МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского»
(ННГУ)

ПРИКАЗ

01.08.2024 № 06.49-04-044/24

Нижний Новгород

Об утверждении Инструкции по обеспечению информационной безопасности при работе с электронными почтовыми сервисами

В целях выполнения требований Федеральных законов от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27.07.2006 №152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию по обеспечению информационной безопасности при работе с электронными почтовыми сервисами в федеральном государственном автономном образовательном учреждении высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского» (далее – ННГУ) (Приложение).

2. Начальнику управления информатизации Махлай С.Н. организовать рассылку Инструкции всем пользователям корпоративной почты ННГУ.

3. Отделу развития бренда обеспечить размещение копии настоящего приказа на официальном сайте ННГУ в информационно-коммуникационной сети «Интернет» на главной странице подраздела «Документы».

4. Контроль за исполнением приказа возложить на проректора по безопасности Малышева А.Е.

Ректор О.В. Трофимов

2

Приложение
к приказу от 01.08.2024 № 06.49-04-0444/24

Инструкция
по обеспечению информационной безопасности при работе с электронными почтовыми сервисами в федеральном государственном автономном образовательном учреждении высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского»

1. Общие положения

1. Настоящая инструкция разработана с целью предотвращения компьютерных инцидентов и ознакомления сотрудников федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского» (далее – ННГУ) с основными положениями и требованиями по информационной безопасности при работе с корпоративными почтовыми сервисами.

2. Корпоративная электронная почта предоставляется сотрудникам ННГУ только для выполнения ими своих должностных обязанностей. Использование электронной почты для пересылки информации в личных целях запрещено.

3. Создание нового почтового ящика проводится только сотрудниками управления информатизации ННГУ в соответствии с действующим регламентом.

4. Сотрудники университета несут персональную ответственность за использование корпоративной электронной почты, и содержание электронных сообщений, отправляемых с помощью электронных ресурсов ННГУ.

5. Электронные письма, создаваемые и хранимые на персональных компьютерах ННГУ, являются собственностью данного учреждения и не подлежат огласке и использованию в личных целях.

6. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя, в случае разглашения сведений конфиденциальной информации или нарушения требований информационной безопасности.

7. Сотрудники должны регулярно проводить смену пароля от электронной почты, используя онлайн-сервис mail.unn.ru. При компрометации пользовательского пароля внеплановая смена пароля для этого пользователя производится незамедлительно.

8. В случае появления подозрений на факт компрометации пароля, выявления инцидентов, связанных со сбоями в аутентификации, или получения «фишинговых» писем (запрос пароля), сотрудники обязаны немедленно проинформировать об этом управление информационной безопасности.

9. При работе с корпоративными электронными почтовыми сервисами сотрудникам ННГУ **запрещается**:

- посылать электронные письма от чужого имени, передавать по электронной почте сведения, составляющие государственную тайну или материалы, имеющие пометку для служебного пользования (ДСП);
- работать в почтовом сервисе без установленных и активированных антивирусных средств на компьютере;
- переходить по подозрительным ссылкам, открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами (обычно производится автоматически), даже если отправитель письма хорошо известен;
- рассылать через электронную почту материалы, содержащие вирусы, компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли;
- распространять информацию, содержание и направленность которой запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной и религиозной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия;
- предоставлять кому бы то ни было пароли доступа к своему почтовому ящику и хранить значения своих паролей на бумажном носителе.

2. Меры безопасности

Для соблюдения мер информационной безопасности **необходимо**:

- проверять имя домена отправителя электронного письма в целях идентификации отправителя. Для этого необходимо обращать внимание на наименование почтового адреса (домена), указанного после символа «@», и сопоставлять его с адресами (доменами) органов (организаций), с которыми осуществляется служебная переписка.
- С особой осторожностью открывать почтовые вложения от неизвестных отправителей. Вложенные файлы, являющиеся исполняемыми программами, могут нести угрозу распространения вирусов, в частности с расширениями *.exe, *.bat, *.com, *.lnk, *.wsf. Подобные файлы также запрещены для пересылки. В почтовом сервисе ННГУ эти файлы автоматически блокируются и не могут быть отправлены с электронного адреса или получены на электронный адрес.
- не открывать и не загружать почтовые вложения писем с тематикой, не относящейся к деятельности ННГУ.

- учитывать **признаки** в письмах, которым не стоит доверять:

- ссылка в виде цифр (пример - 178.248.232.27);
- в тексте более чем одна ошибка или описка;
- ссылка содержит символ «@» (пример - http://bank.ru@phish.ru);
- ссылка с двумя и более адресами (пример - https://bank.ru/bitrix/rd.php?go=https://bitly.com/bank);
- письма с отсутствующими дополнительными контактами (ФИО, должность, телефон, почтовый адрес);
- если в начале адреса сайта есть www, но нет точки или стоит тире (пример - wwwbank.ru или www-bank.ru);
- если в начале адреса сайта есть http или https, но нет «://» (пример - httpsbank.ru);
- когда в адресе сайта несколько точек, смотрите то, что написано в правой части, до первого символа «/», там вы обнаружите исходный сайт и, если он вам не знаком, то ссылка считается подозрительной (пример - www.bank.ru.zlodey.ru/login?id=12/aa/bank.ru);
- email в поле «Отправитель» может быть подделан или самого отправителя могли взломать;
- если при наведении указателя «мыши» ссылка выглядит по-другому (пример - в тексте письма написано tele2.ru, а при наведении мыши, в нижнем левом углу браузера отображается teie2.ru);
- ссылка может быть не кликабельна, но содержать подмененные символы. Злоумышленник надеется, что вы скопируете ссылку и вставите в браузер (пример - в письме указана ссылка teIe2.ru, копируете и вставляете в браузер, но оказывается, что это teie2.ru);
- злоумышленник может заменить букву “o” на цифру “0” или маленькую латинскую букву L — “l”, на большую букву i — “I” или b на d, использовать сочетание букв (rn вместо буквы m, cl вместо d, vv вместо w) и т.д. (пример - 0nIinedank.ru вместо onlinebank.ru);
- если ссылка начинается с https:// — это не значит, что она безопасна;

3. Подозрительные письма

При получении подозрительного письма **необходимо:**

- лично, по телефону, через мессенджер уточнить факт отправки такого письма. Желательно, контакт для связи взять не из письма, а из других источников (собственная записная книжка, визитка, спросить у коллег, узнать на официальных сайтах);

- не открывая вложения и ссылки переслать письмо в управление информационной безопасности (uib@unn.ru).