Приложение
к Приказу АО «Казахтелеком»
от «__» _____ 2022 года
№ _____

Политика сетевой безопасности АО "Казахтелеком"

Алматы, 2022

Оглавление

1 Термины, сокращения и определения

Авторизация – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ;
Администратор ИС – привилегированный пользователь, имеющий расширенные полномочия (привилегии) по настройке и эксплуатации ИС, а так же по управлению доступом к ИС;
Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности;
Бизнес-владелец ИР – субъект, структурное подразделение, отдел, служба, реализующее полномочия владения, пользования и распоряжения информацией ИР в соответствии со своими функциями, задачами и в пределах, установленных законом. Бизнес-владелец ИР определяется на этапе создания ИР;
ИБ – информационная безопасность. Состояние защищённости информационных ресурсов и систем, при которой обеспечивается их конфиденциальность, целостность, аутентичность и доступность, что достигается целым комплексом организационных и технических мер, направленных на защиту данных;
ИР – информационный ресурс (актив). В рамках настоящей Политики понимается упорядоченная совокупность информации, представленная в электронном виде (файлы, базы данных, алгоритмы, компьютерные программы, приложения и т.д.) и содержащаяся, хранящаяся, обрабатываемая, передаваемая и используемая в информационных системах Общества (сети передачи данных, системы хранения, обработки, передачи, визуализации информации и т.п.);
ИС – информационная система. Система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением соответствующих организационных ресурсов (человеческих, технических, финансовых и т. д.);
ИТ – информационные технологии, процесс создания, хранения, передачи, восприятия информации и методы реализации таких процессов;
РД – регламентирующая документация Общества (политики, стандарты, приказы, регламенты, руководства, инструкции и т.п.);
Общество – Акционерное Общество «Казахтелеком»;
Политика – утвержденная в Обществе настоящая Политика управления доступом к информационным ресурсам АО "Казахтелеком";
Пользователь – работник Общества или представитель третьей стороны, работающий с ИС Общества и использующий её ИР в соответствии с установленными правами и правилами доступа к информации;
СП – структурное подразделение Общества;
СП ИТ – структурное подразделение Общества, ответственное за ИТ, технические обслуживание и эксплуатацию ИР и ИС Общества;
Третья сторона, третье лицо – физическое или юридическое лицо, взаимодействующие с Обществом на основании договорных отношений;
Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа. Под субъектом доступа могут пониматься как пользователи и администраторы ИР Общества, так и служебные учетные записи, необходимые для функционирования ИР Общества.

2 Назначение Политики и область ее действия

1. Настоящая политика определяет общие принципы положений, правил и практических приемов, устанавливающих подход организации к использованию сетевых ресурсов и определяющих, как следует обеспечивать защиту сетевой инфраструктуры и сервисов Общества.

2. Политика является регламентирующим документом и предназначена для обязательного использования в Обществе.

3. Положения настоящей Политики направлены на:

1) создание единого подхода в обеспечении ИБ при обеспечении защиты сетевой инфраструктуры и сервисов Общества в целях контроля доступа к информации;

2) предотвращения неавторизованного доступа;

3) обеспечение авторизованного доступа к ИР, операционным системам и информации в системах приложений;

4) определение порядка и требований, реализация которых обязательна для обеспечения эффективности деятельности Общества, сохранения репутации и выполнения Обществом своих обязательств перед контрагентами;

5) разграничение полномочий и определение ответственности за обеспечение ИБ при обеспечении защиты сетевой инфраструктуры и сервисов Общества.

4. Положения настоящей Политики призваны снизить потенциальную опасность (риски) для Общества от ущерба, который может быть нанесен в результате несанкционированного использования ИР Общества.

5. Политика применяется ко всем ИР Общества, а также ко всем лицам (работникам Общества, третьим лица и т.п.), имеющим электронную (цифровую) форму доступа к ИР Общества.

6. Политика регламентирует порядок обеспечения защиты сетевой инфраструктуры и сервисов Общества, порядок контроля соблюдения положений Политики и ответственность за ее несоблюдение.

7. Политика предназначена для распространения внутри Общества и предоставления всем Руководителям, Работникам Общества и прочим заинтересованным лицам – участникам бизнес-процессов Общества.

8. Все исключения из правил и требований настоящей Политики должны быть согласованы со СП ИБ.

3 Общие положения и требования политики

9. Политика разработана в соответствии с законодательством Республики Казахстан в сфере ИБ, НРД регулятора (регулирующих и надзорных органов), Политикой ИБ Общества, Концепцией ИБ Общества, серией международных стандартов по ИБ ISO/IEC 27000, COBIT, ITIL, современным состоянием и ближайшими перспективами развития информационной структуры Общества и возможности современных организационно-технических методов защиты информации.

10. Пересмотр положений Политики осуществляется на постоянной основе, но не реже одного раза в два года.

11. Внеплановый пересмотр Политики осуществляется в случае:

1) изменения нормативных 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 и/или инфраструктуры, ресурсов и бизнес-процессов Общества;

4) выявления существенных недостатков или противоречий положений Политики с другими внутренними документами Общества;

5) при выявлении недостатков в бизнес-процессах Общества, прямо или косвенно связанных с информационной безопасностью, а также реализации корпоративных рисков либо систематически происходящих инцидентов, повлекших за собой утерю информационных активов.

12. Положения Политики, могут дополняться, но не отменяться (заменяться), положениями других внутренних политик ИБ Общества и документами, разработанными на их основе.

13. Дополнительную информацию о безопасной работе и защите информации в ИС Общества можно получить из других внутренних политик ИБ Общества.

14. Согласованные, формализованные процессы управления доступом к ИР Общества являются одним из базовых механизмов защиты информации в Обществе.

15. Все ИР Общества должны быть идентифицированы, учтены, систематизированы, категорированы в виде реестра ИР и иметь своих бизнес-владельцев.

16. Для каждого ИР Общества должны быть разработаны и поддерживаться в актуальном состоянии процедуры (инструкции, правила, требования и т.п.) по работе пользователей и администраторов ИС, согласованные со СП ИБ.

17. Программная и техническая составляющая каждого ИР Общества должна обслуживаться тем или иным уполномоченным эксплуатационным (операционным) СП.

18. Создание и ведение реестра ИР Общества возлагается в установленном порядке на СП ответственного за ИР,

19. Актуальный реестр ИР должен быть доступен всем пользователям в произвольный момент времени.

20. Информация о новом ИР (изменениях в имеющемся ИР) должна быть доведена СП – бизнес-владельцем ИР до уполномоченного за ведение реестра ИР СП в течение двух рабочих дней с момента появления в виде служебной записки или в иной официальной и принятой в Обществе форме, например, посредством автоматизированной электронной системы и т.п., согласованной и подписанной руководителем СП – бизнес-владельцем ИР.

21. Внесение изменений в реестр ИР осуществляется уполномоченным за ведение реестра ИР СП в течение двух рабочих дней с момента появления в виде служебной записки или в иной официальной и принятой в Обществе форме, например, посредством автоматизированной электронной системы и т.п., согласованной и подписанной руководителем СП – бизнес-владельцем ИР.

22. Использование ИР осуществляется в соответствии с инструкциями по эксплуатации к программному и аппаратному обеспечению, и прочими внутренними РД.

23. Запрещается умышленное выведение ИР из строя, блокировка доступа к ним и любые иные действия, препятствующие штатному режиму эксплуатации ИР.

24. Пользователи или иное ответственное лицо (подразделение) обязаны в установленной форме сообщать обо всех фактах (инцидентах), связанных с нарушением требований ИБ и положений Политики, нарушением правил доступа к ИР Общества, обнаружения сбоя в работе ИР и т.п. в СП ИБ.

25. На ИС подключенной к сети Общества должно быть установлено антивирусное ПО с настроенным автоматическим обновлением сигнатур, где это допустимо и технически возможно.

26. Сетевые устройства в Обществе должны обеспечивать отказоустойчивость предоставления сервиса и предусматривать возможность оперативного восстановления.

27. Пропускная способность сети передачи данных должна непрерывно контролироваться, для возможности оперативного реагирования на DDoS атаки с использованием средств защиты от целевых атак и методик предотвращения вторжения в инфраструктуру.

28. Должны быть определены правила доступа к сетевым сервисам Интернет, к которым работники Общества должны иметь ограниченный доступ.

29. Должны быть определены правила доступа к ИР и ИС Общества.

30. Для осуществления фильтрации (пропуска или блокировки) потока данных, необходимо использование межсетевых экранов с применяем правил доступов, необходимым и достаточным для функционирования сервиса.

31. Необходимо обеспечение отключения неиспользуемых служб на всех ИС и ИР.

32. Обеспечение анализа состояния потоков данных на предмет нарушений и взломов, посредством систем обнаружения вторжений, которые позволяют обнаружить и предотвратить различные виды взломов.

33. Проведение проверки эффективности средств обеспечения информационной безопасности.

34. Предоставление доступа к ИР и ИС может осуществляться только в законных целях, не противоречащих интересам Общества и законодательству Республики Казахстан.

35. Действия пользователей и администраторов ИР Общества должны протоколироваться в рамках предоставляемого доступа к ИР.

36. Журналы аудита событий информационной/сетевой безопасности ИР и ИС Общества должны быть информативны, защищены от модификации и храниться в течении срока, потенциально необходимого для использования для расследования возможных инцидентов, связанных с нарушением ИБ, но не менее трех лет и находится в оперативном доступе не менее двух месяцев.

4 Порядок обеспечения сетевой безопасности

37. Доступ к ИР Общества всем пользователям предоставляется только на основании документально оформленных и согласованных, в том числе и с их бизнес-

владельцами, заявок. По умолчанию определяется отсутствие доступа. Оформление, согласование и утверждение заявок при предоставлении доступа к ИР должно осуществляться в установленном порядке и с учетом требований положений настоящей Политики.

38. Сетевая доступность к ИР должна соответствовать требованиям и формам реализации, разработанным и принятым в Обществе и содержать следующую минимальную информацию:

1) данные о функциональном назначении ИР;

2) наименование ИР в соответствии с реестром;

3) перечень портов, протоколов и ip-адресов для взаимодействия, необходимых и достаточных для функционирования ИР;

4) логическая и физическая схема подключения ИР;

5) бизнес владелец ИР.

39. Для предоставления доступа к/от ИР необходимо выполнение одного из следующих условий:

1) доступ необходим для выполнения пользователем должностных обязанностей в соответствии со своим должностными инструкциями и полномочиями;

2) доступ к/от ИР необходим для взаимодействия с другими ИР;

40. Лицо, инициирующее предоставление доступа, обязано представить соответствующее обоснование необходимости предоставления доступа.

41. Общий порядок предоставления доступа к ИР Общества должен включать следующие этапы:

1) инициатор, в лице руководителя (замещающего лица) заинтересованного СП, в установленном порядке оформляет заявку на предоставление доступа к/от ИР, руководствуясь реестром ИР.

2) заявка проходит согласование у бизнес-владельца (-ев) ИР;

3) заявка проходит согласование в СП ИБ, которое в течение одного рабочего дня проверяет наличие основания на доступ к ИР согласно заявке. В случае если доступ к ИР согласно заявке по какой-либо причине не может быть предоставлен, заявка возвращается инициатору, с подробным описанием причины отказа.

4) В случаи необходимости временного предоставления доступа СП ИБ осуществляет предоставление доступа на установленный срок действия;

5) по истечению установленного срока действия предоставленного доступа к ИР осуществляется завершение предоставления доступа СП ИБ с уведомлением инициатора и бизнес-владельца (-ев) ИР Общества.

6) информация об утвержденных заявках предоставления доступа к ИР должна фиксироваться соответствующими средствами протоколирования (ведения аудиторского следа), используемые в рамках управления доступом к ИР.

42. Предоставление доступа для ИР третьих лиц должно осуществляться только на основе действующих договоров и/или соглашений.

43. Доступ третьих лиц ИР к ИР Общества должен предоставляться на период и в объеме, необходимых для проведения работ на основании соглашений о соблюдении требований ИБ, которые должны содержать положения о конфиденциальности, условия о возмещении ущерба, возникающего вследствие нарушения ИБ, а также сбоев в работе ИР и нарушения их безопасности, вызванных вмешательством третьих лиц.

44. На основании проведения оценки риска ИБ, связанного с доступом ИР третьих лиц, СП ИБ должны предусматриваться следующие организационные и/или программно-технические меры по контролю деятельности третьих лиц:

1) проверка результата деятельности ИР третьих лиц;

2) ведение аудиторского следа по действиям ИР третьих лиц;

3) запись сессии доступа к информационным активам специальными программно-техническими комплексами.

45. СП ИБ обязано проводить периодический мониторинг (аудит) соблюдения правил обеспечения сетевой безопасности.

5 Порядок изменения правил доступа

46. В случае необходимости предоставления дополнительных правил по доступу к уже используемому им ИР следует действовать в соответствии с положениями настоящей Политики, регламентирующими порядок предоставления доступа к ИР.

47. В случае необходимости замены (полной или частичной) полномочий по доступу к уже используемому им ИР следует действовать в соответствии с положениями настоящей Политики, регламентирующими порядок отмены доступа к ИР.

6 Порядок отмены правил доступа

48. Отмена прав доступа к/от ИР и/или блокировка происходит в случаях:

1) изменения функциональных задач ИР;

2) истечения периода действия заявки (срока действия доступа);

3) изменения технологических процессов обработки информации таким образом, что доступ более не требуется;

4) нарушения правил доступа к/от ИР;

5) отсутствия производственной необходимости;

6) завершения договорных соглашений с третьими лицами;

7) по иным требованиям руководства Общества.

49. Отмена прав доступа должна быть инициирована в течение одного рабочего дня с момента возникновения соответствующего события (факта).

50. Обязанности по инициированию отмены доступа пользователя к ИР возлагаются на бизнес владельца ИР.

51. Информация об инициировании отмены доступа (с указанием причины) доводится в установленной официальной и принятой в Обществе форме, например, посредством автоматизированной электронной системы и т.п. руководителем заинтересованного СП до СП ИБ.

52. Фактическая реализация отмены доступа к ИР осуществляется уполномоченным СП – бизнес владельцем ИР, после получения согласования со стороны СП ИБ.

53. Информация об отмене доступа к/от ИР должна фиксироваться соответствующими средствами протоколирования (ведения аудиторского следа) в рамках управления доступом к ИР.

7 Контроль правил доступа

54. Со стороны СП ИБ на периодической основе должна производиться проверка (аудит) соответствия правил доступа к/от ИР в соответствии с требованиями положений Политики.

55. Для обеспечения эффективного контроля доступа необходимо вести официальный процесс регулярной проверки правил доступа к/от ИР, отвечающий следующим требованиям:

1) правила доступа ИР должны проверяться через регулярные интервалы (не реже одного раза в полгода), а также после внесения каких-либо изменений в ИР;

2) правила доступа ИР должны проверяться и переназначаться при изменении их функциональных задач;

56. Контроль над выполнением процедур управления доступом ИР должен включать:

1) контроль над добавлением, удалением и изменением портов, протоколов, ip-адресов;

2) немедленное блокирование прав доступа при изменении функциональных задач ИР;

3) включение ИР третьих лицам для взаимодействия с ИР Общества, только на время выполнения работ (соглашения);

4) ознакомление с правилами и процедурами аутентификации всех пользователей, имеющих доступ к сведениям ограниченного распространения;

5) использование механизмов аутентификации при доступе к любой базе данных, содержащей сведения ограниченного распространения, в том числе доступе со стороны приложений, администраторов и любых других пользователей;

6) разрешение запросов и прямого доступа к базам данных только для администраторов баз данных;

7) блокирование доступа к/от ИР при выявлении по результатам мониторинга (просмотра, анализа, аудита) журналов регистрации событий безопасности действий ИР, которые отнесены оператором (администратором) к событиям нарушения ИБ.

57. Контроль и периодический пересмотр правил доступа к/от ИР должен осуществляться в процессе аудита ИБ в соответствии с установленными процедурами.

8 Роли и ответственность

58. Контроль за выполнением требований и правил возлагается на структурное подразделение ИБ Общества.

59. Ответственность за актуальность настоящей Политики, а также внесение в нее изменений возлагается на структурное подразделение ИБ Общества.

60. Ответственность за обеспечение должного исполнения требований и правил Политики возлагается на все заинтересованные структурные подразделения Общества в рамках их полномочий и в соответствии с положениями, установленными настоящей Политикой и разработанными на ее основе документами.

61. Руководители структурных подразделений несут ответственность за своевременное доведение требований Политики до работников их подразделений

и/или представителей третьих сторон в части их касающейся и за выполнение работниками их подразделений и/или представителями третьих сторон требований Политики.

62. Структурное подразделение ИБ Общества ответственно за надлежащую организацию и осуществление общего контроля за соблюдением требований и правил настоящей Политики, а также за выполнение административных и контролирующих функции по организационному и методическому управлению процессами обеспечения сетевой безопасности.

63. Бизнес-владельцы ИР несут ответственность за согласование доступа к/от ИР.

64. Реализация положений настоящей Политики и процедур, связанных с операционным (эксплуатационным) сопровождением процессов управления доступом к/от ИР и поддержкой пользователей ИР, возлагается на структурные подразделения Общества, которые обеспечивают технические поддержку и сопровождение операционной деятельности пользователей и технических систем и средств Общества, обеспечивающих работу ИР.

65. Все пользователи ответственны за свои действия при работе с ИР Общества и обращении с защищаемыми ИР Общества, а также за исполнение требований и правил, установленных настоящей Политикой и внутренними документами, разработанными на ее основе.

66. В случае выявления нарушений требований настоящей Политики пользователем ИР (администратором ИР), которые повлекли или могли повлечь серьезный ущерб бизнес-деятельности Общества, руководство СП должно в обязательном порядке уведомлять о произошедшем СП ИБ и должно инициироваться, и вестись служебное расследование с привлечением заинтересованных СП и в соответствии с утверждённым Порядком расследования инцидентов ИБ.

67. Нарушение положений Политики, включая любое преднамеренное действие, предпринимаемое с целью нарушить, блокировать или иным способом обойти установленные средства контроля в области ИБ, может привести к мерам дисциплинарного взыскания в соответствии с трудовым законодательством, также административному или уголовному наказанию в соответствии с действующим законодательством.

68. Решение о применении и выборе мер ответственности принимается руководством Общества по результатам проведенного служебного расследования в зависимости от целесообразности применения рассматриваемых мер, а также от сведений об умышленности нарушения.