ПАМЯТКА-ИНСТРУКЦИЯ

пользователю Сеченовского Университета

по обеспечению информационной безопасности

Парольная защита

•Никогда не сохраняйте ваши пароли в программах. Большинство программ хранят их в открытом виде и тот, кто получит доступ к вашему компьютеру, получит доступ и к ним. •Сохраняйте в тайне личный пароль. Никогда не сообщайте пароль другим лицам, и не храните записанный пароль в общедоступных местах.

•В случае производственной необходимости (командировка, отпуск и т.п.), при проведении проверочных мероприятий, работ, требующих знания пароля пользователя, допускается раскрытие значений своего пароля начальникам этих подразделений. По окончанию производственных, или проверочных работ работники самостоятельно производят немедленную смену значений "раскрытых" паролей.

•Не используйте пароль доступа в локальную сеть Университета в других программах и на сайтах, где требуется регистрация;

•Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями АС самостоятельно с учетом следующих требований:

* длина пароля должна быть не менее 8 символов;
* в числе символов пароля обязательно должны присутствовать латинские буквы и цифры;
* пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
* при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
* личный пароль пользователь не имеет права сообщать никому.

Антивирусная защита.

•Никогда не отключайте установленное на АРМ антивирусное программное обеспечение.

•Обязательно проверяйте на наличие вирусов все внешние носители информации (дискеты, диски, флешки и т.п.), поступающие со стороны (из внешних организаций, других подразделений Университета и т.п.)

•Не подключая компьютер к сети Интернет, локальной или беспроводной сети, проверить систему на предмет наличия/отсутствия вирусов и другого вредоносного ПО. Один из способов – использование регулярно обновляющейся бесплатной утилиты DrWebCureIT-: необходимо предварительно скачать из сети Интернет (<http://www.drweb.ru/download/>).

Интернет и электронная почта.

•Содержание Интернет-ресурсов, а также файлы, загружаемые из Интернета, обязательно проверяйте на отсутствие вредоносных программ и вирусов.

•Не переходите по ссылкам, не запускайте программы и не открывайте файлы, полученные по электронной почте от неизвестного Вам отправителя.

•Не передавать по электронной почте Ваши пароли.

•Не принимайте никаких соглашений при посещении сайтов, смысла которых Вы не понимаете.

Общие требования

•Не устанавливайте самостоятельно программное обеспечение, если это не входит в Ваши обязанности. Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению Ваших должностных обязанностей программное обеспечение;

•Располагайте мониторы и печатающие устройства таким образом, чтобы исключить несанкционированный доступ к отображаемой и печатаемой информации.

•При временном оставлении рабочего места в течение рабочего дня в обязательным порядке блокируйте компьютер нажатием комбинации клавиш «Win+ L».

Начальник Службы информационной безопасности И.В. Спивак

20.09.2021