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

Политика антивирусной защиты информационных систем АО "Казахтелеком"

Алматы, 2023

Оглавление

1 Термины, сокращения и определения

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.);
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 антивирусной защиты информационных систем АО "Казахтелеком";
Пользователь – работник Общества или представитель третьей стороны, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации;
САЗ – средства антивирусной защиты;
СВТ – средства вычислительной техники (стационарные компьютеры или рабочие станции, переносные компьютеры или ноутбуки и т.п.);
СП – структурное подразделение Общества;
СП ТП – структурное подразделение Общества либо третья сторона, осуществляющая техническую поддержку пользователей и СВТ в Обществе;
ТП – техническая поддержка;
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;
HTTP, HTTPS – Hyper Text Transfer Protocol, Hyper Text Transfer Protocol Secure – протокол передачи гипертекста;
FTP – File Transfer Protocol – протокол передачи файлов;
IMAP – Internet Message Access Protocol – протокол для доступа к электронной почте;
OSI – The Open Systems Interconnection model. Сетевая модель OSI;
POP3 – Post Office Protocol Version 3 – протокол используемый для получения почты с почтового сервера клиентом;
SMTP – Simple Mail Transfer Protocol – протокол используемы для передачи электронной почты между серверами;

TCP/IP – Transmission Control Protocol/Internet Protocol – сетевая модель передачи данных описывающая способ передачи данных от источника к получателю.

2 Назначение Политики и область ее действия

1. Настоящая Политика определяет систему мер, направленных на защиту ИС Общества и СВТ пользователей, включая рабочие станции, ноутбуки, серверы и т.п., от угроз ИБ, разрушающего воздействия компьютерных вирусов и другого вредоносного ПО («троянских» программ, логических бомб и т.п.), а также устанавливает единые требования к организации системы антивирусной защиты ИС и всех типов СВТ, требования к конфигурации применяемых программных средств и процедуры их эксплуатации.

2. Негативные последствия могут включать в себя вероятность заражения вирусами отдельных узлов сети и/или возникновения вирусных эпидемий, раскрытие или утрату чувствительной и конфиденциальной информации, кражу интеллектуальной собственности, репутационные последствия, а также влияние на важные внутренние системы и бизнес-процессы Общества.

3. Действие настоящей Политики распространяется на всех работников Общества и других лиц, которым предоставлен доступ к ИС Общества.

4. Настоящая Политика применяется ко всем ресурсам ИС Общества (серверное оборудование, СВТ, иные технологические сервисы и системы), подключенным к сетям Общества.

5. Политика устанавливает ответственность всех работников Общества и иных лиц, подключающихся к сетям Общества, использующих, эксплуатирующих и сопровождающих ИС Общества.

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

7. В случаях, когда на СВТ, серверное оборудование (и др.) невозможно установить САЗ - использование данного СВТ, серверного оборудования (и др.) возможно только по согласованию с СП ИБ.

3 Общие положения и требования политики

8. 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.

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

10. 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.

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

12. Антивирусная защита достигается путем:

1) эксплуатации САЗ;

2) поддержания в актуальном состоянии баз вирусных сигнатур (антивирусных баз) САЗ на серверах, рабочих станциях, СВТ и прочих технологических сервисах и системах;

3) регулярного обновления ПО САЗ на серверах, рабочих станциях, СВТ и прочих технологических сервисах и системах.

13. Методы борьбы с вредоносным ПО должны включать в себя три составные части:

1) предотвращение – действия, позволяющие предотвратить заражение вредоносным ПО;

2) обнаружение – методология определения наличия вредоносного ПО;

3) удаление – физическое удаление кодов вредоносного ПО из зараженных файлов или зараженной системы.

14. САЗ устанавливаются на сервера, СВТ (рабочие станции) и прочие технологические сервисы и системы либо функционируют в составе комплексных систем защиты (шлюзы безопасности и т.п.) и обеспечивают:

1) периодическую проверку всей информации, хранимой на любых жестких дисках, системах хранения данных технических средств;

2) проверку в режиме «реального времени» запускаемых программ, открываемых файлов, процессов и т.п.;

3) выполнение проверки и контроля сетевого трафика в режиме «реального времени».

15. Порядок использования САЗ определяется положениями Политики, эксплуатационной документацией конкретного САЗ, инструкциями по антивирусной защите и другими НРД.

16. Установка разрешенных в Обществе САЗ на СВТ пользователей осуществляется только уполномоченными работниками (администраторами, техническими специалистами и т.п.) соответствующего СП ТП.

17. Порядок приобретения и установки САЗ:

1) к использованию в ИС Общества допускаются только лицензионные САЗ. Приобретение САЗ и проверка их функциональных возможностей должны осуществляться в соответствии с Политикой безопасности при разработке,

эксплуатации и приобретении программно-аппаратных средств и разрабатываемыми техническими требованиями;

2) установка и настройка САЗ на серверах, рабочих станциях, СВТ и прочих технологических сервисах и системах должна осуществляться только уполномоченными работниками (администраторами, техническими специалистами и т.п.) соответствующих СП Общества, ответственных за техническое обслуживание (эксплуатацию, поддержку, обслуживание и т.п.) САЗ, СВТ, ИС Общества в соответствии с руководствами (инструкциями) по установке приобретенных САЗ.

18. Все САЗ должны соответствовать требованиям настоящей Политики и предоставлять следующие возможности:

1) осуществление сканирования серверного оборудования, СВТ и прочих технологических сервисов и систем по заранее созданному расписанию;

2) проверка сетевого трафика на наличие вирусов и иного вредоносного ПО (на разных уровнях OSI и на уровне различных протоколов HTTP(S), SMTP, FTP, POP3, IMAP и т.п.);

3) определение типов сетевого трафика, подлежащих проверке;

4) мониторинг в режиме «реального времени» всех запускаемых программ и открываемых файлов на предмет наличия вирусов и иного вредоносного ПО;

5) обнаружение вирусов, «троянских коней» и иного вредоносного ПО;

6) блокирование, удаление вредоносного ПО, лечение зараженных файлов;

7) регистрация и сигнализация попыток вирусного заражения ИС Общества, внедрения вредоносного ПО и т.п.;

8) автоматическая и управляемая администратором системы антивирусной защиты загрузка обновлений антивирусных баз с локальных серверов обновления антивирусного ПО, либо с серверов обновлений антивирусного ПО в сети Интернет.

19. Применяемые для серверов и СВТ САЗ должны основываться на клиент-серверной технологии. Серверная часть должна предоставлять возможность централизованного управления клиентскими частями САЗ, а именно:

1) централизованного задания политик антивирусной защиты (запуска антивирусных средств, сканирования и т.д.);

2) централизованного обновления вирусных сигнатур (антивирусных баз).

20. САЗ, являющиеся составной частью комплексных систем защиты (шлюзы безопасности и т.п.), должны работать и управляться в рамках структуры соответствующей системы защиты при соблюдении требований положений настоящей Политики.

21. Загрузка ПО и рабочих файлов на СВТ, сервера и прочие носители информации должна осуществляться с проведением предварительной их проверки САЗ.

22. Всем пользователям ИС Общества (в том числе, администраторам и т.п.) запрещается самостоятельная установка и использование специализированного ПО, не утвержденного официально (не разрешенного) к использованию в Обществе ПО, без предварительного согласования с СП ИБ Общества.

23. Порядок применения САЗ на СВТ:

1) САЗ должны быть установлены на всех СВТ, взаимодействующих с ресурсами сетей и ИС Общества. Допускается не применять САЗ на СВТ, не имеющих сетевые подключения к ресурсам сетей и ИС Общества, технологические процессы обработки информации и т.п.;

2) всем пользователям ИС Общества (в том числе, администраторам, техническим специалистам и т.п.) запрещается создавать, загружать на СВТ и распространять в ИС Общества любые данные, заведомо содержащие вирусы, вредоносный программный код и т.п.;

3) антивирусный контроль всех дисков и файлов стационарных СВТ должен проводиться в автоматическом режиме при загрузке (запуске) СВТ в начале каждого рабочего дня либо в период неактивности пользователя (наименьшего использования СВТ);

4) антивирусный контроль всех дисков и файлов мобильных (носимых) СВТ должен проводиться в автоматическом режиме при каждой загрузке (запуске) СВТ;

5) если проверка всех файлов на дисках СВТ занимает неприемлемо большое время, допускается проводить выборочную проверку только загрузочных областей дисков, оперативной памяти и файлов операционной системы, запущенных процессов. В этом случае полная проверка должна осуществляться в период неактивности пользователя (наименьшего использования СВТ);

6) запуск САЗ, установленных на СВТ, должен осуществляться автоматически по заданию (расписанию), централизованно созданному администратором системы антивирусной защиты Общества с использованием планировщика задач (входящего в поставку операционной системы либо антивирусного ПО);

7) должна осуществляться полная антивирусная проверка всех дисков мобильных компьютеров непосредственно перед их подключением к сетям и ресурсам ИС Общества;

8) обязательному антивирусному контролю подлежат все файлы, полученные из внешних источников (в частности, по электронной почте) или загруженные со съемных носителей (флэш-накопителей, с магнитных дисков, лент, CD-ROM и т.п.). Контроль информации должен проводиться непосредственно после ее загрузки, до момента ее использования (запуска), установленными на СВТ пользователя САЗ;

9) файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль;

10) Устанавливаемое (изменяемое) на серверах ПО должно быть предварительно проверено уполномоченным работником (администратором, техническим специалистом и т.п.) СП ТП на отсутствие вредоносного ПО.

24. Контроль над соблюдением порядка применения САЗ осуществляется администратором САЗ.

25. САЗ применяются на следующих компонентах ИС Общества:

1) на файловых серверах;

2) на серверах приложений, баз данных;

3) на почтовых серверах;

4) на web-серверах;

5) в точках подключения к сетям общего доступа (на интернет-шлюзах, межсетевых экранах) и беспроводным сетям.

26. Применение САЗ на серверах ИС Общества, используемых в качестве файловых серверов, серверов приложений, web-серверов и т.п., должно обеспечивать:

1) антивирусную проверку и лечение файлов в режиме «реального времени», т.е. в момент попытки записи или считывания файла, выполнения операций ввода-вывода на сервере;

2) проверку всех каталогов и файлов по расписанию не реже одного раза в сутки (с учетом нагрузки на сервер).

27. Применение САЗ на серверах ИС Общества, используемых в качестве почтовых серверов, должно обеспечивать проверку всех электронных почтовых сообщений, поступающих на данные сервера.

28. В случае, если проверка сообщения, полученного из внешних по отношению к ИС Общества сетей, на почтовом сервере показала наличие в нем вируса или иного вредоносного ПО, передача данного сообщения адресату (пользователю ИС) должна блокироваться.

29. В случае, если проверка сообщения, полученного от пользователя ИС, на почтовом сервере показала наличие в нем вируса или иного вредоносного ПО, передача данного сообщения адресату (другому пользователю ИС или внешнему лицу) должна блокироваться. При этом должно осуществляться автоматическое оповещение о выявлении вирусов ответственных администраторов ИС и СП ИБ.

30. САЗ, применяемые в точках подключения к сетям общего доступа или беспроводным сетям, должны обеспечивать проверку на наличие вирусов и иного вредоносного ПО, сетевого трафика, входящего и исходящего по отношению к сетям и ресурсам ИС Общества.

31. Процедура архивирования данных (систему хранения/бэкапирования на магнитную ленту или иной носитель, систему) должна включать в себя процедуру предварительного антивирусного контроля.

32. Любое устанавливаемое (изменяемое) ПО на СВТ должно быть взято из утвержденного реестра доверенного ПО Общества с официального репозитория сайта разработчика. При этом, на СВТ (сервере) уже должна быть установлена обновленная (актуальная) версия САЗ. После чего, ответственным администратором ИС (системным администратором, администратором приложений и т.п.) производится установка данного ПО.

33. Системные администраторы серверов и администраторы ресурсов ИС Общества должны постоянно поддерживать максимально возможный уровень информационной безопасности вверенных им программно-технических средств. Для этого необходимо:

1) отслеживать информацию, поступающую от разработчиков системного и ПО об обнаруженных ошибках и уязвимостях;

2) своевременно устанавливать обновления и исправления, официально рекомендуемые разработчиками системного и прикладного ПО;

3) отключить все неиспользуемые сервисы и приложения операционной системы (или прикладного ПО);

4) поддерживать в актуальном состоянии установленные САЗ;

5) вести журналы системных событий и регулярно анализировать их;

6) следовать рекомендациям СП ИБ.

34. Действия при обнаружении вредоносного ПО на серверах ИС:

1) в случае обнаружения зараженных вирусом, вредоносным кодом или иным вредоносным программным обеспечением файлов, процессов, приложений и т.п. на серверах, системные администраторы серверов и/или администраторы ресурсов ИС Общества (при необходимости совместно с уполномоченными работниками СП ТП) должны:

- при необходимости и в целях снижения риска сетевого распространения вирусов, отключить сервер от сетей Общества на период до полного уничтожения вирусов или иного вредоносного ПО и восстановления работоспособности соответствующего серверного оборудования;

- провести лечение и/или уничтожение зараженных файлов, вредоносного кода, процессов и т.п.;

- сообщить о факте обнаружения вредоносного ПО непосредственному руководству СП (подразделения, организации) и в СП ИБ с указанием даты и времени предполагаемого заражения, предположительного источника (отправителя, владелец и т. д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса, проведенных мероприятий по нейтрализации вируса и т.п.

35. Запрещено использование в процессе нормальной (штатной) работы и эксплуатации ИС Общества программных кодов, ПО или алгоритмов, приводящих к разрушению, уничтожению ИР.

36. Пользователям запрещается отключать установленные на СВТ САЗ и/или производить изменения их конфигураций, которые могут понизить установленный уровень защиты и т.п.

37. Обновление вирусных сигнатур (антивирусных баз) САЗ на серверах, рабочих станциях, СВТ и прочих технологических сервисах и системах должно осуществляться локально, с определенных серверов системы антивирусной защиты Общества, исключениями могут быть только случаи, когда отсутствует техническая возможность выполнения данных требований и такие случаи согласованы с СП ИБ.

38. Обновление вирусных сигнатур (антивирусных баз) системы антивирусной защиты Общества должно осуществляться из источников, определенных компанией-производителем (вендором) САЗ.

4 Роли и ответственность

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

40. Ответственность за актуальность Политики, а также внесение в нее изменений возлагается на СП ИБ.

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

42. 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.

43. Реализация положений настоящей Политики, связанных с сопровождением антивирусного ПО, обновлением антивирусных баз на серверах (в том числе на серверах системы антивирусной защиты), возлагается на уполномоченных и ответственных администраторов ИС САЗ.

44. Реализация положений настоящей Политики, связанных с сопровождением антивирусного ПО, обновлением антивирусных баз на СВТ Общества, возлагается на

пользователей и уполномоченных работников второй линии поддержки (сотрудников технической поддержки пользователей) СП ТП.

45. Реализация положений настоящей Политики, связанных с реагированием на сообщения пользователей о выявлении вирусов или иного вредоносного ПО, возлагается на уполномоченных работников первой линии поддержки (Help Desk) СП ТП и в случае необходимости, на уполномоченных работников второй линии поддержки (сотрудников технической поддержки пользователей) СП ТП.

46. Организационное и методическое обеспечение процесса антивирусной защиты возлагается на СП ИБ.

47. Периодический контроль соблюдения пользователями ИС Общества требований настоящей Политики возлагается на СП ИБ в рамках проведения аудитов ИБ.

48. Третьи лица, взаимодействующие и использующие ресурсы сетей и ИС Общества в рамках исполнения своих обязательств на основании действующих соглашений и договоров, несут ответственность за применение, использование или распространение вредоносного ПО в отношении ресурсов сетей и ИС Общества в соответствии с действующим законодательством Республики Казахстан.

49. В случае выявления нарушений требований настоящей Политики пользователем ИС, включая любое преднамеренное действие, предпринимаемое с целью нарушить, блокировать или иным способом обойти установленные средства контроля в области ИБ, которые повлекли или могли повлечь серьезный ущерб бизнес-деятельности Общества, должно инициироваться и вестись служебное расследование со стороны СП ИБ.

50. Несоблюдение мер, предусмотренных настоящей Политикой, влечет за собой ответственность в соответствии с действующим законодательством РК и внутренними документами Общества.