Приложение 1 к приказу
АО «Казахтелеком»
от_____ № _____

Регламент управления инцидентами информационной безопасности в АО «Казахтелеком»

Алматы, 2024

Содержание

Раздел 1. Назначение

1. Настоящий документ «КТ/Р-31-01 Регламент управления инцидентами информационной безопасности в АО «Казахтелеком»» (далее – Регламент) устанавливает единый порядок управления инцидентами информационной безопасности в АО «Казахтелеком».

2. Регламент разработан в соответствии с требованиями международных стандартов ISO 27001:2022, ISO 9001:2015, ISO 14001: 2015, ISO 45001:2018 и их национальных аналогов СТ РК ИСО/МЭК 27001, СТ РК ISO 9001-2016, СТ РК ISO 14001-2016, СТ РК ISO 45001-2019, а также законодательных актов Республики Казахстан.

Раздел 2. Область применения

3. Требования Регламента направлены на повышение уровня информационной безопасности в АО «Казахтелеком» (далее - Общество) посредством повышения защищенности информационной инфраструктуры и информационных систем Общества. Регламент является обязательным для применения во всех структурных подразделениях и Центральном аппарате АО «Казахтелеком».

Раздел 3. Термины, определения и сокращения

4. Термины и определения, применяемые в Регламенте, соответствуют стандартам ISO 27001:2022, ISO 9001:2015, ISO 14001: 2015, ISO 45001:2018 и их национальных аналогов СТ РК ИСО/МЭК 27001, СТ РК ISO 9001-2016, СТ РК ISO 14001-2016, СТ РК ISO 45001-2019:

1) Блок ИБСП – Блок информационной безопасности и специальных проектов ДИТ;

2) Входящая информация – материальный или информационный объект или услуга, входящий в этап процесса;

3) ДИТ - Дивизион информационных технологий – филиал Общества;

4) ДРСУП – Департамент развития систем управления предприятием ДИТ;

5) ДФД – Департамент «Фабрика данных» ДИТ;

6) Заявка – электронный документ в виде учетной записи базы данных ИнфраМенеджер, описывающий проблему, возникшую в ИТ-активе, и историю действий по ее решению;

7) ИБ – информационная безопасность;

8) ИИБ - Инцидент информационной безопасности **(**одно или несколько нежелательных или неожиданных событий информационной безопасности, которые имеют значительную вероятность компрометации бизнес-операций и реализация угрозы информационной безопасности);

9) ИнфраМенеджер – Система автоматизации процессов управления информационными технологиями в Обществе. Обеспечивает автоматизацию

процессов управления инцидентами и запросами на обслуживание, учета и движения ИТ-активов и иных процессов;

10) Исходящая информация – материальный или информационный объект или услуга, являющийся результатом выполнения этапа процесса;

11) ИТ-актив - компьютерное оборудование, серверы, сетевые устройства, программное обеспечение и другие технологические компоненты. Обеспечивают физическую инфраструктуру для хранения и обработки данных;

12) ИТ система - информационная система. Система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением соответствующих организационных ресурсов (человеческих, технических, финансовых и т. д.);

13) МЭ – межсетевой экран;

14) НКЦИБ - Национальный координационный центр информационной безопасности Республики Казахстан;

15) ОИБК – Отдел по информационной безопасности и контролю ДИТ, 2 линия реагирования и обработки ИИБ ОЦИБ;

16) ОС – операционная система;

17) ОЦИБ - оперативный центр информационной безопасности, осуществляющий защиту электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации Общества и проводящий реагирование на ИИБ;

18) ПО – программное обеспечение;

19) Проблемный билет - электронный документ в виде учетной записи базы данных ARS Remedy, описывающий проблему, возникшую в ИТ-активе, и историю действий по ее решению;

20) СИБ – Служба информационной безопасности АО «Казахтелеком»;

21) СМиА – Служба мониторинга и анализа ДИТ, 1 линия реагирования и обработки ИИБ ОЦИБ;

22) СОК3 – Служба Оперативного Контроля 3-го уровня Объединения «Дивизион «Сеть» - филиала АО «Казахтелеком»;

23) СП - Структурное подразделение Центрального аппарата/филиала Общества;

24) СУПБ – Система управления проблемными билетам ASR Remedy;

25) ТБ – Технический блок ДИТ;

26) Шаг – Часть этапа процесса, используется для детализации этапа процесса;

27) ЭБДР - электронная база данных реализованных рисков и инцидентов Общества на консолидированном уровне, инструмент управления рисками, используемый в целях постоянного мониторинга реализованных рисков;

28) ASR Remedy – Система управления проблемными билетами;

29) OSS&IT – Служба систем управления и администрирования OSS и IT Объединения «Дивизион «Сеть» - филиала АО «Казахтелеком»;

30) SOAR – система оркестрации, автоматизации и реагирования на ИИБ;

31) WEB интерфейс ИМ – web интерфейс модуля Службы поддержки в системе ИнфраМенеджер, который позволяет пользователям самостоятельно создавать

заявки и отслеживать ход их решения, исполнителям - отрабатывать заявки по зоне ответственности;

32) WEB-платформа НКЦИБ – web-платформа НЦКИБ, которая обеспечивает оперативное взаимодействие по отработке ИИБ между НКЦИБ и ОЦИБ.

Раздел 4. Ответственность и полномочия

5. Ответственным за организацию процесса управления ИИБ является Блок ИБСП.

6. Ответственность за выполнение Регламента несут участники процесса управления ИИБ.

7. Третьи лица, включая работников подрядных организаций, ответственных за эксплуатацию ИТ-актива и ИТ системы Общества, несут ответственность в части своевременного реагирования и устранения выявленных ИИБ и ответственность должна учитываться в договорах (соглашениях), заключаемых с ними. Ответственность за включение требований положений Регламента, в части реагирования и устранения ИИБ, в договоры/соглашения лежит на кураторе/инициаторе заключения договора, проекты таких договоров должны согласовываться с СИБ.

8. К работникам Общества, нарушившим положения Регламента, могут быть применены меры дисциплинарного взыскания в порядке, установленном законодательством Республики Казахстан и внутренними документами Общества.

Раздел 5. Управление инцидентами информационной безопасности

Глава 1. Общие положения

9. Управлению ИИБ подвергаются все ИТ-активы и ИТ системы Общества, при наличии технической возможности сбора данных.

10. Для повышения оперативности и эффективности процесса, все проводимые в рамках исполнения Регламента коммуникации и операции, должны документироваться в электронном виде в соответствующих системах, указанных в Регламенте.

11. Управление ИИБ предусматривает следующие действия:

1) идентификацию и анализ ИИБ;

2) создание плана мероприятий по устранению ИИБ;

3) устранение ИИБ;

4) подготовку отчета по выявленным и устраненным ИИБ;

5) корректирующие мероприятия и превентивные меры по недопущению ИИБ.

12. Для целей Регламента, для подтверждения процедуры документирования операций и коммуникаций по процессу равнозначными признаются:

1) сообщения, направленные посредством электронной почты с вложением документов в электронном виде;

2) служебные записки в корпоративной системе электронного документооборота с вложением документов в электронном виде;

3) наличие информации в соответствующих системах.

13. Целевое состояние процесса: получение информации об событиях ИБ всех информационных ресурсов, подключенных к информационной инфраструктуре Общества, в реальном времени.

14. Работники Общества, третьи лица ответственные за эксплуатацию ИТ-активов и ИТ систем, в случае самостоятельного обнаружения события ИБ обязаны информировать об этом начальника СМиА, начальника ОИБК, которые в свою очередь информируют Директора по информационной безопасности и специальным проектам ДИТ и Руководителя СИБ.

Глава 2. Функциональные разграничения между структурными подразделениями по инцидентам информационной безопасности

15. СМиА осуществляет:

1) выявление ИИБ, то есть проводит сбор доступной информации с рабочих мест работников, сетевых устройств и других ИТ-активах и ИТ системах с целью своевременного обнаружения и реагирования на возможные ИИБ;

2) проведение первоначального анализа события ИБ на предмет наличия ИИБ, угрозы ИБ, определение характера и степени опасности ИИБ;

3) реагирование на ИИБ – принятие незамедлительных мер по ликвидации ИИБ и минимизации его воздействия, в том числе инициация мероприятий по изоляции скомпрометированных систем, блокировке доступа и других действий;

4) регистрацию ИИБ в ЭБДР в соответствии с утвержденными Правилами по учету и анализу реализованных рисков и инцидентов АО «Казахтелеком»;

5) проведение расследования и анализа ИИБ - ИИБ должен быть расследован с целью выяснения его причины, масштаба и последствий, что позволяет принять меры по устранению ИИБ и для предотвращения повторения ИИБ в будущем.

16. ОИБК осуществляет:

1) сбор уточняющей информации с рабочих мест работников, сетевых устройств и других объектов информационной инфраструктуры, с целью дополнения данных, собранных СМиА для обнаружения и устранения возможности развития ИИБ;

2) проведение оценки характера ИИБ, его масштаба и потенциальных угроз для ИТ-актива/ИТ системы, анализа причин ИИБ и выявления уязвимости, которые могли быть использованы в противоправных действиях;

3) принятие мер для локализации и прекращения действия ИИБ, блокировку (отключение) узлов, имеющих признаки заражения вредоносным ПО и (или) использовании злоумышленниками, изменение настроек безопасности или временное отключение сервисов, по согласованию с СИБ и владельцем ИТ-актива /ИТ системы, в зависимости от масштаба и значимости отключаемого узла;

4) разработку мероприятий по ликвидации (локализации) установленных источников ИИБ организационными, организационно-техническими или техническими мерами, используя для этого аппаратные и программные средства защиты;

5) обеспечение информированности, формирование экспертного заключения по результатам разбора ИИБ для координации усилий по восстановлению ИТ-актива/ИТ сервиса и предотвращению будущих ИИБ;
6) проведение анализа ИИБ – разработку и предоставление в СИБ рекомендаций по усилению Политик и процедур ИБ.

17. СИБ осуществляет курирование вопросов ИБ Общества путем:
1) анализа защищенности информационных систем и ресурсов, периодического аудита (не реже 1 раза в квартал) имеющимися инструментами ИБ, с предоставлением отчетов состояния ИБ Управляющему директору по безопасности;
2) контроля за исполнением мероприятий по процессу управления ИИБ, согласно Блок-схеме процесса "Управление инцидентами информационной безопасности в АО "Казахтелеком" и Матрице рисков и контролей процесса «Управления инцидентами информационной безопасности в АО «Казахтелеком»;
3) осуществления инициативы по проведению обучающих курсов для работников Общества в целях предотвращения повторных ИИБ.

18. ТБ, ДФД, ДРСУП, OSS&IT, СОК3, третьи лица – являющиеся ответственными за эксплуатацию информационной инфраструктуры и информационных систем Общества осуществляют:
1) в случае самостоятельного обнаружения ИИБ, информирование обо всех идентифицированных ими ИИБ Блок ИБСП посредством системы «ИнфраМенеджер»/СУПБ;
2) реагирование на ИИБ принятием незамедлительных мер по остановке ИИБ и минимизации его воздействия, согласно плану мероприятий устранения ИИБ с указанием конкретных действий, полученных от Блока ИБСП и СИБ;
3) ликвидацию (локализацию) установленных источников ИИБ организационными, организационно-техническими или техническими мерами, согласно требованиям и конкретным действиям, полученным от Блока ИБСП и СИБ.

Глава 3. Идентификация и анализ инцидента информационной безопасности

19. Регистрация ИИБ:

Ответственный – Начальник СМиА;

Срок исполнения – 1 рабочий день с момента поступления сообщения о событии ИБ;

Входящая информация: Событие ИБ

Детальное описание действий при идентификации и анализе ИИБ:

Шаг 1. Получение информации о событии ИБ из соответствующих источников (система сбора и корреляций событий ИБ, антивирусное ПО, заявка ITSM, WEB-платформа НКЦИБ и т.д.).

Шаг 2. В течении 15 минут произвести регистрацию события ИБ в SOAR.

Шаг 3. Анализ события ИБ. На данном этапе происходит первичный анализ и определение события как «инцидент ИБ»/«не инцидент ИБ»:

1) в случае определения события как «не инцидент ИБ» производится закрытие события в SOAR;

2) в случае определения события как «инцидент ИБ» производится регистрация ИИБ в SOAR, WEB-платформе НКЦИБ и ЭБДР.

Исходящая информация:

Зарегистрированный ИИБ в SOAR, WEB-платформе НКЦИБ и ЭБДР.

20. Анализ ИИБ:

Ответственный – Директор по информационной безопасности и специальным проектам ДИТ;

Срок исполнения – 1 рабочий день с момента регистрации ИИБ;

Входящая информация:

Зарегистрированный ИИБ в SOAR.

Детальное описание действий при анализе ИИБ:

Шаг 1. Анализ ИИБ и определение области охвата (количество узлов, на которые повлиял данный ИИБ) и степени влияния на узлы (объекты, подверженные ИИБ).

Оценку степени влияния на узлы (объекты, подверженные ИИБ), необходимо осуществлять в соответствии с приложением 1 к Регламенту.

Шаг 2. План мероприятий по устранению ИИБ.

На данном этапе ОИБК производит разработку плана мероприятий по устранению ИИБ. План мероприятий должен включать:

1) детальное описание ИИБ;
2) перечень уязвимых узлов;
3) последовательность действий по ликвидации ИИБ или направленных на уменьшение воздействия ИИБ;
4) перечень действий по оценке влияния этих мероприятий на ИТ-актив подверженный ИИБ в целом.

Перечень мероприятий приведён в приложении 2 к Регламенту, но не ограничивается им и может быть дополнен в зависимости от степени влияния ИИБ.

На данном этапе производится анализ результатов сканирования ИТ-активов/ИТ систем, (подверженных ИИБ), сравнение результатов сканирования от всех средств выявления уязвимостей и подтверждение найденных уязвимостей в результате сравнения версий, настроек ПО и ОС, определённых по результатам сканирования и версий, настроек ПО и ОС, фактически используемых в системе подверженной ИИБ.

Шаг 3. Регистрация заявки в WEB интерфейсе ИМ/Проблемного билета в ASR Remedy с планом работ по устранению ИИБ.

Исходящая информация:

Заявка/Проблемный билет в системе «ИнфраМенеджер»/СУПБ с подробным Планом работ по устранению ИИБ.

Глава 4. Устранение инцидента информационной безопасности

21. Проведение мероприятий по устранению ИИБ.

Курирование проведения мероприятий по устранению ИИБ осуществляет СИБ. Ответственным за контроль над устранением ИИБ является Директор по информационной безопасности и специальным проектам ДИТ. Ответственные за

организацию и исполнение работ по устранению ИИБ являются руководители СП или третьи лица, ответственные за эксплуатацию и сопровождение ИТ-актива и ИТ систем, где зафиксирован ИИБ, совместно с Блоком ИБСП.

Срок исполнения проведения мероприятий по устранению ИИБ – до 7 рабочих дней с момента регистрации Заявки/Проблемного билета в системе «ИнфраМенеджер»/СУПБ;

Входящая информация:

Заявка/Проблемный билет в системе «ИнфраМенеджер»/СУПБ с подробным Планом мероприятий по устранению ИИБ.

Детальное описание операции устранения ИИБ:

При получении плана мероприятий в Заявке/Проблемном билете, его необходимо привести в исполнение.

При этом следует оценить:

1) риск возникновения проблемы совместимости версий ПО;
2) риск появления новых уязвимостей в ИТ системе либо объекте информационной инфраструктуры;
3) трудоёмкость предварительного тестирования мероприятий по ликвидации ИИБ;

Исходящая информация:

Исполненная Заявка/Проблемный билет в системе «ИнфраМенеджер»/СУПБ с внесением результатов действий по устранению ИИБ;

22. Контроль за исполнением Плана мероприятий по ИИБ

Ответственный – Директор по информационной безопасности и специальным проектам ДИТ;

Срок исполнения – 1 рабочий день с момента исполнения Заявки/Проблемного билета в системе «ИнфраМенеджер»/СУПБ;

Входящая информация:

Исполненная заявка/Проблемный билет в системе «ИнфраМенеджер»/СУПБ с подробным Планом мероприятий по устранению ИИБ;

Детальное описание исполнения Плана мероприятий по ИИБ:

Шаг 1. Проведение повторного исследования ИТ-актива/ИТ системы.

На данном этапе происходит проведение повторного исследования ИТ-актива/ИТ системы.

Шаг 2. Анализ и сопоставление результатов повторного исследования с исходными данными об ИИБ.

На данном этапе происходит подтверждение корректности внесённых в ИТ-актив/ИТ систему исправлений:

1) сведения о текущем состоянии ИТ-актива/ИТ системы;
2) подтверждение устранения ИИБ.

Шаг 3. Закрытие ИИБ в SOAR, WEB-платформе НКЦИБ и ЭБДР с детальным описанием устранения ИИБ.

Исходящая информация:

Закрытый ИИБ в SOAR, на WEB-платформе НКЦИБ и ЭБДР

Глава 5. Корректирующие и превентивные действия по выявленным и устраненным инцидентам информационной безопасности

23. Формирование отчета по выявленным и устраненным ИИБ.

Ответственный – Директор по информационной безопасности и специальным проектам ДИТ;

Срок исполнения – 1 рабочий день со дня закрытия ИИБ

Входящая информация:

Закрытая заявка в SOAR.

Детальное описание операции:

Отчёт об инциденте информационной безопасности формируется в соответствии с Приложением 3 к Регламенту.

Исходящая информация:

Отчёт об инциденте информационной безопасности.

24. Корректирующие и превентивные действия по выявленным и устраненным ИИБ.

Ответственный – Директор по информационной безопасности и специальным проектам ДИТ;

Срок исполнения – 7 рабочих дней со дня закрытия ИИБ.

Входящая информация:

Отчет об инциденте информационной безопасности.

Детальное описание операции:

Шаг 1. Аналитический/статистический анализ по устранению ИИБ.

На данном этапе производится анализ и сопоставления выявленных и устраненных ИИБ.

Шаг 2. Формирование корректирующих и превентивных мероприятий по предотвращению повторения ИИБ в будущем с указанием сроков исполнения и ответственных лиц.

Исходящая информация:

План корректирующих и превентивных мероприятий.

Глава 6. Контроль

25. Контроль за соблюдением положений Регламента осуществляется СИБ.

26. В рамках проведения процедур идентификации и анализа ИИБ работники Блока ИБСП имеют право применять все необходимые программные и технические средства, включая те, на которые установлен запрет использования внутренними документами Общества, но не запрещенных нормативными правовыми актами Республики Казахстан.

27. СИБ в случае обнаружения фактов нарушения положений Регламента, возникших в связи с недобросовестным исполнением работниками своих обязанностей в рамках Регламента или возникших в результате нарушения положений внутренних документов Общества в области ИБ, сообщает о данных

фактах непосредственному и курирующему руководителю работника нарушившего положения Регламента, для принятия соответствующих мер.

Раздел 6. Документация

28. Приложение 1 - Оценка степени риска события информационной безопасности.

29. Приложение 2 – Действия, принимаемые при обнаружении события информационной безопасности.

30. Приложение 3 - Отчет об инциденте информационной безопасности.

Раздел 7. Ссылки

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

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

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

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

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

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

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

38. Правила документирования и управления документацией в АО «Казахтелеком».

39. СТ РК ISO/IEC 27001:2022 Информационная технология Методы и средства обеспечения безопасности Системы менеджмента информационной безопасностью. Требования.

Приложение 1
к Регламенту управления инцидентами информационной безопасности в АО «Казахтелеком»
утвержденному приказом АО «Казахтелеком»
от_____ № _____

Оценка степени риска события информационной безопасности

Степень риска	Характеристики
1	Единичные попытки сканирования, сбора информации в отношении узлов внутренней сети. Активность со стороны известных вирусов или червей на отдельных (изолированных) узлах.
2	Единичные попытки сканирования, сбора информации в отношении узлов внутренней сети. Попытки использования уязвимости, с большой долей вероятности присутствующей на узлах сети.
3	Большое число попыток сканирования, сбора информации. Неудачная попытка DoS-атаки или «взлома». Контролируемая активность со стороны известных вирусов или червей на значительном числе узлов сети. Активность со стороны новых вирусов или червей на отдельных (изолированных) узлах.
4	Попытка DoS-атаки или «взлома», оказавшая незначительное влияние на отдельные узлы. Частично успешная атака с легко устраняемыми последствиями. Трудно контролируемая активность со стороны известных вирусов или червей на значительном числе узлов сети. Незначительный риск потери репутации или финансовых потерь.
5	Удачная попытка DoS-атаки или «взлома», оказавшая значительное влияние на узлы корпоративной сети. Значительный риск потери репутации или финансовых потерь. Значительное распространение вирусов или червей, с трудом подлежащее контролю.

Приложение 2
к Регламенту управления инцидентами информационной безопасности в АО «Казахтелеком»
утвержденному приказом АО «Казахтелеком»
от_____ № _____

Действия, принимаемые при обнаружении события информационной безопасности

Степень риска	Действия
1	Запись активности, связанной с ИИБ. Обновление узлов, подверженных атаке. Обновление антивирусного ПО, изменение правил фильтрации на МЭ.
2	Запись активности, связанной с ИИБ. Блокировка взаимодействия с узлом нарушителя. Обновление узлов, подверженных атаке. Обновление антивирусного ПО, изменение правил фильтрации на МЭ.
3	Запись активности, связанной с ИИБ. Блокировка взаимодействия с узлом нарушителя. Обновление узлов, подверженных атаке. Обновление антивирусного ПО, изменение правил фильтрации на МЭ
4	Запись активности, связанной с ИИБ. Изоляция узлов Блокировка взаимодействия с узлом нарушителя. Сбор доказательств для проведения расследования. Обновление узлов, подверженных атаке. Обновление антивирусного ПО, изменение правил фильтрации на МЭ
5	Запись активности, связанной с ИИБ. Выключение узлов или их изоляция. Блокировка взаимодействия с узлом нарушителя. Сбор доказательств для проведения расследования. Обновление узлов, подверженных атаке. Обновление антивирусного ПО, изменение правил фильтрации на МЭ.

Приложение 3
к Регламенту управления инцидентами информационной безопасности в АО «Казахтелеком»
утвержденному приказом АО «Казахтелеком»
от_____ № _____

Отчет об инциденте информационной безопасности

Дата возникновения ИИБ	
Тип ИИБ	
Описание ИИБ	

Описание ИИБ:

Контактная информация	
ФИО работника, обнаружившего ИИБ	
Наименование СП	
e-mail	
Номер телефона	
Дополнительная контактная информация	
Объект атаки	

Имя хоста или IP-адрес	
Назначение хоста (выполняемые функции)	
Источник атаки	
Имя хоста или IP-адрес	
Информирован ли владелец и/или провайдер владельца IPадреса?	
Описание ИИБ	
Дата	
Метод атаки	
Версии ОС и прикладного ПО на атакованном хосте	
Использованные уязвимости	
Прочая информация	
Результат анализа	

Анализ ИИБ:

Какие угрозы реализует ИИБ	
Степень влияния на бизнес-деятельность Общества	
Финансовый ущерб	
Ущерб репутации Общества	

Описание хронологии изменения характера ИИБ:

Дата, время	Описание характера ИИБ

Участники устранения ИИБ

№	Должность	ФИО	Контактная информация

Принятые временные меры по уменьшению воздействия ИИБ:

Принятые меры	Описание	Дата, время	ФИО работника, принявшего меры

Принятые меры по устранению причин возникновения ИИБ:

Принятые меры	Описание	Дата, время	ФИО работника, принявшего меры