



Братство организаторов
студенческого самоуправления



ПАМЯТКА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ УРОВЕНЬ «НОВИЧОК»

Памятка по обеспечению безопасности персональных данных Уровень «новичок»

Цель настоящей памятки – познакомить читателей с основами компьютерной грамотности и безопасности при работе с важными документами.

Настоящая информация не является исчерпывающей, поэтому мы будем рады вашим комментариям, вопросам и предложениям!

С любовью, БОСС ^^

Часть 1 Как обезопасить свой компьютер/ ноутбук/ планшет/ флешку



Всегда нужно исходить из того, что доступ к вашим данным рано или поздно получают посторонние. Флешку можно потерять, компьютер может перестать работать. Опустим печальные истории о воровстве документов, копировании личной информации и использовании ее против вас. Как говорить: «Береженого и Бог бережет!»

Поэтому давайте вспомним и разберем простые пункты компьютерной грамотности и безопасности.

1. Не использовать одну УЧЕТНУЮ ЗАПИСЬ для всех пользователей компьютера, тем более с правами администратора.

2. Использовать ПАРОЛЬ ДЛЯ ВСЕХ учетных записей пользователей компьютера. Запретить гостевой вход в систему.

2.1. В идеале пользователи не должны обмениваться своими паролями даже при полном доверии друг другу.

2.2. Не стоит пытаться придумать и запомнить пароль, который читается с трудом, вы его забудете быстро и легко. Используйте:

- короткую фразу;
- в которой несколько букв заменены цифрами;
- она может иметь или не иметь смысл;
- содержать или не содержать ошибки в словах.

Например, «Жм8ут галбши офигенн1» (Жмут галоши офигенно), «Бур9 мгл0ю небо кр0ет» (Буря мглою небо кроет), «С0нца светет 9рка» (Солнце светит ярко).

Помните, что лучше допустить одну ошибку, заменить одну и ту же букву одной и той же цифрой. Со временем сложный пароль вы-то вспомните, а какие ошибки допустили и цифры использовали, может остаться тайной.

3. Потратить некоторое время на РАЗГРАНИЧЕНИЕ ДОСТУПА.

Ограничения доступа должны быть максимально жёсткими, но при этом достаточно свободными для комфортной работы пользователей. Чтобы задать правила доступа к ресурсу (например, к папке, диску) (см. Приложение 1 в конце) в ОС начиная с Windows XP достаточно открыть свойства папки и во вкладке «Безопасность» нажать кнопку «Изменить». Задавать их можно как для конкретных пользователей поименно, так и для групп.

Например, пусть все члены семьи пользуются одним компьютером и для каждого настроена отдельная учетная запись, при этом имеется группа “Неопытные пользователи”, куда входят Мама и неграмотный по малолетству Петя. Имеет смысл разрешить пользователю Вася полный доступ к папке “Васина папка”, а группе “Неопытные пользователи” и пользователю Вася разрешить просмотр содержимого папки “Семейные фотографии”. В таком случае мама и Петя не смогут просмотреть или повредить Васиные файлы, бездумно согласившись на установку вредоносных программ от своего имени.

4. Использовать программные сетевые экраны (firewall) или комплексы интернет-безопасности (internet security suite) при работе на компьютере, подключенном к сети.

В Интернете полно людей и автоматических сканеров, постоянно ищущих компьютеры, к которым можно подключиться и использовать уязвимости ПО для своих целей. Провайдер и домашний маршрутизатор могут блокировать часть входящих подключений, но при работе с важными данными не следует полагаться на них полностью.

Выбор имеется, бесплатных хватает:

- ZoneAlarm (про настройку можно прочитать здесь <http://sonikelf.ru/zashhishhaemsysya-ot-xakerov-chervej-i-prochej-shushery/>, только

Это был превью ☺

Если вы хотите получить полную версию памятки, заполните на сайте форму, и вам будет выслана на ящик ссылка для скачивания. Скачать памятку можно БЕСПЛАТНО!

Форма для заполнения: <http://aboss.by/metodichka-kompyuternaya-bezopasnost>

Спешите жить в безопасном интернете!