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

Политика обеспечения безопасности удаленного доступа к ресурсам сетей и информационных систем АО "Казахтелеком"

Алматы, 2023

Оглавление

1 Термины, сокращения и определения

ИС ЕСК – информационная система «Единая служба каталогов». Централизованный программно-аппаратный комплекс Общества, созданный на базе программного обеспечения Microsoft Active Directory;
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. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
Локальный доступ или подключение – процесс получения доступа к сетям и ИС Общества локально, в местах и на объектах, принадлежащих и находящихся под контролем Общества (здания, офисы, филиалы, представительства, иные обособленные СП, включая расположенные в другой местности);
НРД – нормативно-регламентирующая документация Общества (политики, стандарты, приказы, регламенты, руководства, инструкции и т.п.);
Общество – Акционерное Общество «Казахтелеком»;
ПО – программное обеспечение;
Политика – утвержденная в Обществе настоящая Политика обеспечения безопасности удаленного доступа к ресурсам сетей и информационных систем 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;
СВТ – средства вычислительной техники (стационарные компьютеры или рабочие станции, переносные компьютеры или ноутбуки и т.п.);
СП – структурное подразделение 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;
Удаленный доступ – процесс получения доступа к сетям и ИС Общества из других (сторонних) сетей, в том числе из сети Интернет, не являющихся постоянно

соединенными физически или логически с сетями Общества и не находящихся под контролем Общества.

2 Назначение Политики и область ее действия

1. Настоящая Политика определяет свод правил, требований и допустимых способов для процедур предоставления, использования, контроля и обеспечения ИБ удаленного доступа из сторонних (внешних) сетей к ресурсам сетей и ИС Общества.

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

3. Правила и требования Политики призваны минимизировать потенциальную опасность (риски) Общества от ущерба, который может быть нанесен в результате несанкционированного использования ресурсов Общества.

4. Политикой удаленного доступа охватываются все ресурсы сетей и ИС Общества, которые используются при удаленном доступе. В состав ресурсов сетей и ИС Общества включаются данные, информация, ПО, аппаратные средства, средства обслуживания и телекоммуникации. Политика применима ко всем лицам, использующим в своей деятельности удаленный доступ к ресурсам сетей и ИС Общества, включая всех работников и представителей третьих сторон, использующих эти ресурсы.

5. Политика распространяется на все виды технических реализаций удаленного доступа с применением любых видов и типов СВТ, используемых для подключения к ресурсам сетей и ИС Общества.

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

3 Общие положения и требования политики

7. 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.

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

9. 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 аудитов);

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.

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

11. Удаленный доступ – это привилегия, которая должна подлежать дополнительному контролю, отражающему дополнительные риски, которые она представляет для ресурсов сетей и ИС Общества, к которым предоставляется доступ.

12. Принципы удаленного доступа, изложенные в положениях настоящей Политики, должны распространяться на все виды и формы подключений, в том числе посредством технологий xDSL, xPON и т.п., к сетям и ресурсам Общества из мест и объектов, не принадлежащих и не находящихся под физическим контролем Общества: здания, гостиницы, сторонние офисы, филиалы (размещенные физически обособленно, не в помещениях Общества), домашние офисы, представительства, иные обособленные СП, включая расположенные в другой местности и т.п.;

13. Удаленный доступ имеет такое же значение и статус, как и локальный доступ к ресурсам сетей и ИС Общества, к нему применяются те же требования действующих НРД, что и к локальному доступу.

14. Предоставление удаленного доступа к ИР и ИС Общества не может быть полным (по правам, уровню доступа к ИР/ИС и т.д.) и неограниченным по времени.

15. По умолчанию, удаленный доступ отключен для любого пользователя в Обществе.

16. Удаленный доступ должен предоставляться пользователям только в случае объективной необходимости.

17. Предоставление удаленного доступа работнику Общества не может осуществляться без одобрения и согласования его непосредственного руководителя (замещающего лица).

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

19. Процесс получения, изменения или отмены удаленного доступа для пользователя должен быть официальным и организован в соответствии с настоящим документом, в соответствии с процедурой управления удаленным доступом (методикой, инструкцией, правилами и т.п.), которая должна быть разработана на основе положений настоящей Политики, других НРД и Политик ИБ Общества, законодательства Республики Казахстан в области ИБ, НРД регулятора (регулирующих и надзорных органов) и международных стандартов ИБ.

20. Процедура управления удаленным доступом для работников Общества (методика, инструкция, правила и т.п.) должна обеспечивать регистрацию следующих сведений:

1) данные о лице, которому предоставляется доступ (ФИО, должность, подразделение и т.п.);
2) цель предоставления удаленного доступа;
3) перечень с наименованиями ИС или ИР, к которым организуется удаленный доступ;
4) дата предоставления доступа и обоснование предоставления доступа.

21. Пользователи удаленного доступа должны быть зарегистрированы в ИС ЕСК и иметь в ней действующие персональные учетные данные (записи) – логин и пароль. Возможно использовать и другие методы аутентификации, такие как, многофакторные методы, аппаратные ключи, сертификаты и др.

22. Управление ролями учетных записей в рамках предоставления пользователям удаленного доступа должно основываться на доступном функционале ИС ЕСК, в которой на основании соответствующих разработанных процедур (методик, инструкций, правил и т.п.), также должно выполняться распределение учетных данных пользователей по определенным группам, к которым в дальнейшем должны применяться политики управления привилегиями и безопасностью в системах технического обеспечения удаленного доступа (шлюзы безопасности).

23. Все действия, производимые в ИС ЕСК в рамках управления удаленным доступом (предоставление, изменение, отмена и т.п.), должны согласовываться с СП ИБ.

24. Применение локальных учетных данных пользователей в системах технического обеспечения удаленного доступа не допустимо. Исключения могут составлять только отдельные не стандартные случаи, случаи отсутствия технической реализации/возможности и/или случаи с подключениями типа «сеть-сеть».

25. Для исключительных случаев может устанавливаться иной, но не противоречащий требованиям и правилам Политики, порядок организации удаленного доступа, официально согласованный и контролируемый СП ИБ.

26. Срок действия удаленного доступа для работников Общества должен определяться периодом времени, необходимым и достаточным для выполнения работником задач в соответствии со своими функциональными и должностными обязанностями.

27. Срок действия удаленного доступа для представителей третьих сторон должен определяться условиями договорных соглашений, но не должен быть более одного календарного года с момента предоставления удаленного доступа в рамках действующих договорных соглашений. В случае длительных договорных обязательств, более одного календарного года, необходимо обеспечить заблаговременное выполнение официальной процедуры по продлению удаленного доступа на новый установленный отчетный период согласно требованиям Политики.

28. Срок действия удаленного доступа должен на регулярной основе, с момента его предоставления, проверяться и контролироваться на предмет актуальности и/или истечения срока действия самим пользователем, его непосредственным руководителем или иным лицом, ответственным за подобный процесс, соответствующего заинтересованного СП. В случае с представителями третьих сторон, обязательства за выполнение указанных требований возлагаются на курирующее и ответственное лицо от заинтересованного СП в рамках действующих договорных соглашений.

29. Для продления срока действия удаленного доступа пользователю и/или руководителю заинтересованного СП необходимо обеспечить заблаговременное, не менее чем за 10 рабочих дней до истечения срока действия доступа, инициирование официального процесса в соответствии с процедурой управления удаленным доступом (методикой, инструкцией, правилами и т.д.) на продление удаленного доступа.

30. В случае отсутствия со стороны пользователя и/или руководителя, заинтересованного СП инициации процесса на продление удаленного доступа, в целях соблюдения должного уровня ИБ, удаленный доступ блокируется автоматически, без каких-либо предварительных уведомлений.

31. В случае отсутствия необходимости дальнейшего использования пользователем удаленного доступа руководитель такого СП должен уведомить СП ИТ и СП ИБ соответствующей служебной запиской в течении 2-х рабочих дней.

32. Процедура удаленного доступа прекращается на основании уведомления СП ИБ подразделением ЕХ (при переводе, увольнении, длительный отпуск и т.д.).

33. Пользователям запрещено использовать удаленный доступ для доступа в сеть Интернет через сети Общества в развлекательных, коммерческих, личных или иных интересах, не являющихся интересами Общества.

34. Выполнение любых незаконных действий через сети Общества любым пользователем удаленного доступа строго запрещено. Пользователь несет полную ответственность за последствия неправомерного (незаконного) использования предоставленного ему удаленного доступа.

35. Запрещается использование удаленного доступа без официального прохождения процедуры (методики, инструкции и т.п.) получения удаленного доступа.

36. Удаленный доступ к ресурсам сетей и ИС Общества должен организовываться только через защищенные сетевые соединения с использованием принятых к использованию в Обществе технологий VPN, на базе корпоративных технических средств и систем ИБ Общества и при соблюдении следующих базовых требований:

1) наличие уникального идентификатора у каждого пользователя;
2) использование надежных парольных фраз и/или инфраструктуры открытых ключей с устойчивыми к взлому ключевыми фразами;
3) идентификация и аутентификация пользователей с использованием соответствующих защищенных протоколов;
4) шифрование среды передачи данных стойкими алгоритмами;
5) ведение записей (логирование) удачных и неудачных попыток авторизации в процессе подключения;
6) использование защищенных протоколов передачи данных, таких как IPsec и SSL;
7) применение ограничения времени действия сессии удаленного доступа типа «узел-сеть» в пределах 12 - 24 часов с момента ее установления. По истечению установленного времени должен выполняться автоматический разрыв и/или ре-инициализация соединения удаленного доступа. Для удаленного доступа типа «сеть-сеть» временные критерии должны выставляться в соответствии с индивидуальными требованиями при согласовании параметров соединения между участниками процесса;
8) доступ из беспроводных сетей пользователей, не прошедших идентификацию и аутентификацию, должен предоставляться только в гостевые сегменты и/или сеть Интернет.

37. В целях обеспечения должного уровня безопасности удаленного доступа и минимизации рисков ИБ, пользователям запрещено использование, отличного от разрешенного к использованию в Обществе ПО, стороннего ПО и/или облачных

сервисов (GoToMyPC, LogMeIn, Teamviewer и т.п.), для организации удаленного доступа.

38. Пользователи, использующие удаленное подключение типа «узел-сеть», должны быть уверены и гарантировать, что их СВТ не подключено одновременно к какой-либо другой сети, не являющейся сетью Общества. В случае соединений удаленного доступа типа «сеть-сеть», в целях дополнения, но не исключения, положений настоящей Политики могут применяться правила и требования, определяемые положениями договоров и/или соглашений, которые должны регламентировать различные технологические параметры и аспекты соединения, например, применяемый перечень СВТ, возможности и рамки использования сетевой инфраструктуры взаимодействующих сторон, типы шифрования и т.п.

39. При доступе к ресурсам сетей и ИС Общества, пользователи несут полную ответственность за предотвращение доступа к любой информации и данным Общества со стороны лиц (в том числе членов семьи, родственников, знакомых и т.д.), не имеющих соответствующих правовых разрешений и привилегий от Общества. Данное правило должно соблюдаться, пока активно соединение удаленного доступа к сетям Общества.

40. Пользователям запрещены разглашение и передача своих учетных данных (логин и пароль) в каком-либо виде (устно, письменно, по электронной почте и т.п.) и кому-либо, в том числе и членам семьи.

41. Личные СВТ, которые используются для удаленного доступа, должны соответствовать тем же требованиям НРД, которые предъявляются к СВТ, принадлежащим Обществу.

42. На всех используемых для удаленного доступа СВТ, должны быть установлены новейшие версии лицензионного и утвержденного в Обществе ПО (VPN, антивирус, локальные брандмауэры и операционные системы и т.п.). Если СВТ содержит нелицензионное ПО и/или устаревшие версии ПО, операционных систем, которые не соответствуют требованиям корпоративных стандартов Общества, необходимо в обязательном порядке устранить данные несоответствия до начала использования удаленного доступа.

43. Использование пользователем удаленного доступа каких-либо не регламентированных и/или ограниченных информационных ресурсов, должно быть заранее официально ободрено непосредственным руководителем заинтересованного СП и согласовано СП ИБ.

44. Любое ПО, система или средство пользователя, которые могут мешать или работать в обход технических средств и систем Общества по обеспечению маршрутизации и безопасности удаленного доступа, должны быть отключены на время работы сессии удаленного доступа.

45. При использовании удаленного доступа категорически запрещается копирование, тиражирование, хранение и распространение данных, содержащих коммерческую, конфиденциальную и иные тайны Общества, в том числе персональные данные работников Общества.

4 Роли и ответственность

46. Контроль за выполнением требований и правил Политики возлагается на СП ИБ.

47. Ответственность за контроль исполнения и актуальность настоящей Политики, а также внесение в нее изменений возлагается на СП ИБ.

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

49. Руководители СП 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.

50. СП ИБ 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 удаленного доступа.

51. Реализация положений настоящей Политики и процедур, связанных с операционным (эксплуатационным) сопровождением процессов удаленного доступа и поддержкой пользователей удаленного доступа, возлагается на СП, которые обеспечивают техническую поддержку и сопровождение операционной деятельности пользователей и технических систем и средств Общества, обеспечивающих удаленный доступ.

52. В случае выявления нарушений требований настоящей Политики пользователем ИС, которые повлекли или могли повлечь серьезный ущерб бизнес-деятельности Общества, должно инициироваться и вестись служебное расследование с привлечением заинтересованных СП и в соответствии с утверждённым Порядком расследования инцидентов ИБ.

53. 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.

54. 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 и причиненного ущерба.