Руководителям
отделов, лабораторий и подразделений

О мерах по предотвращению реализации угроз безопасности информации

Анализ сведений об угрозах безопасности информации, проводимый в условиях сложившейся обстановки, показывает, что зарубежными хакерскими группировками планируются компьютерные атаки на информационную инфраструктуру Российской Федерации. С целью предотвращения реализации угроз безопасности информации рекомендуется принять следующие дополнительные меры защиты информации:

1. Обеспечить резервирование информации, обрабатываемой в информационной системе и наличие актуальных резервных копий.
2. Обеспечить хранение резервных копий в изолированном от сети «Интернет» сегменте информационной системы (съемный носитель информации).
3. Для защиты научных разработок, обработку результатов экспериментов следует производить на компьютерах, изолированных от сети «Интернет». По окончании работ данные переносить на съемные носители.
4. Запретить пользователям подключать к информационным системам неучтенные носители информации, мобильные устройства, открывать любые ссылки из почтовых сообщений, скачивать файлы из сети «Интернет».
5. Запретить подключение личных мобильных устройств (смартфоны, планшеты и т.п.) к беспроводным сетям (wi-fi) института.
6. Пользователи информационной системы института обязаны соблюдать правила безопасной работы с электронной почтой, а именно:

- внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;
- не открывать письма от неизвестных адресатов;
- не открывать письма в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы и т.д.;
- не переходить по ссылкам, которые содержаться в электронных письмах;
- не нажимать на ссылки из письма, если они заменены на слова, не наводить на них мышкой и просматривать полный адрес сайтов;
- проверять ссылки, даже если письмо получено от другого пользователя информационной системы института;
- не открывать вложения;
- внимательно относится к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;
- в случае появления сомнений – направлять полученное письмо как вложение администратору информационной системы на адрес **karantin@academpharm.ru**;
- письма от доменов-отправителей, страной происхождения которых являются США и страны Европейского союза **в любом случае** пересылать на указанный выше адрес.

С данной рекомендацией должен быть ознакомлен каждый сотрудник лаборатории.

Ответственный за кибербезопасность
Заместитель директора по общим вопросам С.В. Власов