Приложение
к Приказу АО «Казахтелеком»
от «__» _____ 2023 года
№ _____

Политика управления доступом к информационным ресурсам АО "Казахтелеком"

Алматы, 2023

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.);
Реестр ИР – перечень информационных ресурсов, в электронном виде. Владельцем Реестра ИР является СП ИТ.
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.);
НРД – нормативно-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, техническое обслуживание и эксплуатацию ИР и ИС Общества;
Третья сторона, третье лицо – физическое или юридическое лицо, подрядчик, поставщик, партнер, контрагент, контрактник, и т.п., взаимодействующие с Обществом на основании договорных соглашений и не являющееся штатным работником Общества;

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 предоставления и управления доступом к ИР 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 предоставлении и управлении доступом к ИР 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 предоставлении и управлении доступом к ИР 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 предоставления и управления доступом к ИР 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 частных 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 частных 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 ИТ.

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

20. Информация о новом 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 ИТ в течение двух рабочих дней с момента появления в виде служебной записки или в иной официальной и принятой в Обществе форме, 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 НРД.

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. Предоставление доступа к ИР, должно производиться путем формирования и внедрения ролей для обеспечения соответствия прав (полномочий, привилегий) доступа пользователей и администраторов ИР их функциональным обязанностям. Совокупность таких ролей представляет собой матрицу доступа к ИР, которая формируется в электронной форме или на бумажном носителе. Для каждого ИР в Обществе должна быть разработана, внедрена и использоваться соответствующая матрица доступа, которая должна быть согласована со СП ИБ.

26. "Ролевое" управление должно являться основным механизмом управления правами (полномочий, привилегий) доступов пользователей и администраторов ИР в Обществе.

27. Роли должны формироваться с учетом принципа минимальности полномочий. Уровень полномочий субъекта доступа должен соответствовать принципу минимальной достаточности для решения поставленных перед субъектом доступа (пользователем) функциональных задач и/или должностных обязанностей.

28. Ни одна роль не должна позволять пользователю проводить единолично критичные операции (удаление данных, изменение привилегий и т.п.).

29. Критичные технологические процессы должны быть защищены от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления должны выполняться через специальные роли в ИР без непосредственного доступа к данным. В критичных системах по решению бизнес-владельца ИР может вводиться роль администратора ИБ ИР, в функции которого входит подтверждение прав и полномочий пользователей, заведенных в системе ее Администратором ИС.

30. Процесс управления (создание, внедрение, изменение, использование и т.п.) матрицами доступов и ролями должен осуществляться в соответствии с разработанными процедурами (правилами, инструкциями, и т.п.) и быть реализован в той или иной официальной и принятой в Обществе форме, например, посредством автоматизированной электронной системы и т.п. на основании требований положений настоящей Политики, законодательства Республики Казахстан в области ИБ, НРД регулятора (регулирующих и надзорных органов) и международных стандартов ИБ.

31. Должен быть определен перечень тех ИР, к которым предоставляются права доступа «по умолчанию» (т.е. минимальный набор ИР, необходимых для работы того или иного подразделения/работника), а также сами права доступа «по умолчанию». Такие права доступа должны быть минимальными.

32. Предоставление доступа работнику Общества не может осуществляться без одобрения и согласования его непосредственного руководителя, или в случае с

третьими лицами – ответственного лица Общества (подразделения - куратора), наличия подписанного договора о не разглашении сведений (NDA), согласования и контроля со стороны СП ИБ.

33. Предоставление доступа к ИР Общества не может быть полным и неограниченным по времени.

34. Пользователям запрещено использовать чужие полномочия по доступу к ИР и/или передавать кому-либо такие полномочия (передача своего пароля другому лицу);

35. Каждому пользователю ИР присваивается уникальный идентификатор (имя пользователя). Доступ ко всем ИР Общества должен осуществляться на основе аутентификации и авторизации пользователя.

36. В качестве методов аутентификации могут быть использованы пароли, многофакторный метод, физические носители кода, биометрические параметры и другие носители, методы.

37. Пароль для первоначального входа в систему или физический носитель должен быть представлен пользователю способом, исключающим возможность его компрометации.

38. Для смены пароля пользователя в процессе работы должны использоваться интерактивные процедуры, обеспечивающие достаточное количество паролей.

39. Пользователь обязан регулярно менять свой пароль доступа к ИР, а функциональность ИР должна позволять это делать.

40. Прямой доступ пользователей к базам данных не предоставляется.

41. Все действия с паролями должны выполняться в строгом соответствии с требованиями положений Политики парольной защиты.

42. Доступ к ИР не предоставляется (прекращается) в случае отсутствия производственной необходимости, изменения функциональных и должностных обязанностей, увольнения работника, расторжения контракта или нарушения договоров и/или соглашений.

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

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

45. Журналы аудита действий пользователей и администраторов ИР 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 предоставления доступа

46. 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.

47. Заявки на предоставление доступа к ИР должны соответствовать требованиям и формам реализации, разработанным и принятым в Обществе и содержать следующую минимальную информацию:

1) данные о лице (субъекте), которому предоставляется доступ (ФИО, должность, подразделение);

2) наименование ИР в соответствии с реестром, к которому запрашивается доступ;

3) перечень запрашиваемых ролей доступа (а в случае, если роли не определены - права доступа);

4) дату предоставления доступа и обоснование предоставления доступа;

5) срок действия, на который предоставляется доступ.

48. Для предоставления доступа пользователю к 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 необходим для выполнения пользователем обязанностей другого пользователя по поручению (в виде служебной записки) руководителя СП;

3) доступ необходим для выполнения пользователем обязанностей другого пользователя по указанию (в виде приказа или распоряжения) руководства Общества;

4) доступ необходим для выполнения пользователем работ по указанию (в виде приказа или распоряжения) руководства Общества;

5) доступ необходим для выполнения пользователем работ в ходе реализации контрактов, соглашений, договоров, заключенных Обществом (для представителей третьих сторон).

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

50. Лицо, которому предоставляется доступ (субъект доступа) должно быть ознакомлено с настоящей Политикой и другими частными политиками ИБ Общества, регламентирующими использование ИР.

51. 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 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 у пользователя 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) ответственное СП осуществляет предоставление доступа на установленный срок действия;

5) по истечению установленного срока действия предоставленного доступа к ИР осуществляется завершение предоставления доступа ответственным СП 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.

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

53. Доступ третьих лиц к ИР Общества должен предоставляться на период и в объеме, необходимом 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.

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

1) проверка результата деятельности третьих лиц;

2) осуществление деятельности третьих лиц только в присутствии ответственных работников Общества;

3) ведение аудиторского следа по действиям третьих лиц;

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

55. СП ИБ обязано проводить периодический мониторинг (аудит) соблюдения правил предоставления доступа.

5 Порядок изменения прав доступа

56. В случае необходимости предоставления пользователю дополнительных полномочий (ролей) по доступу к уже используемому им ИР следует действовать в соответствии с положениями настоящей Политики, регламентирующими порядок предоставления доступа к ИР.

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

6 Порядок отмены доступа

58. Отмена прав доступа к ИР и/или блокировка учетных записей происходит в случаях:

1) изменения функциональных и/или должностных обязанностей, штатного расписания, формы занятости работника;

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

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

4) нарушения пользователем правил доступа к ИР;

5) ухода работника в декретный отпуск (отпуск по уходу за ребенком);

6) длительного отсутствии, неактивности работника продолжительностью более 45 календарных дней;

7) смены должности, формы занятости или уволившихся из Общества;

8) отсутствия производственной необходимости;

9) завершения договорных соглашений с третьими лицами;

10) по иным требованиям руководства Общества.

59. При изменении функциональных и/или должностных обязанностей, штатного расписания, формы занятости и т.п. работника Общества отменяются все имеющиеся права доступа, и присваиваются новые права доступа, соответствующие его новым обязанностям и статусу в соответствии с требованиями положений Политики.

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

61. Обязанности по инициированию отмены доступа пользователя к ИР возлагаются:

1) в случае истечения периода действия предоставленного доступа, изменения функциональных и/или должностных обязанностей, штатного расписания, формы занятости и т.п. работника Общества или его увольнения, изменения технологических процессов обработки информации таким образом, что доступ работнику более не требуется - на непосредственного руководителя, соответствующего заинтересованного СП;

2) в случае выявления доступов с нарушениями сроков действия, нарушений пользователем правил доступа к ИР и/или иных требований настоящей Политики – СП ИТ либо СП ИБ в ходе проведения аудитов.

62. 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.

63. Фактическая реализация отмены доступа к ИР осуществляется уполномоченным СП ИТ, после получения согласования со стороны СП ИБ.

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

7 Контроль прав доступа

65. Со стороны СП ИБ на периодической основе должна производиться проверка (аудит) соответствия прав доступа к ИР матрице доступа, а также контроль отмены прав доступа уволенным работникам и блокирования доступа длительно отсутствующим работникам и т.п., в соответствии с требованиями положений Политики.

66. Для обеспечения эффективного контроля доступа необходимо вести официальный процесс регулярной проверки прав доступа пользователей, отвечающий следующим требованиям:

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

2) права доступа пользователей должны проверяться и переназначаться при изменении их должностных обязанностей в Обществе, а также при переходе с одной работы на другую в пределах Общества;

3) проверка прав пользователей, имеющих особые привилегии для доступа в систему, должна проводиться чаще (но не реже одного раза в 6 месяцев);

4) необходимо регулярно проверять адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав;

5) изменение привилегированных учетных записей должно протоколироваться.

67. Контроль над выполнением процедур управления доступом пользователей должен включать:

1) контроль над добавлением, удалением и изменением идентификаторов, данных аутентификации и иных объектов идентификации;

2) проверку подлинности пользователей перед сменой паролей;

3) немедленное блокирование прав доступа при увольнении;

4) блокирование учётных записей, неактивных более 45 дней;

5) включение учётных записей, используемых третьими лицами для удалённой поддержки (работы), только на время выполнения работ;

6) отслеживание удалённых учётных записей, используемых третьими лицами, во время работ;

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

8) 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;

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

10) блокирование учётной записи на период равный 30 минутам или до разблокировки учётной записи администратором;

11) блокирование учетных записей пользователей при выявлении по результатам мониторинга (просмотра, анализа, аудита) журналов регистрации событий безопасности действий пользователей, которые отнесены оператором (администратором) к событиям нарушения ИБ.

68. Контроль и периодический пересмотр прав доступа пользователей к ИР должен осуществляться в процессе аудита ИБ в соответствии с установленными процедурами Политики аудита ИБ.

8 Роли и ответственность

69. Контроль за выполнением требований и правил, а также ответственность за актуальность настоящей Политики (внесение в неё изменений) возлагается на структурное подразделение ИБ Общества.

70. 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.

71. 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.

72. 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 доступов к ИР.

73. Бизнес-владельцы ИР несут ответственность за согласование доступа к ИР.

74. Реализация положений настоящей Политики и процедур, связанных с операционным (эксплуатационным) сопровождением процессов управления доступом к 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.

75. Структурными подразделениями HR Общества должна осуществляться деятельность по обязательному и своевременному предоставлению информации о происходящих изменениях в штатном расписании в отношении уволенных и/или временно не работающих, длительно отсутствующих работниках Общества в структурное подразделение ИБ Общества для обеспечения исполнения требований положений настоящей политики в части контроля и аудита доступов к ИР Общества. Информация должна предоставляться в официальной и принятой в Обществе форме, например, посредством автоматизированной электронной системы и т.п. Предоставление информации необходимо выполнять:

1) на регулярной основе, по факту возникновения вышеуказанных изменений, подтвержденных согласованными распорядительными документами (приказы, распоряжения и т.п.);

2) на ежемесячной основе в виде предоставления сводного отчета с информацией о всех вышеуказанных изменениях за отчетный период.

76. 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.

77. В случае выявления нарушений требований настоящей Политики пользователем ИС (администратором ИС), 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.

78. Нарушение положений Политики или разработанных в поддержку настоящей политики документов, включая любое преднамеренное действие, предпринимаемое с целью нарушить, блокировать или иным способом обойти установленные средства контроля в области ИБ, может привести к административному или уголовному

наказанию в соответствии с действующим законодательством, а также НРД по управлению персоналом Общества.

79. 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.