Памятка по информационной безопасности

При соблюдение данных простых правил вы значительно повышаете информационную безопасность в университете от возможных различных утечек.

**Соблюдайте данные правила:**

* Не допускайте посторонних лиц к работе на закрепленном компьютере (кроме случаев, связанных с выполнением работ специалистами технического подразделения, в рамках своих служебных и должностных обязанностей, или по указанию руководителя отдела);
* Не открывайте или запускайте приложения, полученные по электронной почте из неизвестного источника, с подозрительным названием и (или) не затребованные пользователем;
* Не передавайте параметры доступа к почтовому ящику третьим лицам;
* Не посещайте следующие категории сайтов: о наркотиках; о насилии; о терроризме; сайты содержащие нецензурную лексику; сайты связанные с азартными и прочими играми; об оружии; порносайты; чаты; социальные сети; сайты электронных почтовых серверов, не являющихся почтовыми системами Университета
* Не получайте и передавайте через линии связи информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения;
* Не играть в различные игры;
* Не использовать различные сайты и программы для анонимного доступа в сеть Интернет;
* Не использовать программы для зарабатывания денег в сети интернет.
* Не скачивать музыкальных и видео файлов, а также файлов, не имеющих отношения к текущим служебным обязанностям работника, без согласования с руководством.
* Не использовать оборудование, сетевые программы для деятельности, не обусловленной производственной необходимостью и должностной инструкцией;
* Самостоятельно не устанавливать или удалять любое ПО на компьютерах, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;
* Самостоятельно не переустанавливать операционные систему.
* Не вскрывать компьютеры, сетевое и периферийное оборудование, разбирать, изменять настройку оборудования общего пользования, подключать к компьютеру дополнительное оборудование, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет, дисков, FLASH-накопителей и др;
* Самовольно не подключатся компьютеру к Сети Университета, а также изменять IP и MAC-адрес компьютера, устанавливать дополнительные сетевые протоколы, изменять конфигурацию настроек сетевых протоколов без предварительного уведомления ДИ. Передача данных в сеть с использованием других IP и MAC адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах;
* Не получать и не передавать в сеть информацию, противоречащую законодательству и нормам морали общества, представляющую конфиденциальную, коммерческую или государственную тайну, распространять через сеть информацию, которая охраняется законодательством об интеллектуальной собственности, либо задевающую честь и достоинство граждан, а также рассылать обманные, угрожающие и др. сообщения;
* Не предпринимать попытки обхода учетной системы безопасности, системы статистики, ее повреждения или дезинформации;
* Не использовать иные формы доступа к сети, пытаться обходить установленный межсетевой экран;
* Не закрывать доступ к информации паролями без согласования с руководителя подразделения;
* Не передавать другим лицам свои личные атрибуты доступа (регистрационное имя и пароль) к компьютеру, а также предоставлять доступ к каналам сети пользователям других сетей (например, посредством proxy-server, socks-proxy, open relay и т.п.);
* Не использовать, распространять и хранить программы, предназначенные для осуществления несанкционированного доступа, взлома паролей, для нарушения функционирования компьютерного оборудования и компьютерных сетей, а также компьютерные вирусы и любые программы ими инфицированные, использовать, распространять и хранить программы сетевого управления и мониторинга, осуществляющих сканирование сети (различные «трассеры», «сниферы», сканеры портов и т.п.), без письменного предупреждения и разрешения ДИ, а также разрешения службы безопасности Университета, с объяснением служебной необходимости подобных действий;
* Не предоставлять доступ к компьютерному оборудованию незарегистрированным пользователям без согласования с руководителем отдела;
* Не использовать в работе съемные носители информации без непосредственного руководителя. Съемные носители информации, перед началом работы с ними, обязательно должны пройти проверку антивирусной программой;
* Не хранить файлы, не относящихся к выполнению служебных обязанностей сотрудника (музыка, фотографии, игры, видео, виртуальные CD и т.п.);
* Не оставлять авторизированными рабочие компьютеры при покидание рабочего места.