ІПЗ-33\1 Гоша Давід Олександрович

Лабораторна №1

№	Вид загрози	Можливий механізм реалізації загрози	Джерело загрози	Наслідки			Шляхи запобігання (Заходи нейтралізації)
				Ц	К	Д	
1	Загроза віддаленого адміністрування	Віддалене адміністрування дозволяє брати чужий комп'ютер під своє управління. Це може дозволити копіювати і модифікувати наявні на ньому дані, установлювати довільні програми, у тому числі й шкідливі, використовувати чужий комп'ютер для вчинення злочинних дій у мережі від імені його власника	Людина	+	+	+	Варто обмежити доступ сторонніх осіб до мережних комп' ютерів звичайним адміністративним способом (фізичне обмеження доступу, пароль тощо)
2	Загроза активного змісту	Активний зміст - це активні об'єкти, вбудовані у веб-сторінки. На відміну від пасивного змісту (текстів, малюнків, аудіокліпів тощо), активні об'єкти містять у собі не тільки дані, а й програмний код, що одержує клієнт веб-сторінки, яка завантажується. Агресивний програмний код, що потрапив у комп' ютер, здатний поводитися як комп'ютерний вірус чи як агентська програма. Так, наприклад, він може як руйнувати дані, так і взаємодіяти з віддаленими програмами і, таким чином, працювати як засіб віддаленого доступу чи готувати ґрунт для його установки.	Веб-застосунок	+	+	+	Захист від активного змісту. Сторона, яка захищається, повинна оцінити загрозу своєму комп' ютеру і, відповідно, налаштувати браузер так, щоб небезпека була мінімальною.

3	Загроза перехоплення чи підміни даних на шляхах транспортування	Наприклад, розрахунки електронними платіжними засобами (картками платіжних систем) передбачають відправлення покупцем конфіденційних даних про свою картку продавцю. Якщо ці дані будуть перехоплені на одному з проміжних серверів, немає гарантії, що ними не скористається зловмисник. Крім того, через Інтернет передаються файли програм. Підміна цих файлів під час транспортування може призвести до серйозних негативних наслідків.	Веб або Десктоп застосунки	+	+	-	Підтвердження (аутентифікацію) цілісності даних. Сьогодні в електронній комерції захищають і аутентифікують дані, а також ідентифікують віддалених партнерів за допомогою криптографічних методів, технологічно реалізованих в ЕЦП.
4	Загроза втручання в особисте життя	В основі цієї загрози лежать комерційні інтереси рекламних організацій. У наш час річний рекламний бюджет Інтернету складає кілька десятків мільярдів доларів США. У бажанні збільшити свої доходи від реклами безліч компаній організує веб-вузли, причому не стільки для того, щоб надавати клієнтам серверні послуги, скільки для того, щоб збирати про них персональні відомості	Веб-додатки, операційні системи	-	+	-	Захист від втручання в особисте життя. Збір відомостей про учасників роботи в Інтернеті. Крім засобів активного впливу, існують і засоби пасивного спостереження за діяльністю учасників мережі Інтернет. Вони використовуються рекламно-маркетинговими службами.
5	Загроза постачання даних неприйнятного змісту	Не вся інформація, яка публікується в Інтернеті, може вважатися суспільно корисною, і досить часто люди хочуть від неї захиститися.	Застосунки які мають доступ до мережі інтернет	-	-	-	Налаштування фільтрації неприянатного контенту. Майже усі соціальні мережі та браузери мають можливість обмежувати доступ до дорослого або шокуючого контенту автоматично.