересмотров результатов контроля	Несанкционированное использование оборудования
	Нехватка процедур для того, чтобы сообщить об уязвимости безопасности	Несанкционированное использование оборудования
	Нехватка процедур согласования условий с интеллектуальной собственностью	Использование подделки или скопированного программного обеспечения

Приложение 5
к Методике оценки рисков
информационной безопасности
АО «Казахтелеком»

КТ/Ф-31-05 – Реестр рисков ИБ

№	Информаци-онный актив	Риск	Вероятность возникновения		Оценка вероятности	Возможные последствия					Оценка последствий	Оценка риска (вероятность * последствия)	План управления риском (для риска уровня >4) Может ссылаться на внешний план	Фактор риска после реализации плана
			Вероятность	Предыдущие проявления		Вероятность потери Клиента Общества	Потециальный вред ИС Общества	Не возможность соответствовать требованиям регулятора	Потенциальное несоответствие законодательству РК	Влияние на репутацию Общества				

Приложение 6
к Методике оценки рисков
информационной безопасности
АО «Казахтелеком»

КТ/Ф-31-06 – План обработки рисков ИБ

Общее описание риска

Дата заполнения	
Наименование риска	
Код риска	
Владелец риска/Должность	
ФИО	
Структурное подразделение	

Меры по управлению рисками

№	Фактор/последствие риска	Наименование мероприятия	План реализации (этапы мероприятия)	Срок реализации	Ответственное подразделение за мероприятие	Бюджет (тыс. тг)	Ожидаемый результат/ Цель	Показатель /расчет эффекта

Приложение 7

к Методике оценки рисков
информационной безопасности
АО «Казахтелеком»

КТ/Ф-31-07 – Отчет о выполненных мероприятиях по обработке рисков ИБ

Общее описание риска

Дата заполнения	
Наименование риска	
Код риска	
Владелец риска/Должность	
ФИО	
Структурное подразделение	

Меры по управлению рисками

№	Фактор/последствие риска	Наименование мероприятия	План реализации (этапы мероприятия)	Срок реализации	Ответственное подразделение за мероприятие	Статус исполнения (Да/Нет)	Бюджет (тыс.тг)	Ожидаемый результат/Цель	Показатель /расчет эффекта	Результат с учетом проведенных мер (эффект)

Приложение 8
к Методике оценки рисков
информационной безопасности
АО «Казахтелеком»

Форма регистрации рисковых событий по рискам ИБ

на ___ _____ 20___ года

Структурное подразделение АО «Казахтелеком»_____

Дата возникновения (обнаружения) события	Структурное подразделение Общества, в результате деятельности которого возникло событие	Описание события/факт нарушения	Причина возникновения события	Предполагаемый/ фактический размер последствий рискового события (ущерб/ убыток) *	Меры по минимизации / устранению рискового события или его последствий
1	2	3	4	5	6

* В графе "Предполагаемый/ фактический размер последствий рискового события (ущерб/ убыток)" указать возможную (фактическую) сумму убытка и/или другие возможные или фактические последствия

Исполнитель: _____ подпись: _____ дата:_____
Согласовано: _____