

Быкова О.И., Герасим О.Ч.

БГЭУ, ФФБД, группа ДФК-2, ДФР-1, 1 курс

ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Цель:

1. выяснить, что угрожает нашей компьютерной безопасности
2. выяснить, каким образом возможно обеспечить компьютерную информационную безопасность
3. определить основные правила компьютерной безопасности

Задачи:

1. проверить, возможно ли следовать этим правилам на практике
2. выяснить, что мы приобретаем если будем следовать этим правилам
3. выяснить, что мы теряем, если будем следовать этим правилам

Объект: теоретические и практические аспекты компьютерной безопасности

Предмет: возможность применения на практике правил компьютерной информационной безопасности.

Актуальность работы. Современная экономика полностью ориентирована на применение информационных технологий: как новейших технических средств, так и огромного количества информационных баз данных, где находится огромный объем информации о клиентах, партнерах, конкурентах и вообще о любых людях. Если объединить все базы организаций, получается огромный массив информации обо всех направлениях деятельности человека. Именно из-за этого растет уровень обеспокоенности населения, тем, что о них известно практически все, т.е. за ними следят.

Научная новизна работы заключается в том, что несмотря огромное количество различных правил по поводу того, как себя вести, мы решили опробовать эти правила на себе, чтобы выяснить, возможно ли им следовать.

Правило №6. Как можно реже пользуйтесь компьютером в общественных местах. Но как быть тем людям, чья работа требует постоянного наличия инетрнет-соединения?

Правило №5. Никогда не храните личную информацию на компьютере. Следовать этому правилу вполне реально. Нам кажется, что не составляет труда перенести личную информацию на внешние носители.

Правило №4. Покупайте симкарты для телефонов в подземных переходах, где у вас не требуют паспорт. Однако, как мы выяснили для нашей страны данное правило не является актуальным. Вы не сможете купить сим-карту без регистрации паспортных данных.

Правило №3. Никогда не подписывайтесь ни на какие компьютерные рассылки. К этому правилу нужно подходить избирательно: не подписываться на компьютерные рассылки, источнику которого мы не доверяем.

Правило №2. Используйте программы-анонимайзеры. Это правило имеет место быть, но оно не обеспечивает 100% защиты. Опытный хакер без труда определит ваш IP, даже если вы используете такие программы.

Правило №1. Не верьте всему, что пишут в интернете! Сейчас огромное количество людей убеждены: телевидение и газеты лгут, правду пишут только в интернете. На самом деле интернет является точно таким же СМИ как и телевидение, только нового уровня. Поэтому, во-первых, нельзя доверять одному источнику и, во-вторых, надо проверять любую информацию.

Таким образом, если мы будем следовать этим правилам, мы в какой-то степени сохраним свою безопасность и анонимность, а также сможем оградить себя от негативного воздействия информации на нас.

LLLLLLLLLLLL LLLLLLLLLLLLL LLLLLLLLLLLLL LLLLLLLLLLLLL. LLLLLLLLLLLLL.
LLLLLLLLLLLL LLLLLLLLLLLLL LLLLLLLLLLLLL LLLLLLLLLLLLL. LLLLLLLLLLLLL.

БДЭУ Беларускі дзяржаўны эканамічны ўніверсітэт. Бібліятэка.
БГЭУ Белорусский государственный экономический университет. Библиотека.
BSEU Belarus State Economic University. Library.
<http://www.bseu.by> elib@bseu.by