Приложение
к Приказу АО «Казахтелеком»
от «__» _____ 2024 года
№ _____

ИНСТРУКЦИЯ
о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях АО «Казахтелеком»

Алматы, 2024

СОДЕРЖАНИЕ

Глава 1. Общие положения

1. Инструкция о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях АО «Казахтелеком» (далее - Инструкция) определяет порядок действий пользователей по реагированию на инциденты информационной безопасности и внештатные (кризисные) ситуации АО «Казахтелеком» (далее – Общество).

2. Инструкция разработана в соответствии с законодательством Республики Казахстан и Политикой информационной безопасности Общества, иными внутренними документами Общества.

3. Настоящая Инструкция распространяется на всех работников Общества.

Глава 2. Термины, определения и сокращения

4. В настоящей Инструкции используются следующие термины, определения и сокращения:

1) ИБ - информационная безопасность;

2) инцидент информационной безопасности (далее - инциденты ИБ) - 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;

3) 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;

4) информационно-коммуникационная инфраструктура (далее ИКИ) – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

5) пользователь – работник Общества, имеющий доступ к ИКИ;

6) СВТ – средства вычислительной техники;

7) СУПБ – Система управления проблемными билетам ASR Remedy;

8) система управления бизнес-процессами Общества – программное обеспечение, предназначенное для сбора, распределения запросов и эффективной поддержки корпоративных пользователей;

9) структурное подразделение ответственное за ИБ (далее СП ИБ) – подразделение, осуществляющее внутренний контроль за обеспечением ИБ в Обществе;

10) объект информатизации (далее - ОИ) – электронные информационные ресурсы, программное обеспечение, интернет-ресурс и информационно-коммуникационная инфраструктура;

11) SOAR – система оркестрации, автоматизации и реагирования на ИИБ

12) информационная система (далее- ИС) - Система, предназначенная для

хранения, обработки, поиска, распространения, передачи и предоставления информации с применением соответствующих организационных ресурсов (человеческих, технических, финансовых и т. д.);

13) информационный ресурс (актив). (далее- ИР) – Упорядоченная совокупность информации, представленная в электронном виде (файлы, базы данных, алгоритмы, компьютерные программы, приложения и т.д.) содержащаяся, хранящаяся, обрабатываемая, передаваемая и используемая в информационных системах Общества (сети передачи данных, системы хранения, обработки, передачи, визуализации информации и т.п.)

Глава 3. Порядок действий в случае возникновения инцидентов ИБ в ИКИ Общества

§1. Инциденты ИБ

5. Инциденты ИБ могут возникнуть в результате преднамеренных действий злоумышленника или непреднамеренных действий пользователей, аварий или стихийных бедствий.

6. По степени серьезности и последствий инциденты ИБ подразделяются на следующие категории:

1) высокая - инциденты ИБ, приводящие к полному выходу из строя информационной системы, информационных ресурсов, ИКИ и неспособности выполнять свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации;

2) средняя – инциденты ИБ, приводящие к выходу из строя отдельных компонентов ИС, ИР, ИКИ (частичной потере работоспособности, потере производительности).

7. К инцидентам ИБ категории «Высокая» относятся: сбои и отказы сервисов ОИ Общества, несанкционированный доступ к ОИ Общества, несанкционированное изменение конфигурации ОИ.

8. К инцидентам ИБ категории «Средняя» относятся: выход из строя рабочей станции с потерей информации; сбой программного обеспечения ОИ; обнаружение вредоносных объектов в ИКИ Общества; несоблюдение установленных требований нормативно - технической документации по ИБ Общества.

9. Источниками информации о возникновении инцидентов ИБ (далее - Источник) являются:

1) пользователи, обнаружившие несоответствия, другие подозрительные изменения в работе, конфигурации ИС, ИР, ИКИ или средствах её защиты;

2) технические и программные средства защиты информации;

3) системные журналы операционных систем и телекоммуникационного оборудования, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения инцидента ИБ;

§2. Обязанности и действия ответственных работников Общества

10. В случае самостоятельного обнаружения работником инцидента ИБ, производится информирование обо всех идентифицированных ими инцидентов ИБ Блок информационной безопасности и специальным проектам Дивизиона информационных технологий – филиала АО «Казахтелеком» посредством системы «ИнфраМенеджер»/СУПБ.

11. С момента получения информации от источников, работники СП ИБ и при необходимости совместно с работниками выполняют следующие действия:

1) определяют является ли обнаруженное или сообщенное работником событие ИБ инцидентом ИБ;

2) локализуют область ИКИ, задействованной в инциденте ИБ;

3) ограничивают доступ к ОИ при необходимости, задействованным в инциденте ИБ;

4) собирают информацию о протекающем в реальном времени инциденте ИБ;

5) привлекают при необходимости компетентных специалистов для консультации и взаимодействия;

6) обеспечивают сохранность и должное оформление доказательств (снятие дампов памяти, при необходимости создание образа дисков и т.д.);

7) при обнаружении вредоносного объекта проводят первичный анализ, при необходимости глубокого анализа взаимодействуют с Национальным координационным центром информационной безопасности Республики Казахстан;

8) проводят анализ зафиксированных в SOAR всех инцидентов ИБ;

9) по результатам анализа вырабатывают предложения по улучшению защитных мер и исключению повторного появления инцидента ИБ;

10) ведут учет инцидентов ИБ в SOAR;

11) оформляют служебную записку на имя Управляющего директора по безопасности о факте возникновения инцидента ИБ.

12. Ответственные администраторы серверного и сетевого оборудования, а также работники проводят работы по устранению инцидента ИБ в зоне своей ответственности.

§3. Требования по разработке процедур восстановления работы в случае их остановки

13. Ниже приведены ситуации по возможным внештатным (кризисным) ситуациям и действия по устранению.

I	**Техногенные угрозы**	
1	**Перебои в электроснабжении**	
1.1.	Нарушение подачи электроэнергии	Перевод работы основных серверов и критических рабочих мест на работу от источника резервного электропитания
2	**Отказ компьютерного оборудования**	
2.1	Отказ серверов	Переход на резервный сервер, восстановление работоспособности основного сервера и переход на восстановленный сервер
2.2	Отказ рабочих станций	Переход на резервное рабочее место, восстановление

		работоспособности основного рабочего места и переход на восстановленное рабочее место
3	**Отказ коммуникационного оборудования**	
3.1	Отказ коммуникационного оборудования	Переход на резервное оборудование, восстановление работоспособности основного оборудования и переход на восстановленное оборудование
3.2	Отказ канала связи провайдера	Переход на резервный канал связи, восстановление работоспособности основного канала связи и переход на восстановленный канал связи
3.3	Отказ телефонной связи	Переход на резервные телефонные каналы связи, восстановление работоспособности основных каналов связи и переход на восстановленные каналы связи
4	**Атаки злоумышленников**	
4.1	Отказ серверов	Ликвидация уязвимости в защите и переход на резервный сервер, восстановление работоспособности основного сервера и переход на восстановленный сервер
4.2	Отказ рабочих станций	Ликвидация уязвимости в защите и переход на резервное рабочее место, восстановление работоспособности основного рабочего места и переход на восстановленное рабочее место
4.3	Отказ коммуникационного оборудования	Ликвидация уязвимости в защите и переход на резервное оборудование, восстановление работоспособности основного оборудования и переход на восстановленное оборудование
5	**Компьютерные вирусы**	
5.1	Отказ серверов	Ликвидация вируса и переход на резервный сервер, восстановление работоспособности основного сервера и переход на восстановленный сервер
5.2	Отказ рабочих станций	Ликвидация вируса и переход на резервное рабочее место, восстановление работоспособности основного рабочего места и переход на восстановленное рабочее место
6	**Аварии систем жизнеобеспечения**	
6.1	Отказ сантехнического оборудования	Вызов специалиста по ремонту оборудования. В случае повреждения оборудования переход на резервное оборудование, восстановление работоспособности основного оборудования и переход на восстановленное оборудование
6.2	Отказ кондиционерного оборудования	Вызов специалиста по ремонту оборудования. В случае выхода из строя оборудования переход на резервное оборудование, восстановление работоспособности основного оборудования и переход на основное оборудование
6.3	Отказ системы отопления	Вызов специалиста по ремонту. В случае выхода из строя оборудования переход на резервное оборудование, восстановление работоспособности основного оборудования и переход на основное оборудование
6.4	Отказ оборудования водоснабжения	Вызов специалиста по ремонту оборудования. В случае повреждения оборудования переход на резервное оборудование, восстановление работоспособности основного оборудования и переход на восстановленное оборудование
II	**Природные угрозы**	
1	**Ураганы**	
1.1	Повреждение помещений	Организация эвакуации работников, посетителей, оборудования из помещений. В случае повреждения оборудования переход на резервное оборудование, восстановление работоспособности основного оборудования

		и переход на восстановленное оборудование.
1.2	Эвакуация работников	Организация эвакуации работников
1.3	Эвакуация оборудования	Организация эвакуации оборудования
2	**Землетрясения**	
2.1	Эвакуация работников	Организация эвакуации работников
2.2	Эвакуация оборудования	Организация эвакуации оборудования
III	**Природно-техногенные угрозы**	
1	**Пожар**	
1.1	Эвакуация работников	Организация эвакуации работников
1.2	Эвакуация оборудования	Организация эвакуации оборудования

14. Действия по устранению причин нарушения работоспособности, возобновлению обработки и восстановлению поврежденных (утраченных) данных определяются функциональными обязанностями ответственных работников структурных подразделений.

15. Событие в обязательном порядке регистрируется дежурным работником, с указанием точного времени инцидента ИБ, краткого описания возникновения инцидента ИБ, с указанием Ф.И.О. оповещенных работников.

16. Вынос и внос оборудования из помещений, если развитие внештатной (кризисной) ситуации этого потребует, осуществляются работниками Общества, в рамках, возложенных на них задач, только по согласованию с руководством Общества.

17. Организацию работ и действий во внештатных (кризисных) ситуациях осуществляют в рамках, возложенных на них задач.

§4. Требования по осуществлению контроля за выполнением профилактических действий для предотвращения возникновения внештатных (кризисных) ситуаций

18. Непрерывность процесса функционирования ИКИ и своевременность восстановления ее работоспособности достигается:

1) проведением организационных мероприятий, разработкой и актуализацией документов по вопросам обеспечения непрерывности, резервирования и восстановления работоспособности ИС, ИР, ИКИ;

2) регламентацией процесса обработки информации с применением СВТ и действий работников;

3) назначением и подготовкой должностных лиц, отвечающих за организацию и осуществление практических мероприятий по обеспечению резервирования и восстановления информации;

4) четким знанием и строгим соблюдением всеми работниками, использующими СВТ, требований руководящих документов по обеспечению непрерывности, резервирования и восстановления;

5) применением различных способов резервирования ресурсов, эталонного копирования ПО и резервного копирования информационных ресурсов;

6) эффективным контролем за соблюдением требований настоящей Инструкции;

7) проведением анализа эффективности мер и средств обеспечения непрерывности, резервирования и восстановления работоспособности ИС, ИР, ИКИ, при необходимости разработкой и реализацией предложений по их совершенствованию.

§5. Требования по расследованию случаев возникновения инцидентов и других внештатных (кризисных) ситуаций

18. При необходимости по решению руководства Общества назначается комиссия и проводится служебное расследование по факту возникновения инцидента ИБ, с целью выяснения ее причин, оценки причиненного ущерба, определения причастных лиц и принятии соответствующих мер воздействия.

19. Состав комиссии определяет Управляющий директор по безопасности Общества, а её деятельность осуществляется в режиме конфиденциальности.

20. Комиссия проводит:

1) анализ и идентификацию причин инцидента ИБ, определение причастных лиц;

2) определение ущерба, нанесенного внештатной (кризисной) ситуацией;

3) планирование мер для предотвращения повторения, нейтрализации последствий (если это возможно);

4) анализ и сохранение доказательств, следов инцидента ИБ, улик и свидетельств;

5) определение мер взыскания с причастных лиц;

6) взаимодействие при необходимости с правоохранительными органами.

21. При сохранении улик, если есть возможность, ответственным структурным подразделением производится резервное копирование защищаемой информации, технических средств, вовлеченных в инцидент ИБ, включая события (логи).

22. По результатам деятельности комиссии составляется акт с описанием ситуации. К акту прилагаются поясняющие материалы (копии экрана, распечатки журнала событий, и др.). По результатам расследования организуются мероприятия по реализации предложенных комиссией мер.

23. При проведении расследований, необходимо ответить на следующие вопросы:

1) можно ли было предупредить внештатную (кризисную) ситуацию?

2) вызвана ли она слабостью средств защиты информации?

3) это первая внештатная (кризисная) ситуация такого рода?

4) достаточно ли имеющегося резерва?

5) есть ли необходимость пересмотра системы защиты?

6) есть ли необходимость пересмотра настоящей Инструкции?

Глава 4. Ответственность

24. Контроль за исполнением требований настоящей Инструкции осуществляет Служба ИБ Общества и руководители ответственных структурных подразделений Общества.

25. Ответственность за актуальность Правил, а также внесение в нее

изменений возлагается на Службу ИБ Общества.

26. Со стороны СП ИБ на постоянной основе производится анализ инцидентов ИБ по фактам нарушений требований защиты информации.

27. Руководители СП несут ответственность за своевременное доведение требований Инструкции до своих работников в части их касающейся и за выполнение работниками подразделений требований Инструкции.

28. Работники Общества несут ответственность в соответствии с законодательством Республики Казахстан за неисполнение или ненадлежащее исполнение требований Инструкции, и информирование об инцидентах ИБ в процессе своей деятельности.

29. СП ИБ Общества ответственно за выполнение административных и контролирующих функции по организационному и методическому управлению процессами реагирования на инциденты ИБ.

Глава 5. Порядок пересмотра Инструкции

30. Пересмотр Инструкции осуществляется на постоянной основе, но не реже одного раза в два года.

31. Внесение изменений и дополнений в Инструкцию осуществляется на основании решения Управляющего директора по безопасности.

32. Внеплановый пересмотр Инструкции осуществляются в случае:

1) изменения нормативно-правовых документов Республики Казахстан, НРД регулятора (регулирующих и надзорных органов), внутренних документов Общества, определяющих требования ИБ;

2) выявления снижения общего и/или частного уровня ИБ Общества (по результатам внутреннего или внешнего аудита);

3) существенных изменений организационной деятельности и/или инфраструктуры, ресурсов и бизнес-процессов Общества;

4) выявления существенных недостатков или противоречий данной Инструкции с другими внутренними документами Общества.

5) при выявлении недостатков в бизнес-процессах Общества, прямо или косвенно связанных рисков либо систематически происходящих инцидентах, повлекших за собой утерю информационных активов.

33. Содержание настоящей Инструкции, может дополняться, но не отменяться (заменяться), положениями других частных правил ИБ Общества и документами, разработанными на их основе

Глава 6. Вступление в силу. Срок действия

34. Настоящая Инструкция вступает в силу с момента его утверждения Председателем Правления и вводится в действие его соответствующим приказом.

35. Настоящая Инструкция обязательны для исполнения всеми Работниками.

Глава 7. Ссылка

36. ISO 27005-2010 Менеджмент риска информационной безопасности.

37. СТ РК ИСО/МЭК 31010-2010 Методы оценки риска
38. ISO 9001:2015 Системы менеджмента качества. Требования.
39. СТ РК 9001-2016 Системы менеджмента качества. Требования.