**Загрози при роботі в Інтернеті і їх уникнення**

**Як програмне забезпечення може становити загрозу інформаційній безпеці користувача Інтернету?**

Сьогодні найбільшу кількість інформації опрацьовують за допомогою персональних або робочих комп’ютерів, саме тому атаки на комп’ютерні системи набули такої поширеності. До таких атак ми можемо віднести:

* шкідливе програмне забезпечення (віруси);
* інтернет-шахрайство;
* атаки на відмову в обслуговуванні;
* крадіжки коштів; крадіжки персональних даних;
* несанкціонований доступ до інформаційних ресурсів та систем;
* розповсюдження завідомо недостовірної інформації.

Крім того, вам відомі основні загрози інформаційній безпеці користу­вача Інтернету, які йдуть від авторизованих користувачів та електронних методів впливу.

Розглянемо вплив на безпеку з боку різного шкідливого програмного забезпечення, яке поширюється мережею Інтернет.

**Шкідливе програмне забезпечення** (англ. malware, malicioussoftware — шкідлива програма, зловмисне програмне забезпечення) — будь-яке програмне забезпечення, призначене для отримання несанк­ціонованого доступу до обчислювальних ресурсів самого комп’ютера або до інформаційних ресурсів, які зберігаються на ньому, призначене для несанкціонованого власником їх використання чи спричинення шкоди (нанесення збитку) власникові комп’ютера, інформації чи комп’ютерній мережі шляхом копіювання, спотворення даних, видалення або підміни інформації. Термін «шкідлива програма» *(malware* — це скорочення від *«malicioussoftware*») за трактуванням корпорації *Microsoft* зазвичай ви­користовується як загальноприйнятий термін для позначення будь-якого програмного забезпечення, спеціально створеного для того, щоб заподі­ювати збитки окремому комп’ютеру, серверу або комп’ютерній мережі, незалежно від того, чи є воно вірусом, шпигунською програмою тощо.

Перешкодами в роботі зараженого комп’ютера є: починаючи від від­криття-закриття піддону CD-ROM і закінчуючи знищенням даних і по­ломкою апаратного забезпечення; блокування антивірусних сайтів, антивірусного програмного забезпечення й адміністративних функцій операційної системи з метою ускладнення їх лікування; саботаж вироб­ничих процесів, керованих комп’ютером (цим відомий хробак *Stuxnet).*

Виконуючи інсталяцію іншого шкідливого програмне забезпечення: завантаження з мережі (*downloader*); розпаковування іншої шкідливої програми, що вже міститься всередині файла*{dropper),* шкідливе про­грамне забезпечення зменшує ресурси комп’ютера.

До несанкціонованих дій із даними відносять: крадіжку, шахрай­ство, здирство і шпигунство за користувачем. Для крадіжки може засто­совуватися сканування жорсткого диска, реєстрація натиснень клавіш *(Keylogger)* і перенаправлення користувача на підроблені сайти, в точності повторюючи вихідні ресурси; викрадання даних, які представляють цін­ність або таємницю; крадіжка аккаунтів різних служб (електронної по­шти, мессенджерів, ігрових серверів, платіжних систем). Аккаунти при цьому застосовуються для розсилання спаму, а через електронну пошту можна роздобути паролі від інших аккаунтів, водночас як віртуаль­не майно можна продати в MMOG (*Massivelymultiplayeronlinegame).*

Шкідливе програмне забезпечення створює блоку­вання комп’ютера, шифрування файлів користувача з метою шантажу і здирства грошових коштів. Зде­більшого після оплати комп’ютер або не розблокову- ється, або незабаром блокується вдруге. Шкідлива програма використовує телефонний модем для здійс­нення дорогих дзвінків, що спричиняє значні суми в телефонних рахунках. Можливим є також створення платного програмного забезпечення, яке імітує, на­приклад, антивірус, але нічого корисного для цього не робить (*fraudware* або *scareware).*

Шкідливі програми також виконують іншу не­законну діяльність: отримання несанкціонованого (і дармового) доступу до ресурсів самого комп’ютера або третіх ресурсів, доступних через нього, у т.ч. пря­ме управління комп’ютером (так званий *backdoor*); здійснюють організацію на комп’ютері відкритих релеїв і загальнодоступних проксі-серверів. Зара­жений комп’ютер (у складі ботнета) може бути ви­користаний для проведення DDoS-атак, збирання адрес електронної пошти й поширення спаму, у т.ч. у складі ботнета. До такої діяльності належить також накручування електронних голосувань, клацань по рекламних банерах; генерування монет платіжної системи Bitcoin, використання ефекту 25-го кадра для зомбування людини.

Небажане програмне забезпечення може запису­вати файли, які не є істинно шкідливими, але зде­більшого небажаними: жартівливе програмне забез­печення, тобто робить які-небудь речі, що непокоять користувача. Наприклад, програма *Adware* показує рекламу, а програма *Spyware* посилає через мережу Інтернет інформацію, несанкціоновану користува­чем. Створюють видимість «отруєння» документів, які дестабілізують програмне забезпечення, що від­криває їх (наприклад, архів розміром менше мегабайта може містити гігабайти даних, а при його архівуванні може надовго «зависнути» архіватор). Програми віддаленого адміністрування можуть застосовуватися як для того, щоб дистанційно вирішувати проблеми з комп’ютером, так і для зловмисних цілей.

Інколи шкідливе програмне забезпечення для власного «життєзабез­печення» встановлює додаткові утиліти: IRC-клієнти, програмні марш- рутизатори, відкриті бібліотеки перехоплення клавіатури. Таке програм­не забезпечення не є шкідливим, але разом з ним встановлюється більш шкідлива програма, яка визначається антивірусами. Буває навіть, що шкідливим є тільки скрипт з одного рядка, а останні програми сповна ле­гітимні.

Шкідливі програми за методом розмноження:

1. експлойт — теоретично нешкідливий набір даних (наприклад, графіч­ний файл або мережевий пакет), що некоректно сприймається програ­мою, яка працює з такими даними. Тут шкоду наносить не сам файл, а неадекватна поведінка програмного забезпечення з помилкою. Також експлойтом називають програму для генерування подібних «отрує­них» даних;
2. логічна бомба в програмі спрацьовує за певної умови, є невід’ємною від корисної програми-носія;
3. троянська програма не має власного механізму розмноження;
4. комп’ютерний вірус розмножується в межах комп’ютера та через змін­ні диски. Розмноження через локальну мережу можливе, якщо корис­тувач сам викладе заражений файл у мережу. Віруси, водночас, поді­ляються за типом файлів, що заражаються (файлові, завантажувальні, макро-файлові, такі, що автозапускаються); за способом прикріплення до файлів (паразитні, супутні й такі, що перезаписують) тощо;
5. мережевий хробак здатний самостійно розмножуватися мережею. По­діляється на IRC2, поштові, такі, що розмножуються за допомогою експлойтів і т.д.

Шкідливе програмне забезпечення може утворювати ланцюжки: на­приклад, за допомогою експлойта на комп’ютері жертви розгортається завантажувач, який встановлює з мережі Інтернет хробака.

**Чи є безпечним використання публічного Wi-Fi?**

Сьогодні багато хто з нас користується Інтернетом за допомогою ноут- буків чи смартфонів. Для зручності в багатьох публічних місцях (кафе, ба­рах, готелях, торговельних центрах та навіть трамваях) є можливість ско­ристатися Wi-Fi і без проблем подивитися на прогноз погоди, перевірити електронну пошту, чи надіслати щось у соціальну мережу. Але користу­вача в загальнодоступних Wi-Fi мережах може очікувати ряд загроз. При підключенні до Wi-Fi пристрої (ноутбук, планшет чи смартфон) почина­ють передавати та отримувати інформацію в Wi-Fi мережі. Зловмисник, використовуючи спеціальні програми, може зібрати різну інформацію че­рез мережу: які пристрої підключені, чи є загальнодоступні ресурси (фай­ли, папки, принтери) на підключених пристроях, на які сайти заходять користувачі цих пристроїв. Деякі з цих програм (*Zenmap, Inssider, Wi­FiAnalyzer)* можна без проблем легально знайти в Інтернеті. При більш серйозному підході зловмисники також можуть отримати інформацію про введені логіни та паролі.

**Які загрози здоров’ю користувача може становити Інтернет?**

Основною проблемою забезпечення психологічної безпеки, у першу чергу психологічного здоров’я користувачів комп’ютерними і мереже­вими технологіями, стала проблема інформаційного (когнітивного) пе­ревантаження. Специфіка гіпертекстового формату подання інформації призвела до виникнення в користувача Інтернету особливого психологіч­ного феномена, який отримав назву «проблема втрати орієнтації в гіпер- просторі» (англ. *Lostinhyperspaceproblem).* Цей психологічний феномен проявляється в тому, що користувач не може локалізувати своє місцезна­ходження в інформаційному просторі веб-сайту, він постійно повертаєть­ся до одних і тих самих матеріалів, не розуміє, куди йому треба звертати­ся за потрібного інформацією (навіть якщо підозрює, що вона існує десь у досліджуваному гіпертекстовому просторі), не знає, як повернутися до раніше переглянутих тем, забуває початкові мотиви свого пошуку і зміст переглянутих веб-сторінок тощо. Утрата орієнтації в гіперпросторі часто веде до втрати смислових зв’язків між кількістю переглядів матеріала­ми, і майже завжди викликає вкрай поверхневе сприйняття їх змісту.

Другою не менш істотною проблемою є безконтрольне поширення в мережі інформації, яка може завдати психологічної травми або спрово­кувати користувача на вчинення будь-яких протиправних дій. Для вирі­шення цих проблем достатньо успішно ведуться роботи з вдосконалення різних видів користувальницького інтерфейсу, а також зі створення про­грамних додатків, здатних фільтрувати інформаційний потік за заданим набором параметрів.

В окремих користувачів Інтернету, які затрачають на це багато часу, спостерігається ефект відчуження від соціального оточення. Відомі випад­ки, коли інтенсивне застосування Інтернету призводить до звуження соці­альних зв’язків аж до самотності, скорочення родинного спілкування й на­віть до розвитку депресивних станів. Існують й інші дані, що свідчать про негативний вплив Інтернету на індивідуальну та групову психічну діяль­ність. Наприклад, було доведено, що використання Інтернету може сприя­ти аутизации дітей і підлітків, вести до порушень у процесах їх соціальної адаптації тощо.

Фахівці-психологи наголошують на складних взаєминах людської психіки з феноменом віртуальної реальності (англ. *MUD* — *Multi- UserDimensions),* про можливий зв’язок віртуального світу з проблема­тикою змінених станів свідомості, неконтрольованої психологічної за­лежності від Інтернету, яка набуває хворобливі форми. Психологічну небезпеку становить захоплення рольовими іграми в Інтернеті, їх мож­ливий зв’язок з асоціальною поведінкою, психологічна мотивація вико­ристання аватара як спробу змінити свою ідентичність або створювати множинну мережеву ідентичність тощо.

Небезпек психологічного впливу Інтернету на людину можна уник­нути через власний контроль часу роботи в Інтернеті, розвиток уміння ставити цілі, завдання та здійснювати предметний пошук відомостей в Інтернеті. А проблеми, які вже виникли через необдумане використання Інтернету, важливо обговорювати з батьками та психологами.

**Яких правил варто дотримуватись при користуванні Інтернетом?**

Вам уже відомі загальні правила безпечного використання Інтернету:

1. перед підключенням до Інтернету необхідно перевірити, чи включе­но антивірусний захист на комп’ютері користувача, й оновити (якщо необхідно) версію захисного програмного забезпечення;
2. не рекомендується активізувати гіперпосилання, які можуть призвес­ти до завантаження на комп’ютер користувача будь-яких файлів;
3. не рекомендується встановлювати на комп’ютер користувача про­грамне забезпечення з невідомих веб-сайтів;
4. не варто активізувати банери (рекламного чи розважального характе­ру), які розміщені на незнайомих користувачеві веб-сайтах;
5. забороняється відкривати файли, прикладені до електронних пошто­вих відправлень, адресант яких користувачеві невідомий;
6. не рекомендується ділитись в Інтернеті будь-якою особистою ін­формацією;
7. забороняється проводити будь-які фінансові операції через непереві- рені веб-сайти (веб-сайти, які не можуть пред’явити сертифікати вста­новленого зразка, що забезпечують безпеку трансакцій);
8. використовуйте захищені сайти, які зазвичай вимагають введення імені користувача та пароля. Пароль має складатись не менш як з восьми символів, ураховуючи букви та числа. І головне, паролем не повинно бути щось очевидне, якісь слова чи дати;
9. не погоджуватись на зустріч із людиною, з якою познайомилися через Інтернет, не надсилати своє фото інтернет-знайомим, не давати незна­йомим людям таку інформацію, як повне ім’я, адреса, номер школи, розклад занять або відомості про родину.

При використанні мережі Wi-Fi в публічних місцях потрібно дотри­муватись таких правил.

1. Відключіть доступ до своїх даних, інакше пристрій та інформація на ньому може стати легкою здобиччю для зловмисників. На комп’ютері під управлінням *Windows* у налаштуванні загального доступу (*Панель управління*/ *Мережа та інтернет)* слід вимкнути спільний доступ до файлів, а також заборонити знаходження комп’ютера іншими корис­тувачами мережі.
2. Використовуйте VPN. Найбезпечніше користуватися громадським Інтернетом через VPN (ця абревіатура розшифровується як *virtualprivatenetwork* — приватна віртуальна мережа). VPN перенаправляє трафік через так звану безпечну мережу, навіть при підключенні до безкоштовного Wi-Fi. VPN буде доречним, якщо часто користуватися незахищеними та публічними мережами. Зробити це можна як безко­штовно, так і з використанням платних, ще більш надійних, сервісів. Останні, наприклад, дозволяють вибирати, через які країни проходи­тиме трафік даних, і вони не обмежують обсяг і швидкість передаван­ня даних.
3. Небажано автоматично підключатися до Wi-Fi мереж. Сучасні но­утбуки, смартфони та планшети вміють автоматично підключатися до відкритих Wi-Fi-точок, проте це може бути небезпечно. Пристрій може «підчепити» мережу, створену зловмисниками спеціально для того, щоб красти інформацію. У більшості сучасних мобільних при­строїв автоматичне підключення до мереж вимкнено за замовчуван­ням, але краще витратити кілька секунд, щоб перевірити це зайвий раз у розділі «Налаштування Wi-Fi».
4. Використовуйте SSL. Багато сайтів використовують криптографічний протокол SSL, що забезпечує обмін даними між сервером та користу­вачами в зашифрованому вигляді. Усе відбувається автоматично, по­трібно тільки в налаштуваннях безпеки браузера поставити галочку навпроти пункту «SSL». Зазвичай цей протокол увімкнений за замов­чуванням, при встановленні браузера.
5. Не нехтуйте двоетапною аутентифікацією (авторизація на сайті). Най­частіше двоетапна аутентифікація зводиться до того, що сайт просить заздалегідь установлений пароль, а також код, надісланий по SMS на введений людиною номер мобільного телефону. Таким чином, якщо хтось вкраде пароль, його одного буде недостатньо для того, щоб ви­користовувати чужий обліковий запис. Двоступенева аутентифікація займає трохи більше часу, що може дратувати (таку схему викорис­товує більшість інтернет-банків. Деколи хочеться її відключити, але часто зробити це неможливо, адже це одна з головних умов авториза­ції на сайті). Важливо підключити подвійну перевірку доступу там, де це можна зробити добровільно, наприклад, у *Google* акаунта, де зв’язані разом пошта, відеохостинг, документи та багато інших сер­вісів, якими користуються мільйони людей. *Google* запропонує ввести номер мобільного й надішле SMS-кою шестизначний код, який буде потрібний для того, щоб зв’язати акаунт із телефоном. Подібний код потрібно буде вводити кожного разу додатково до пароля при спробі увійти в обліковий запис.
6. Уточнюйте назву мережі. Часом шахраї можуть створити мережу для крадіжки даних, яка за назвою схожа на справжню. Наприклад, окрім офіційної мережі THOMSON можна побачити «THOMPSON», що може бути мережею, створеною зловмисником для крадіжки осо­бистих даних та несанкціонованого доступу до мобільного пристрою. Якщо виявлений у кафе Wi-Fi викликає хоч найменший сумнів, по­трібно обов’язково звернутися до працівників закладу й уточнювати в них, як повинна називатися їхня мережа.
7. Захищайте свої паролі. Головне та дуже просте й важливе правило: не встановлювати один і той самий пароль для зареєстрованих на різних сайтах акаунтів. Також важливо не лінуватися та придумувати склад­ні паролі: використовувати цифри упереміш з великими та малень­кими буквами. Якщо паролів багато, то в них можна заплутатися. Для цього можна використати менеджер паролів, на зразок *KeePass*або *LastPass.* Ці програми — безкоштовні, обидві шифрують дані, але роблять це різним чином: *KeePass* зберігає зашифровані дані на комп’ютері, a *LastPass* — на хмарному сервері. У кожного зі способів є свої за і проти, проте загалом обидва сервіси забезпечують високий рівень захисту.
8. Включіть «фаєрвол» (мережевий екран). Деякі операційні системи мають вбудований найпростіший файервол, який відстежує вхідні і вихідні інтернет-з’єднання та не дозволяє проникненню чи надси­ланню з комп’ютера конфіденційних даних. Існує багато програм- фаєрволів — як платних, так і безкоштовних. Фаєрвол не гарантує стовідсоткову безпеку, але це корисна захисна опція, яку варто три­мати включеною. У *Windows* вона включається в секції *Система й безпека (SystemAndSecurity)* у панелі управління.

**Як захистити авторське право в Інтернеті?**

Винахід і швидке й повсюдне поширення Інтернету поставило перед інформаційним співтовариством нові, досить серйозні питання у сфері законодавчого регулювання відносин автора твору та його споживача. Технологічна основа комп’ютерної мережі забезпечує вільне копіювання інформаційного об’єкта будь-якого виду, який розміщено в Інтернеті, з будь-якого комп’ютерного пристрою на будь-який інший комп’ютер або гаджет, які підключені до цієї мережі. Але це не є підставою для пору­шення усталених норм авторського права.

Авторське право в Україні регулюється Цивільним кодексом та За­коном України «Про авторське право та суміжні права». До об’єктів ав­торського права відносять: літературні та художні твори (романи, поеми, статті та інші письмові твори; лекції, промови, проповіді та інші усні тво­ри; драматичні, музично-драматичні твори, пантоміми, хореографічні, інші сценічні твори; інші групи об’єктів); комп’ютерні програми; компіляції даних (бази даних), якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності; інші твори.

Не є об’єктом авторського права: а) повідомлення про новини дня або поточні події, що мають характер звичайної прес-інформації; б) тво­ри народної творчості (фольклор); в) видані органами державної влади в межах їх повноважень офіційні документи політичного, законодавчого, адміністративного характеру (закони, укази, постанови, судові рішення, державні стандарти тощо) та їх офіційні переклади; г) державні символи України, державні нагороди; символи та знаки органів державної влади, Збройних Сил України та інших військових формувань; символіка тери­торіальних громад; символи та знаки підприємств, установ й організа­цій; д) грошові знаки; е) розклади руху транспортних засобів, розклади телерадіопередач, телефонні довідники та інші аналогічні бази даних, що не відповідають критеріям оригінальності й на які поширюється право виі^епегів (своєрідне право, право особливого роду).

Тобто об’єкти авторського право досить різноманітні й напевно, з розвитком культури і суспільства ще будуть з’являться нові об’єкти. Так, з розвитком світової мережі Інтернет з’явилися такі об’єкти, як комп’ютерні програми та компіляції даних.

Відповідно до нещодавно внесених доповнень розміщення твору в оцифрованому вигляді в Інтернет вважається публікацією твору або його поширенням і тому потребує дозволу власника авторського права. Розмі­щення в Інтернет копії твору чи його частини без дозволу автора є пору­шенням Закону й може бути оскаржене в суді з вимогою відшкодування моральної шкоди та завданих матеріальних збитків (упущеної вигоди).

Найпоширенішими видами порушень у мережі Інтернет є: незакон­не відтворення й копіювання музичних, художніх, літературних творів чи комп’ютерних програм без попереднього надання на це згоди автором чи правовласником. Це виражає порушення матеріальних прав авторів. Крім цього, усе популярнішим стає такий вид порушень, як плагіат. Такі дії в мережі Інтернет порушують матеріальні й нематеріальні права авто­рів. Забезпечити захист авторських прав можна такими заходами:

**на етапі до порушення:** 1) обмежена функціональність — автори роз­повсюджують програми, які не здатні друкувати документи або збе­рігати їх у пам’яті комп’ютера; 2) «годинникова бомба» — автор роз­повсюджує повноцінний об’єкт авторського права, але встановлює дату, після якої доступ до нього буде неможливим; 3) захист від копі­ювання, тобто автор установлює кількість разів, коли файл може бути скопійований; 4) криптографічні конверти — твір зашифровано так, що доступ до нього можливий з використанням ключа до шрифту; 5) контракти-угоди «наскрізного клацання», укладені через Інтернет, це — дозволи автора на використання творів; 6) запобіжні заходи: попередня публікація матеріалу на традиційному матеріалі, підтвер­дження факту існування твору на певну дату, засвідчення в нотаріуса дати створення твору, запис на лазерному диску й поміщення в архів або веб-депозитарій; 7) клірингові центри — автор надає центру право ліцензувати свої права на твір, центр приимає плату від користувача й передає її власнику авторських прав;

**на етапі після порушення:** 1) агенти — це комп’ютерні програми, які автоматично виконують попередньо визначені команди, наприклад, пошук у мережі контрафактних примірників творів; 2) стенографія — процес приховування інформації у файлах, наприклад, «водяного знака» автора твору, що буде доказом авторства цієї особи щодо цього твору; 3) «маячок» — це особлива мітка, яка розміщується у творі й спрацьовує під час несанкціонованого використання, надаючи мож­ливість знайти порушника авторських прав; 4) використання кодових слів.

Для перевірки авторства текстів за відповідними базами текстів в Інтернеті можна скористатись програмою виявлення плагіату.

***Практичне завдання.***

Двохфакторнаавторизація - цеспосіб входу до акаунту, при якомупотрібно **крімвведеннялогіну та паролю** виконатипевнудодатковудію, наприклад **ввести код**, отриманий:

* в смс
* на електроннупошту
* в голосовому повідомлення

Також, для дужеважливихакаунтіввикористовуються:

* унікальнізовнішнінакопичувачі
* зчитувачібіометричнихданих

Для переходу до налаштуваньдвохфакторноїавторизаціїможете обрати адресу дляпотрібного для Вас сервісу (звісно ж Ви маєтевже бути в ньомузареєстровані):

***Мета-акаунти:***

[Google](http://accounts.google.com/SmsAuthConfig) - http://accounts.google.com/SmsAuthConfig

[Apple](http://support.apple.com/kb/HT5570?viewlocale=ru_RU) - http://support.apple.com/kb/HT5570?viewlocale=ru\_RU

[Microsoft](https://account.live.com/Proofs/Manage) - https://account.live.com/Proofs/Manage

***Соціальнімережі:***

[Facebook](https://www.facebook.com/settings?tab=security) - https://www.facebook.com/settings?tab=security

[Twitter](https://twitter.com/settings/security) - https://twitter.com/settings/security

[LinkedIn](https://www.linkedin.com/settings/security-v2) - https://www.linkedin.com/settings/security-v2

***Хмарнісховища***

[Dropbox](https://www.dropbox.com/account/security) - https://www.dropbox.com/account/security