Приложение 9
к Положению об
информационной безопасности

Правила работы с корпоративной электронной почтой

1. Общие положения

1. Настоящие Правила работы с корпоративной электронной почтовой системой Университета (далее - Правила) регламентируют порядок работы с почтовой системой в Евразийском национальном университете им. Л.Н. Гумилева (далее – Университет).

2. Термины и определения

2. Университет - Некоммерческое акционерное общество «Евразийский Национальный Университет»;

3. КЭПС - Корпоративная электронная почтовая система Университета для внутренней и внешней переписки сотрудников;

4. Отдел информационной безопасности - Подразделение Университета, осуществляющее контроль информационной безопасности в области информационных систем и технологий;

5. HelpDesk – Отдела технического обслуживания Университета, обеспечивающая сервис в части технической поддержки пользователей; (автоматизированная служба единого окна для приема, регистрации и обработки обращений пользователей о сбоях в аппаратном и программном обеспечении, инфраструктуре информационной вычислительной сети Университета, а также заявок на обеспечение техникой и предоставление ИТ-сервисов.);

6. Администратор КЭПС - Представитель HelpDesk, обеспечивающий настройку и поддержку компонентов КЭПС;

7. Модератор - Ответственный работник Университета, который несет ответственность за своевременную публикацию либо отклоняет сообщения, направленные пользователями на массовые группы рассылок;

8. Пользователь - Обучающиеся, профессорско – преподавательский состав и иные категории работников Университета, которым предоставлено право пользования КЭПС;

9. ПО – Программное обеспечение;

10. ПК – Персональный компьютер.

3. Нормативные ссылки

11. При разработке Правил использовались нормативные документы:

1) Закон Республики Казахстан от 24.11.2015 года № 418-V «Об информатизации» (с изменениями и дополнениями по состоянию на 02.01.2021 г.);

2) СТ РК ИСО/МЭК 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью»;

3) СТ РК ISO/IEC 27002-2015 «Методы и средства обеспечения безопасности. Свод правил по средствам управления информационной безопасности»;

4) СТ РК ИСО/МЭК 17799-2006 (ISO/IEC 17799-2005, IDT) «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защитой информации»;

5) Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;

6) СТ РК 34.005-2002 «Информационная технология. Основные термины и определения»;

7) СТ РК 34.007-2002 «Информационная технология. Телекоммуникационные сети».

12. Правила являются внутренним нормативным документом Университета и соответствуют Политике информационной безопасности Университета.

13. Вся информация и сообщения, которые были созданы, отправлены, приняты или сохранены посредством КЭПС, принадлежат Университету, за исключением случаев, предусмотренных законодательством Республики Казахстан.

4. Описание КЭПС

14. Для обеспечения функционирования электронной почты допускается применение коммерческого лицензионного ПО, указанного в Паспорте ПК.

15. Доступ к сервису почты без настройки возможен с помощью веб-интерфейса, для чего необходимо указать в браузере адрес https://outlook.office365.com/.

16. Объем электронного сообщения и размер почтового ящика ограничен. Объем почтового ящика, выделяемого для каждого пользователя, составляет 25 Gb. Размер почтового сообщения ограничен до 20 Mb.

17. В качестве названия корпоративного почтового ящика берется фамилия, имя и отчество пользователя, написанные латинскими буквами и стандартного значка @, доменного имени enu.kz. (например: Иван Александрович Петренко petrenko.ia@enu.kz).

18. Допускается применение почтовых ящиков подразделений с использованием аббревиатуры наименования подразделения. (например: Служба информационной безопасности it-security@enu.kz).

5. Требования при работе пользователей с КЭПС

19. КЭПС Университета может быть использована только в служебных целях. Использование КЭПС в других целях категорически запрещено.

20. Использование ресурсов КЭПС предназначено для:

1) выполнения пользователями своих служебных обязанностей;

2) предоставления пользователями учебных и информационных сведений, материалов;

3) получения и распространения информации, связанной с деятельностью Университета;

4) осуществления информационно-аналитической работы;

5) обмена почтовыми сообщениями с внешними организациями, должностными и физическими лицами в служебных, учебных целях.

21. При использовании КЭПС пользователь обязан выполнять следующие требования информационной безопасности и электронного этикета:

1) оказывать получателю электронного сообщения то же уважение, что и при устном общении;

2) не рассылать письма, содержащие файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования;

3) при получении электронного сообщения, содержащие подозрительные прикрепленные файлы, распаковывать и запускать исполняемые модули только если отправитель не вызывает подозрений и функциональность модуля предварительно известна;

4) не участвовать в рассылке сообщений, пересылаемых по цепочке (спам, реклама и другое);

5) не пересылать по собственной инициативе по произвольным адресам незатребованную информацию, если это не входит в его служебные обязанности;

6) не использовать для массовой рассылки широковещательные возможности КЭПС за исключением выпуска объявлений;

7) при массовой рассылке пользователи должны использовать в качестве адресатов только заинтересованную аудиторию;

8) проверять правописание, грамматику, адрес получателя и перечитывать свое сообщение перед отправлением;

9) для уменьшения размера электронных сообщений и объединения нескольких вложенных файлов в один рекомендуется использовать программы для сжатия (компрессии) вложенных документов (WinRar);

10) ставить подпись в электронном письме после текстового сообщения с указанием следующих данных: имя, фамилия; должность, название организации, наименование структурного подразделения; номер телефона; при необходимости мобильный номер телефона, а также предупреждение о соблюдении тайны переписки и конфиденциальности*. В почтовом клиенте

---

* **Пример:**
С уважением, Имя Фамилия
Название должности
НАО «Евразийский Национальный Университет»
Адрес: г. Астана, ул. Сатпаева, 2,
www.enu.kz
сл.:+7 7172….
моб.:+7 …….
ПРЕДУПРЕЖДЕНИЕ О СОБЛЮДЕНИИ ТАЙНЫ ПЕРЕПИСКИ И КОНФИДЕНЦИАЛЬНОСТИ
Настоящее сообщение и все переданные с ним приложения предназначены исключительно для адресата и могут содержать сведения, охраняемые законом, и иную конфиденциальную информацию. Если настоящее сообщение попало не к его адресату, предупреждаем, что любое использование настоящего сообщения и приложенных к

существует возможность создания подписи и автоматической вставки ее в электронное сообщение. При необходимости можно создать несколько подписей для различных получателей;

11) не использовать КЭПС для агитации, пропаганды религиозных или политических идей;

12) не предоставлять пароль доступа к своему почтовому ящику другим лицам посредством электронной почты либо по телефону;

13) запрещается формирование и публикация сводных списков электронных почтовых адресов пользователей Университета, как в печатном, так и в электронном виде, а также передача таких списков третьим лицам;

14) не использовать КЭПС для создания грубых, оскорбительных или провокационных сообщений. Таковыми считаются, в том числе, сообщения, содержащие сексуальные домогательства, расовые оскорбления, дискриминацию по половому признаку или другие комментарии, затрагивающие в оскорбительной форме вопросы возраста, религиозные или политические пристрастия, национальность или состояние здоровья;

15) не использовать КЭПС при пересылке информации, конфиденциального характера;

16) учитывать принятые ограничения в Университете при отправке сообщения респонденту;

17) неукоснительно соблюдать принятые в Университете правила информационной безопасности и оказывать содействие администратору КЭПС и ответственному работнику Отдела информационной безопасности Университета в борьбе с нарушителями установленных правил.

6. Создание, блокировка и удаление почтовых ящиков

22. Корпоративные электронные почтовые ящики заводятся автоматически всем пользователям, при их оформлении в кадровой службе Университета на основании заявки на организацию рабочего места пользователю.

23. Логин и временный пароль к корпоративному почтовому ящику пользователь получает персонально.

24. Устанавливается временный пароль новых пользователей для доступа к корпоративным почтовым ящикам, пользователь может сменить свой пароль в соответствии с принятыми в Университете Правилами парольной защиты, при первом входе в КЭПС.

25. При изменении анкетных данных пользователю необходимо обратиться в HelpDesk;

26. В случае необходимости замены пароля для доступа к электронному почтовому ящику КЭПС пользователь должен обратиться в HelpDesk.

27. HelpDesk направляет обращение пользователя о сбросе пароля в Отдел информационной безопасности для рассмотрения.

28. После одобрения Отделом информационной безопасности Администратором КЭПС производится сброс пароля и устанавливается временный пароль.

29. Пользователю необходимо подойти за временным паролем в HelpDesk, предъявив документ, подтверждающий личность.

30. Удаление почтовых ящиков Пользователей производится администратором КЭПС на основании обходного листа работника Университета, обучающегося Университета. Процедура удаления предполагает блокировку корпоративного почтового ящика на 1 год и безвозвратное удаление по окончании данного срока.

31. Отмена блокировки корпоративного почтового ящика возможна, если блокировка произошла по причине ошибки, с обязательной процедурой подачи заявки в HelpDesk, так же отмена блокировки возможна по служебной записке, с согласованием заинтересованных сторон, на срок не более 1 года, с возможностью дальнейшего продления.

32. Восстановление содержимого корпоративного почтового ящика, удаленного по окончании срока блокировки, невозможно.

7. Ограничения при массовой рассылке сообщений на адрес группы all@enu.kz

33. Рассылка сообщений, объявлений для всеобщего обозрения пользователей Университета проходит обязательную проверку группой модераторов Университета, которые имеют право: удалять, блокировать сообщения, если они содержат запрещенную информацию, согласно установленным в Университете Правилам.

8. Мониторинг качества и результативности сервиса

34. В целях повышения качества функционирования сервиса и предупреждения случаев нарушения настоящих Правил ответственный работник Отдела информационной безопасности проводит регулярную, не реже одного раза в год, полную или выборочную проверку безопасности и корректности работы сервиса.

35. В ходе проведения проверки ответственным работником Отдела информационной безопасности производится проверка сервиса по перечисленным выше целям, а также выполняются следующие мероприятия:

1) производится выборочная проверка рабочих мест пользователей;

2) производится выборочная проверка скорости доставки сообщений;

3) производится выборочная проверка по доставке защищенных сообщений на предмет возможности взлома;

36. по согласованию с пользователем и его непосредственным руководителем производится выборочная проверка, отправленных по электронной почте писем пользователей, на предмет конфиденциальности отправляемой информации.

37. В рамках проведения проверки обеспечивается сохранность найденных «уязвимых» мест безопасности функционирования сервиса в секрете до устранения.

38. По результатам проведения проверки сервиса по отдельному запросу вышестоящего руководства ответственный работник Отдела информационной безопасности готовит сводный отчет по установленной форме «Отчет о проведении проверки корпоративной электронной почтовой системы» (Приложение 1).

9. Критерии и методы мониторинга качества и результативности функционирования сервиса

39. Критериями оценки качества и результативности функционирования сервиса являются следующие параметры:

1) количество негативных отзывов пользователей сервиса, оформленных в качестве служебных записок, заявок поданных в Help Desk, Отдел информационной безопасности, связанные с недоступностью или низким качеством функционирования сервиса;

2) количество выявленных нарушений по качеству сопровождения сервиса.

40. Сравнение количества и объема передаваемой и получаемой информации за отчетный период с аналогичным периодом прошедшего года.

10. Ответственность и полномочия

41. Ответственность за контроль внедрения требований, указанных в настоящих Правилах, несет руководитель Отдела информационной безопасности.

42. Отдел информационной безопасности имеет право проверять электронную переписку пользователей КЭПС без предварительного уведомления, если данная проверка будет согласована с курирующим Руководством, по форме, согласно Приложению 2 к настоящим Правилам.

43. Служба информационной безопасности имеет право на использование дополнительных аппаратных и программных средств, в целях защиты электронной почты от спам-рассылок и защиты служебной и конфиденциальной информации от утечек во внешнюю среду.

44. Пользователи несут ответственность за строгое соблюдение настоящих Правил.

45. Администратор КЭПС несет ответственность за:

1) установку и корректную настройку соответствующих механизмов, обеспечивающих функционирование КЭПС;

2) корректную интеграцию антивирусного комплекса с КЭПС, обеспечивающую надежную антивирусную защиту электронных сообщений;

3) качество работы КЭПС, включая отдельные его компоненты;

4) строгое соблюдение настоящих Правил.

46. Ответственный работник Отдела информационной безопасности несет ответственность за:

1) осуществление мониторинга по выполнению пользователями требований настоящих Правил;

2) осуществление по утверждённому курирующем Руководством плану, выборочную или массовую проверку рабочих мест, по соблюдению настоящих Правил пользователями;

3) строгое соблюдение настоящих Правил.

11. Заключительное положение

47. Ознакомление работников Университета с настоящими Правилами проводится руководителями структурных подразделений Университета с оформлением подписи в «Листе ознакомления к Правилам работы с КЭПС в Университете» (Приложение 3).

48. Ознакомление обучающихся Университета с настоящими Правилами проводится Департаментом по академическим вопросам с оформлением подписи в «Листе ознакомления к Правилам работы с КЭПС в Университете» (Приложение 3).

49. Пользователь несет ответственность за соблюдение настоящих Правил в соответствии с действующим законодательством Республики Казахстан и внутренними нормативными документами Университета.

Приложение 1
к Правилам

Отчет о проведении проверки корпоративной электронной почтовой системы

(ФИО)_____

Довожу до Вашего сведения результаты проверки использования КЭПС:

Основания для проведения проверки:

Дата проведения проверки:
Период, охваченный проверкой:
Проверено:

Выявлено:

Рекомендации:

Начальник Отдела
информационной безопасности
(подпись)_____ (ФИО)_____

Дата

Приложение 2
к Правилам

(ФИО)_____

Прошу разрешить проверку журналов входящей/исходящей электронной почты, следующих обучающихся/работников Университета.

Т.А.Ж / ФИО	Құрылымдық бөлімшенің атауы/ Наименование структурного подразделения	Кез /Период

Ответственный работник Отдела (подпись)_____
(ФИО)_____
информационной безопасности

Начальник Отдела (подпись)_____
(ФИО)_____
информационной безопасности

Приложение 3
к Правилам

Лист ознакомления

Правила работы с корпоративной электронной почтовой сис темой в НАО «Евразийский Национальный Университет им. Л.Н. Гумилева»

Т.А.Ж / ФИО	Лауазымы /Должность	Визаның қойылған күні/Дата визирования	Қолы /Подпись