Приложение 2
к приказу ДИТ – филиала
АО «Казахтелеком»
от «07___»08.2024_ __№ 172__

Интегрированная система менеджмента/
Система менеджмента услуг/
Система менеджмента информационной безопасности

План мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации

ДИТ/ПЛ 05-28-45

Содержание

Глава 1. Назначение

1. Настоящий документ «План мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации» (далее – План) является частью системы управления информационными технологиями (далее - ИТ) Дивизиона информационных технологий – филиала АО «Казахтелеком» (далее – ДИТ).

2. Настоящий План определяет предупредительные организационно-технические мероприятия, обеспечивающие снижение рисков возникновения и влияния последствий аварийных ситуаций на деятельность ДИТ, а также порядок действий Работников при возникновении аварийной ситуаций, для обеспечения своевременного восстановления критичных ИТ сервисов ДИТ.

3. Целями настоящего Плана являются:

1) обеспечение безопасности работников ДИТ;

2) обеспечение непрерывного предоставления ИТ сервисов ДИТ;

3) снижение рисков несвоевременного восстановления критичных ИТ сервисов при возникновении аварийной ситуации.

4. Документы интегрированной системы менеджмента, касающиеся деятельности Общества в соответствии с ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, ISO 50001:2018, и их национальных аналогов СТ РК ISO 9001-2016, СТ РК ISO 14001-2016, СТ РК ISO 45001-2019, СТ РК ISO 50001:2019 (далее – ИСМ Общества)», а также Система менеджмента услуг (СМУ) в соответствии со стандартом ISO 20001:2018/ СТ РК ISO/IEC 20000-1-2016, Системы менеджмента информационной безопасности (СМИБ) в соответствии с требованиям СТ РК ISO/IEC 27001-2023.

Глава 2. Область применения

5. Действие настоящего Плана распространяется на ДИТ и носит рекомендательный характер для формирования собственных планов по обеспечению непрерывности деятельности в области ИТ и восстановления критичных ресурсов.

Глава 3. Термины, определения и сокращения

6. Термины и определения, применяемые в настоящей Документированной процедуре, соответствуют стандартам ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, ISO 50001:2018, ISO/IEC 20000-1:2018, и их национальных аналогов СТ РК ISO 9001-2016, СТ РК ISO 14001-2016, СТ РК ISO 45001-2019, СТ РК ISO 50001:2019, СТ РК ISO/IES 20000-1-2016, и СТ РК ISO 27001:2023.

7. В настоящем документе используются следующие обозначения и сокращения:

Восстановление критичных ресурсов – совокупный процесс, осуществляемый ДИТ с целью восстановления процессов.

Критичные ресурсы - виды бизнес процессов, которые необходимо осуществить для предоставления основных продуктов и услуг, позволяющие достигать наиболее важные цели (выполнение принятых на себя обязательств перед клиентами, осуществление расчетов и пр.), потеря которых может оказать в краткосрочный период времени максимальное негативное воздействие на Общество и подлежит восстановлению в кратчайшие сроки.

Команда восстановления - команда, ответственная за технический и имущественный анализ чрезвычайной ситуации и принятие мер к скорейшему восстановлению инфраструктуры и/или сервисов.

Непрерывность деятельности - стратегическая и тактическая способность Общества планировать свои действия и реагировать на критичные события с целью продолжения критичных процессов на определенном приемлемом уровне.

План по обеспечению непрерывности деятельности - план, определяющий цели, задачи, порядок, способы и сроки осуществления комплекса мероприятий, применяемых вовремя и/или после критичного события для экстренного возобновления критичных бизнес-процессов Общества на заранее согласованном минимальном (аварийном) уровне, а также регламентирующий исключительно восстановление деятельности структурных подразделений и/или бизнес-процессов Общества.

Процедуры обеспечения непрерывности деятельности ресурсами - применяемые Обществом процедуры, реализующие непрерывность деятельности Общества в рамках требований настоящих Правил.

Тестирование – деятельность, в ходе которой полностью или частично отрабатываются действия в соответствии с Планом.

8. Применяемые сокращения:

ДИТ - Дивизион информационных технологий;
ЗТД – Заместитель технического директора.
ИБ – Информационная безопасность;
ИТ – Информационные технологии;
ОАиК – Отдел анализа и контроля;
ОДС – Объединение «Дивизион Сеть»;
Общество – Акционерное Общество «Казахтелеком»;
ООУ – Отдел оперативного управления;
СУПБ – Система управления проблемными билетами;
ТД – Технический директор.

Глава 4. Ответственность и полномочия

9. Ответственность за выполнение настоящего Плана несет Технический директор ДИТ.

Глава 5. Описание плана

§1. Общие положения

10. Настоящий План является внутренним документом ДИТ и не подлежит передаче третьим лицам без санкции Руководства ДИТ.

11. Вся детальная информация, в частности контактная информация и процедуры восстановления (а также другая техническая информация) является «Конфиденциальной» и не подлежит передаче лицам/Работникам, которые непосредственно не вовлечены в процесс реализации плана по обеспечению непрерывности деятельности ДИТ в области ИТ и восстановления критичных ресурсов.

§2. Приоритет восстановления критичных ИТ сервисов и их компоненты

12. Критичные ИТ сервисы и их целевое время восстановления были определены в рамках интервью с представителями структурных подразделений ДИТ. На основе полученных данных все критичные ИТ сервисы, предоставляемые ДИТ распределены по приоритетам восстановления (Таблица 1. Приоритеты восстановления ИТ сервисов).

Таблица 1. Приоритеты восстановления ИТ сервисов

Приоритет восстановления	Контрольный срок
Критичный	До шести часов
Высокий	До двенадцати часов
Средний	До двух суток
Низкий	До четырех суток

13.Для каждого критичного ИТ сервиса был определен и проанализирован перечень компонентов, от которых зависит его предоставление. Результаты определения приоритетности критичных ИТ сервисов в Приложении «Приоритетность восстановления критичных ИТ сервисов ДИТ и их компоненты».

§3. План организационно-технических мероприятий

14. С учетом резервирования ключевых элементов инфраструктуры выработаны следующие организационно-технические мероприятия:

1)общие мероприятия для всех приоритетов восстановления;

2)мероприятия для критичного приоритета восстановления;

3)мероприятия для высокого приоритета восстановления;

4)мероприятия для среднего приоритета восстановления;

5)мероприятия для низкого приоритета восстановления.

15. При разработке организационно-технических мероприятий рассмотрены следующие факторы влияющие на обеспечение непрерывности работы компонент ИТ сервисов:

1)системы безопасности и жизнеобеспечения;

2)системы обеспечения отказоустойчивости;

3)системы резервного копирования и хранения;

4)организационные мероприятия.

16. Результаты определения плана организационно-технических мероприятий представлены

§4. Команды восстановления и обязанности работников

17. Для восстановления каждого критичного ИТ сервиса в ДИТ определена команда восстановления. Перечень ИТ сервисов и соответствующие им команды восстановления приведены в Приложении «Команды восстановления и ключевые поставщики критичных ИТ сервисов».

18. Руководство командой восстановления осуществляется Менеджером команды восстановлении, назначенный из числа работников ДИТ. В случае недоступности Менеджера команды восстановления его функции выполняет заместитель Менеджера команд восстановления.

19. Руководителем команд восстановления является Технический директор ДИТ.

20. Руководитель команд несет ответственность за:

1) оперативное управление командами восстановления и координацию их действий по восстановлению критичных ИТ сервисов и оборудования инженерной инфраструктуры (система электропитание, источник бесперебойного питания (далее – ИБП) и климатехники) в зоне ответственности ДИТ;

2) оперативное участие со структурными подразделениями ОДС при восстановлении оборудования инженерной инфраструктуры (система электропитание, ИБП и климатехники), которые находятся в зоне ответственности ОДС.

§5. Обязанности руководителя команды восстановления

21. В обязанности Руководителя команд восстановления входят:

1)взаимодействие с вышестоящим Руководством в рамках ДИТ;

2)координация и управление командами восстановления;

3)обеспечение обучения членов команд восстановления применению настоящего Плана;

4)организация тестирования настоящего Плана;

5)организация регулярного обновления настоящего Плана;

6)принятие решений о необходимости привлечения ключевых поставщиков.

§6. Обязанности менеджера команды восстановления

22. Менеджер команды восстановления имеет такие же обязанности по администрированию, координации, обучению, тестированию и поддержке Плана, как и Руководитель команд восстановления. Однако зона его ответственности распространяется только непосредственно на курируемую команду восстановления и вопросы, входящие непосредственно в зону ответственности данной команды.

§7. Обязанности члена команды восстановления

23. Члены команд восстановления ответственны за надлежащее и оперативное выполнение распоряжений Руководителя команд восстановления, инструкций Менеджера команды восстановления, в которую входит данный работник и надлежащее выполнение процедур восстановления систем.

§8. Внешнее хранение данных

24. Для следующего перечня данных и документов должно быть обеспечено внешнее хранилище. Рекомендуется обеспечить хранение на расстоянии не менее 10 километров от офиса:

1) План по обеспечению непрерывности деятельности ДИТ в области ИТ ресурсов;
2) Приоритетность восстановления критичных ИТ сервисов ДИТ и их компоненты;
3) Команды восстановления и ключевые поставщики критичных ИТ сервисов;
4) Процедура проведения плановых учений.

25. Территориально удаленным хранилищем может быть несгораемый сейф, расположенный у внешнего сервисного провайдера ДИТ, либо арендуемая банковская ячейка.

§9. Источники информации в случае аварийной ситуации

26. Источниками информации о возникновении аварийной ситуации являются:

1) внешние признаки, явно указывающие на возникновение аварийной ситуации (пожар, затопление, задымление, пламя, возгорание и т.п.);
2) программно-аппаратные средства защиты и мониторинга (срабатывание пожарной сигнализации и т.п.);
3) системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения аварийной ситуации;
4) пользователи, обнаружившие аномальное поведение в характере работы ИТ сервисов ДИТ.

§10. Реагирование на аварийную ситуацию

27. При получении информации об аварийной ситуации работник отдела оперативного управления (далее – ООУ) должны зафиксировать проблемный билет в системе управления проблемными билетами (далее – СУПБ) и далее выполнять обязанности ООУ, установленные в регламенте процесса устранения неисправностей ресурсов сетей телекоммуникации АО «Казахтелеком».

28. В случае наличия явных признаков аварийной ситуации (пожар, затопление и т.п.) работник ООУ оповещает соответствующие экстренные службы, согласно Приложения 3 к настоящему Плану «Контактные данные» и оповестить Технического директора ДИТ.

§11. Реагирование на аварийную ситуацию

29. Решение о необходимости активации Плана восстановления критичных ИТ сервисов принимает Руководитель команды восстановления или в случае его недоступности его заместитель, на основании анализа характера аварийной ситуации и ее последствия.

30. В случае принятия Руководителем команды восстановления решения о активации плана:

1) Руководитель команды восстановления (или его заместитель) информирует Руководство ДИТ об аварийной ситуации, планируемых мероприятиях и ожидаемых сроках их реализации;

2) по согласованию, Руководитель команды или заместитель доводит данное решение и необходимую информацию до соответствующих Менеджеров команд восстановления, согласно Приложения «Команды восстановления и ключевые поставщики критичных ИТ сервисов»;

3) по согласованию, Менеджеры команды восстановления или работник ООУ оповещает членов команды восстановления согласно приложения по форме Приложения «Команды восстановления и ключевые поставщики критичных ИТ сервисов», обеспечивает их необходимой информацией и сообщает им время и место сбора и в случае необходимости привлекаются ключевые внешние поставщики ИТ услуг;

4) учитывая то, что информация об аварийных ситуациях может иметь конфиденциальный характер, передача её третьим лицам без санкции Руководителя команды восстановления или Технического директора ДИТ запрещена.

31. Мобильные телефоны Руководителей команд, Менеджеров и членов команд восстановления включены 24х7 дней в неделю. При изменениях контактных данных, ООУ актуализирует информацию и уведомляет всех заинтересованных лиц об изменениях.

§12. Восстановление критичных ИТ сервисов

32. Одновременно с началом проведения восстановительных работ пользователи отсутствующих ИТ сервисов по возможности должны быть уведомлены о начале и предполагаемой длительности восстановительных работ. Это позволит пользователям перейти на альтернативные способы выполнения служебных обязанностей.

33. Последовательность восстановления ИТ сервисов должна выполняться в четком соответствии с утвержденными приоритетами восстановления, которые приведены в Приложении №1 «Приоритетность восстановления критичных ИТ сервисов ДИТ и их компоненты».

В процессе восстановления ИТ сервисов, команды восстановления должны учитывать необходимость восстановления компонентов, соответствующих ИТ сервисов.

34. В ходе восстановления могут потребоваться дополнительные ресурсы (люди, транспорт, программное и аппаратное обеспечение и т.п.). Задача Руководителя и Менеджеров команд восстановления – принять к сведению потребности структурных

подразделений и сообщить Руководству ДИТ о необходимых ресурсах и соответствующих затратах.

§13. Порядок действий команд восстановления при любой ситуации, повлекшей за собой полную или частичную остановку предоставления ИТ сервисов

35. Предполагается, что в результате ситуации ИТ сервисы были полностью или частично уничтожены.

36. В целом действия команд восстановления при ситуации, повлекшей за собой полное или частичное уничтожение ИТ сервисов, должны быть следующими:

1) анализ последствий аварийной ситуации;

2) детальное планирование восстановления;

3) восстановление ИТ сервисов согласно приоритетам;

4) предоставление отчетности Руководству ДИТ.

37. Детальная процедура восстановления при ситуации, повлекшей за собой полную или частичную остановку предоставления ИТ сервисов представлена в Приложение 4 к настоящему Плану «Процедура восстановления при ситуации, повлекшей за собой полную или частичную остановку предоставления ИТ сервисов».

§14. Порядок действий команд восстановления при нарушении политики и процедур информационной безопасности

38. Предполагается, что в результате нарушения политики и процедур информационной безопасности могла произойти:

1) компрометация информационной безопасности и получение несанкционированного доступа к ИТ сервисам ДИТ;

2) компрометация корпоративной сети ДИТ.

39. В случае компрометации информационной безопасности ИТ инфраструктуры ДИТ, действия команд восстановления включают, но не ограничиваются следующим перечнем шагов:

1) блокирование/отключение доступа к атакуемому ИТ сервису, либо остановка ИТ сервисов;

2) анализ и определение возможного источника атаки;

3) анализ последствий аварийной ситуации (проведение расследования);

4) анализ причин и выработка плана корректирующих мероприятий по восстановлению ИТ сервисов;

5) информирование Руководства ДИТ и при необходимости компетентных органов;

6) реализация корректирующих мероприятий, направленных на восстановление ИТ сервисов;

7)предоставление отчетности Руководству ДИТ по результатам проделанных работ.

40. В случае компрометации информационной безопасности корпоративной сети ДИТ, процедуры восстановления при этом остаются идентичными, с единственным отличием, что действия команд восстановления выполняются совместно с внешним поставщиком услуг размещения и поддержки корпоративной сети ДИТ.

41. Детальная процедура восстановления при компрометации информационной безопасности ИТ инфраструктуры и корпоративного сети ДИТ представлена в Приложение 5 к настоящему Плану «Процедура восстановления при нарушении политики и процедур информационной безопасности».

§15. Тестирование плана и анализ результатов тестирования

42. План по обеспечению непрерывности деятельности ДИТ в области ИТ ресурсов должен подвергаться регулярному тестированию, но не реже одного раза в год, выборочно в структурных подразделениях ДИТ.

43. Тестирование Плана восстановления критичных ИТ сервисов предусматривает применение следующих видов проверок:

1) тестирование с использованием анкет;
2) тестирование без остановки ИТ сервисов;
3) тестирование с частичной и полной остановкой ИТ сервисов.

44. Процесс тестирования должен быть документирован согласно Приложения 4 к настоящему Плану «Процедура восстановления при ситуации, повлекшей за собой полную или частичную остановку предоставления ИТ сервисов», Приложения 5 к настоящему Плану «Процедура восстановления при нарушении политики и процедур информационной безопасности».

45. Проведение полугодового анализа ОАиК по выявленным нарушениям/недостаткам, выявление коренных причин с целью дальнейшего совершенствования плана и процедуры тестирования с предоставлением отчета Техническому директору ДИТ.

§16. Обучение работников и распространение Плана

46. Начальники структурных подразделений технического блока, на регулярной основе проводят обучение и информирование Работников ДИТ, но не реже одного раза в год.

47. Работники, вовлеченные в процесс восстановления, обязаны ознакомиться с Планом и при необходимости проходить независимую профессиональную сертификацию в области обеспечения непрерывности бизнеса.

48. План, доводиться только до членов команд восстановления и Менеджеров команд восстановления. Обязательно предусматривается копия Плана у ЗТД ДИТ, ООУ и в регионах.

§17. Мониторинг исполнения организационно-технических мероприятий

49. Регулярно, но не реже одного раза в квартал необходимо выполнять мониторинг результатов исполнения организационно–технических мероприятий.

50. Результаты мониторинга должны быть формализованы и тщательно проанализированы. По результатам анализа вырабатывается план корректирующих мероприятий, направленный на полноценную реализацию организационно–технических мероприятий.

51. Рекомендуется, чтобы мониторинг исполнения организационно–технических мероприятий осуществлялся стороной независимой от их реализации.

§18. Порядок утверждения и внесения изменений

52. Настоящий План утверждается Генеральным директором ДИТ. Приложения настоящего Плана подлежат регулярной актуализации ООУ. Пересмотр и обновление настоящего Плана производится на ежегодной основе, а также в случае внесения изменений в список приложений, Приложения к настоящему Плану «Перечень критичных ИТ сервисов», «Организационная структура ДИТ» и т.д.

53. Работа по пересмотру настоящего Плана вносится в ежегодный план работы ООУ. Об изменениях настоящего Плана должны быть уведомлены все заинтересованные лица структурных подразделений ДИТ.

Глава 6. Документация

54. План организационно - технических мероприятий (Приложение 1 к Плану).

55. Перечень критичных ИТ сервисов (Приложение 2 к Плану).

56. Форма «Контактные данные» (Приложение 3 к Плану).

57. Процедура восстановления при ситуации, повлекшей за собой полную или частичную остановку предоставления ИТ сервисов (Приложение 4 к Плану).

58. Процедура восстановления при нарушении политики и процедур информационной безопасности (Приложение 5 к Плану).

Глава 7. Ссылки

59. ISO 9000:2015 Системы менеджмента качества. Основные положения и словарь.

60. ISO 9001:2015 Системы менеджмента качества. Требования.

61. ISO 14001:20015 Системы экологического менеджмента. Требования и руководство по применению.

62. ISO 45001:2018 Системы менеджмента профессиональной безопасности и здоровья. Требования.

63. СТ РК 9001-2016 Системы менеджмента качества. Требования.

64. СТ РК 14001-2016 Системы экологического менеджмента. Требования и руководство по применению.

65. СТ РК ISO 45001-2019 Системы менеджмента профессиональной безопасности и здоровья. Требования.

66. СТ РК ISO/IES 20000-1-2016 "Информационные технологии. Менеджмент услуг. Часть 1. Требования к системе менеджмента услуг".

67. ДИТ/ДП-05-08-01 «Управление документированной информацией».

68. ДИТ/ДП -05-28-50 «Процедура проведения плановых учений».

69. СТ РК ISO 50001-2019 Системы экологического менеджмента. Требования и руководство по применению.

70. ISO 50001:2018 Системы энергетического менеджмента. Требования и руководящие указания по применению.

71. ISO/IEC 20000-1:2018 Информационные технологии. Менеджмент сервисов. Часть 1. Требования к системе менеджмента сервисов.

72. СТ РК ISO/IEC 27001-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности».

Приложение 1
к «ДИТ/ПЛ-05-28-45 «План по обеспечению
непрерывности деятельности ДИТ в области ИТ ресурсов»
в утвержденной приказом АО «Казахтелеком» от _____ № ___

План организационно-технических мероприятий

№	Мероприятия
1	Обеспечение и выполнение требований регламента резервного копирования данных (back-up) систем, эксплуатируемых в ДИТ.
2	Обеспечение оповещение при получении аварийного сообщения в СУПБ или вручную аналитиком ООУ для работников ДИТ.
3	Обеспечение автоматического отключения серверов ИТ сервисов с обязательным оповещением пользователей в случае отключения основного источника питания и отказа/остановки работы дизельного электрогенератора.
4	Обеспечение рабочих станций источниками бесперебойного питания с возможностью стабилизации напряжения.
5	Организация кольцевой топологии корпоративной сети передачи данных, при которой все активные сетевые устройства имеют два независимых подключения.
6	Рекомендуется обеспечение внешнего хранения, на расстоянии не менее 10 километров, следующих данных: - резервных копий; - «План по обеспечению непрерывности деятельности ДИТ в области ИТ и восстановления критичных ИТ ресурсов».
7	Организация резервного центра обработки данных в дата центрах с возможностью дублирования следующих компонент ИТ сервисов: Аппаратное обеспечение, Программное обеспечение и Данные. Мероприятия для критичного приоритета восстановления.
8	Организация резервирования канала доступа к сети Интернет посредством резервирования последней мили (канала связи до узла доступа интернет провайдера) с возможностью дублирования конечного активного сетевого оборудования.
9	Мероприятия для высокого приоритета восстановления.
10	Организация телефонной связи от двух администраторов. Основной администратор должен обеспечить возможность переадресации входящих звонков на второго администратора в случае необходимости.
11	Обеспечение замены аппаратного обеспечения и комплектующих на складе. Склады не должны быть совмещены с серверными и коммуникационными помещениями.
12	Обеспечение образами (эталонные копии) серверных операционных систем с установленными приложениями.
13	Обеспечение хранения образов на внешних носителях в несгораемом сейфе.

14	Обеспечение автоматического контроля содержимого веб-сайта и в случае наличия компрометирующей информации автоматическое обновление содержимого из резервных копий.
15	Назначение и подготовка должностных лиц, отвечающих за организацию и осуществление следующих мероприятий: - оповещение хостинг провайдера об отсутствии доступности корпоративного веб-сайта; - замена аппаратных средств и восстановление приложении посредством образов; - восстановление ИТ сервисов из эталонных копии.

Приложение 2
к «ДИТ/ПЛ-05-28-45 «План по обеспечению
непрерывности деятельности ДИТ в области ИТ ресурсов»
в утвержденной приказом АО «Казахтелеком» от 07.08.2024_ № 172_

Перечень критичных ИТ сервисов.

№	ИТ сервисы	Критерий успешного восстановления
1	ABACUS	Успешная передача электронного письма между двумя соучастниками группы восстановления
2	Active Directory Microsoft	Пользователь видит главное окно системы, и система предоставляет ответ на запрос информации
3	ASAP	Пользователь видит главное окно системы, и система предоставляет ответ на запрос информации
4	BigData	Пользователь видит главное окно системы, и система предоставляет ответ на запрос информации
5	CRM (CRM 2.0, Siebel CRM филиалов, Siebel CRM ДКБ)	Пользователь видит главное окно системы, и система предоставляет ответ на запрос информации
6	Cramer NRI	Пользователь видит главное окно системы, и система предоставляет ответ на запрос информации
7	GENESYS	Пользователь видит главное окно системы, и система позволяет регистрировать проблемный билет и осуществляет поиск ранее зарегистрированные проблемные билеты.
8	СЭД	Бухгалтер может открыть главную книгу
9	ISMET.KZ	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
10	MoneyMap	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
11	Remedy ARS (СУПБ, УТО, СУЗТОРС, Ремонтооборот, СУИСТ1, СУИСТ2, ЦБР, НОВО, ППУА, Contour Reporter)	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации

12	T-Interconnect	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
13	SAP ERP	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
14	SOA платформа	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
15	Telecom.kz	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
16	VCIP ЦБД	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
17	АИСТУ Спутник	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
18	ГИС SmallWorld	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
19	ИнфраМенеджер	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
20	ИС ССП	Пользователь видит главное окно системы, и система позволяет регистрировать инциденты/запросы и осуществляет поиск ранее зарегистрированные инциденты/запросы.
21	Автоматизированная система мониторинга	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
22	Система выставления счетов (АСР 1.3 филиалы, АСР 1.3.5 ДИС, АСР 1.3.5 ДКБ, АСР ККМ, АСР Аренда каналов, АСР BiMEG, Справка Мегалайн)	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
23	Система отчетности	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
24	ССПОТ MD	Успешное создание файла/каталога на файл сервере

25	СТПМС	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
26	СУСТ Netcool	Администратор видит главное окно системы, и система предоставляет ответ на запрос информации
27	СУСТФ	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
28	ПАК CheckPoint	Предоставление доступа к панели управления vCloudDirector
29	ЦБС Amdocs	Доступность портала video.telecom.kz, доступ к просмотру видео с камер и архива(при его наличие).
30	IDHost	Доступность портала
31	VDC	Доступность портала
32	Интеллектуальная платформа	Доступность портала
33	SDP	Доступность портала
34	SmartCity	Доступность портала ismet.kz
35	ОВН	Доступность портала
36	ОФД ККМ	Доступность портала
37	Wi-Fi Target	Доступность портала
38	Wi Fi SOHO	Доступность портала
39	ARIS	Доступность портала
40	СУПП	Доступность портала
41	Idport.kz	Доступность портала
42	КЭПС	Доступность портала
43	mail.telecom.kz	Доступность портала
44	DNS	Доступность портала
45	ЭПР	Доступность портала
46	web-модуль PBD	Доступность портала
47	4telecom.kz	Доступность портала
48	Cisco UCM	Доступность портала
49	FTP	Доступность портала
50	СУДТП	Доступность портала
51	OpenAPI	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
52	NRI Router	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
53	ВКС - Телепрезенс	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации

54	СУМП	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
55	IOT	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
56	AntiCovid	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
57	Wi-fi B2B	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
58	СУБД Clickhouse АИС	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
59	ПТК «Автоматизация учебного процесса»	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
60	HSE Telecom	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
61	IVA MCU	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
62	АПК Anti-DDoS	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
63	Mirapolis HCM	Пользователь видит главное окно системы, и она предоставляет ответ на запрос информации
64	ИС «PostMonitoring»	Доступность портала
65	ИС «Метрологическая лаборатория»	Доступность портала
66	ИС «Эталонный справочник»	Доступность портала
67	ИС «Активация ресурсов GPON»	Доступность портала

Приложение 3
к «ДИТ/ПЛ-05-28-45 «План по обеспечению
непрерывности деятельности ДИТ в области ИТ ресурсов»
в утвержденной приказом АО «Казахтелеком» от _07.08.20204__ № 172

Контактные данные.

Экстренная служба	Контактные данные
Пожарная служба	101
Отделение милиции	102
Скорая помощь	103
Служба газа	104
Служба спасения	112

Приложение 4
к «ДИТ/ПЛ-05-28-45 «План по обеспечению
непрерывности деятельности ДИТ в области ИТ ресурсов»
в утвержденной приказом АО «Казахтелеком» от 07.08.2024___ № _172

Процедура восстановления при ситуации, повлекшей за собой полную или частичную остановку предоставления ИТ сервисов.

Действия по восстановлению	Ответственный за выполнение	Сделано (Да/Нет)
1. Проинформировать экстренные службы, смотри Приложение №3	Дежурный работник ООУ	
Проинформировать Руководителя команд восстановления, смотри Приложение № 2 *(к настоящему Приказу)*	Дежурный работник ООУ	
3. Проинформировать Менеджеров команд восстановления, смотри Приложение № 2 *(к настоящему Приказу)*	Дежурный работник ООУ	
4. Проинформировать ключевых участников команды восстановления и организовать их доставку к месту восстановления, смотри Приложение № 2 *(к настоящему Приказу)*.	Дежурный работник ООУ	
5. Проинформировать Руководство ДИТ.	Руководитель команд восстановления	
6. Получить всю возможную информацию о характере и масштабе аварийной ситуации, включая: 6.1. Проверить перечень ИТ сервисов и определить какие из сервисов не доступны.	Члены команды восстановления	
ИТ сервис	Отметить недоступные ИТ сервисы	
ABACUS		
Active Directory Microsoft		
ASAP		
BigData		
CRM (CRM 2.0, Siebel CRM филиалов, Siebel CRM ДКБ)		
Cramer NRI		
GENESYS		
СЭД		
ISMET.KZ		
MoneyMap		
Remedy ARS (СУПБ, УТО, СУЗТОРС, Ремонтооборот, СУИСТ1, СУИСТ2, ЦБР, НОВО, ППУА, Contour Reporter)		

T-Interconnect		
SAP ERP		
SOA платформа		
Telecom.kz		
VCIP ЦБД		
АИСТУ Спутник		
ГИС SmallWorld		
ИнфраМенеджер		
ИС ССП		
Автоматизированная система мониторинга		
Система выставления счетов (АСР 1.3 филиалы, АСР 1.3.5 ДИС, АСР 1.3.5 ДКБ, АСР ККМ, АСР Аренда каналов, АСР BiMEG, Справка Мегалайн)		
Система отчетности		
ССПОТ MD		
СТПМС		
СУСТ Netcool		
СУСТФ		
ПАК CheckPoint		
ЦБС Amdocs		
IDHost		
VDC		
Интеллектуальная платформа		
SDP		
SmartCity		
ОВН		
ОФД ККМ		
Wi-Fi Target		
Wi Fi SOHO		
ARIS		
СУПП		
Idport.kz		
КЭПС		
mail.telecom.kz		
DNS		
ЭПР		
web-модуль PBD		
4telecom.kz		
Cisco UCM		
FTP		
СУДТП		
OpenAPI		

NRI Router		
ВКС - Телепрезенс		
СУМП		
IOT		
AntiCovid		
Wi-fi B2B		
СУБД Clickhouse АИС		
ПТК «Автоматизация учебного процесса»		
HSE Telecom		
IVA MCU		
АПК Anti-DDoS		
Mirapolis HCM		
ИС «PostMonitoring»		
ИС «Метрологическая лаборатория»		
ИС «Эталонный справочник»		
ИС «Активация ресурсов GPON»		
6.2. Составить перечень приоритетных ИТ сервисов которые должны быть восстановлены незамедлительно и определить компоненты ИТ сервисов для немедленного восстановления, смотри Приложение № 1 *(к настоящему Приказу)*.	Члены команды восстановления	
6.3. Восстановить ИТ сервисы и их компоненты самостоятельно (определить в общем состояние и работоспособность систем), в противном случае перейти на шаг 6.4.	Члены команды восстановления	
6.4. Определить и оповестить ключевых поставщиков от которых зависит восстановление ИТ сервисов, смотри Приложение №2 *(к настоящему Приказу)*.	Менеджер команды восстановления	
7. Принять управленческое решение с Руководством ДИТ о необходимости организации резервной площадки.	Руководитель команд восстановления	
8. Организовать доступ к резервной площадке (если предусмотрена) для ключевых специалистов команды восстановления в соответствии со специальным списком.	Менеджер команды восстановления	
9. Организовать доступ к резервной площадке (если предусмотрена) для ключевых пользователей в соответствии со специальным списком.	Менеджер команды восстановления	
10. Запустить резервную площадку: 10.1. Убедиться, что все рабочие места готовы	Члены команды восстановления	

10.2. Перенаправить необходимый сетевой трафик для поддержки требуемых сервисов. 10.3. Организовать работу ООУ. Дежурный работник ООУ. 10.4. Организовать сервис печати и поддержки принтеров. 10.5. Начать поддержку бизнес-приложений. 10.6. Проверить доступность приложений. 10.7. Проверить и установить необходимое дополнительное оборудование.		
11. Получить актуальные ленты с резервными копиями из ближайшего хранилища.	Члены команды восстановления	
12. Начать процесс восстановления в соответствии с инструкциями по восстановлению ИТ сервисов (в случае если ИТ сервис был восстановлен автоматически (кластер и т.п.), то члены команд восстановления переходят к восстановлению следующего по приоритету ИТ сервиса).	Члены команды восстановления	
13. Записывать все проводимые изменения.	Члены команды восстановления	
14. Описать ситуацию в целом Руководству ДИТ и для отдельных структурных подразделений.	Руководитель команд восстановления	
15. Подготовить для Руководства ДИТ, в случае необходимости: • отчет о текущей ситуации; • ежечасный отчет об изменениях в устной форме.	Руководитель команд восстановления	
16. Провести анализ готовности ИТ сервисов к возврату в первоначальное состояние и возможности перехода в штатный режим эксплуатации.	Руководитель команд восстановления	
17. Начать возврат в первоначальное состояние и переход в штатный режим эксплуатации ИТ сервисов.	Члены команды восстановления	
18. Организовать, в случае необходимости круглосуточный режим работы и проживание команды восстановления (воспользоваться гостиничными услугами). Обеспечить команду восстановления едой.	Менеджер команды восстановления	
19. По результатам тестирования, обеспечить внесение корректировок в План восстановления критичных ИТ ресурсов	Руководитель команд восстановления	

Приложение 5
к «ДИТ/ПЛ-05-28-45 «План по
обеспечению непрерывности деятельности ДИТ в области ИТ ресурсов»
в утвержденной приказом АО «Казахтелеком» от 07.08.2024_ № 172___

Процедура восстановления при нарушении политики и процедур информационной безопасности.

Действия по восстановлению	Ответственный за выполнение	Сделано (Да/Нет)
1.Проинформировать Менеджера информационной безопасности/Поставщика услуг о взломе корпоративного веб-сайта с целью его блокирования.	Работник ООУ	
2. Блокировать доступ злоумышленнику к атакуемому сервису (блокировка учетной записи, настройка межсетевого экрана, изоляция точки подключения злоумышленника на сетевом оборудовании, физическое отключение точки подключения или сегмента сети на сетевом оборудовании)/ веб-сайту.	Менеджер информационной безопасности/ Поставщик услуг веб-сайта	
3. Проинформировать Руководителя команд восстановления.	Менеджер информационной безопасности	
4. Зарегистрировать факт атаки в журнале регистрации.	Менеджер информационной безопасности	
5. Получить всю возможную информацию об атаке/взломе веб-сайта, включая: 5.1. Системные журналы операционных систем 5.2. Журналы активного сетевого оборудования 5.3. Журналы бизнес приложений 5.4. Журналы межсетевого экрана 5.5. Журналы системы обнаружения вторжений (IDC)	Члены команды восстановления и Менеджер информационной безопасности/ Поставщик услуг веб-сайта	
6. Оценить масштаб атаки/взлома веб-сайта и возможное влияние на ДИТ.	Члены команд восстановления и Менеджер информационной безопасности/ Поставщик услуг веб-сайта	
7. Проинформировать о происшедшем Руководителя команд восстановления.	Менеджер информационной безопасности	

8. В случае необходимости проинформировать: Руководство ДИТ; компетентные органы.	Руководитель команд восстановления	
9. Начать процесс восстановления остановленных ИТ сервисов/веб-сайта в соответствии с инструкциями по восстановлению ИТ сервисов	Члены команды восстановления/ Поставщик услуг веб-сайта	
10. Подготовить отчетность для Руководства ДИТ (в случае необходимости).	Руководитель команд восстановления	
11. По результатам тестирования, обеспечить внесение корректировок в План и мероприятия восстановления.	Руководитель команд восстановления	