Комитет по образованию
Санкт-Петербурга

МОРСКАЯ ТЕХНИЧЕСКАЯ АКАДЕМИЯ
имени адмирала Д.Н. Сенявина

ПРИКАЗ

№ 568 «10» ноября 2023 г.

«Об усилении мер безопасности при работе
с электронной почтой в подразделениях академии»

В соответствии с письмом Комитета по образованию от 07.11.2023 № 03-17-133/23-0-0, письмом Комитета по информатизации и связи от 01.11.2023 № 15-02-8466/23-0 и от 24.07.2023 № 15-02-5585/23-0 «О мерах по повышению защищенности информационной инфраструктуры Российской Федерации» и с целью обеспечения устойчивого функционирования автоматизированных рабочих мест, имеющих доступ в сеть интернет, и предотвращения реализации угроз безопасности информации, связанных с фишингом, при работе с электронной почтой

ПРИКАЗЫВАЮ:

1. Продолжить функционирование академии в условиях усиленных мер по обеспечении безопасности.
2. Руководителям всех подразделений проинформировать сотрудников о необходимости:
   - проверки адреса отправителя, даже в случае совпадения имени с уже известным контактом;
   - проверки писем, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
   - проверки ссылок, содержащихся в электронном письме, даже если письмо получено от другого пользователя информационной системы;
   - внимательного отношения к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;
   - отправки подозрительных писем, получаемых пользователями почтового сервиса, на единый (отдельный) электронный почтовый адрес (далее – Почтовый адрес) для их проверки администратором безопасности. При возможности для этих целей использовать почтовую «песочницу»;
   - осуществлять проверку всех поступающих на почту вложений с использованием средств антивирусной защиты, антиспама.
3. Начальнику отдела информатизации Козлову А.С.:
   - создать Почтовый адрес, на который пользователи информационной системы будут присылать письма, которые могут содержать вредоносное содержание (ссылку или вложение) и сообщить данный адрес руководителям подразделений;
   - отслеживать сроки действия лицензий антивирусной защиты;
   - использовать для работы с электронной почтой учетные записи пользователей операционной системы с минимальными возможными привилегиями;
   - активировать механизмы проверки электронной почты, проверки подлинности домена-отправителя (например, использовать технологии DKIM, DMARC, SPF), а также настроить проверку входящих писем с использованием этих технологий (в соответствии с рекомендациями Комитета по информатизации и связи от 24.07.2023 № 15-02-5585/23-0);
   - на Почтовый адрес переадресовывать электронные письма с вложениями, имеющие следующие расширения: ADE, ADP, APK, APPX, APPXBUNDLE, BAT,

CAB, CHM CMD COM CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH с последующей их фильтрацией;

- организовать формирование базы доменов отправителей, входящих в «черный» список;
- минимизировать коммуникации на сетевом уровне по протоколу SMPT с зарубежными IP-адресами;
- настроить функции уведомления пользователей в тексте сообщения при получении электронного письма от внешнего отправителя.

4. Принять к сведению, что ответственность за обеспечение защиты информации на рабочем месте пользователя возлагается непосредственно на пользователя (потребителя информации).

5. Начальнику отдела информатизации Козлову А.С. с целью оперативного информирования сотрудников разместить настоящий приказ на сайте академии в разделе «Информационная безопасность» в срок до 15.11.2023.

6. Контроль за исполнением настоящего приказа возлагаю на заместителя директора по информатизации и внешним связям Урядова А.К.

Директор академии В.А. Никитин