**УДК: 004.056.53**

*Корнієнко О.В., студент групи 301 – ТН*

*Полтавський національний технічний університет*

 *імені Юрія Кондратюка*

**ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ. КІБЕРЗЛОЧИННІСТЬ.**

Шкідливе програмне забезпечення (ШПЗ) -  [програмне забезпечення](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F), яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем. Може проявлятися у вигляді [коду](https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%80%D1%86%D0%B5%D0%B2%D0%B8%D0%B9_%D0%BA%D0%BE%D0%B4), [скрипта](https://uk.wikipedia.org/wiki/%D0%A1%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0%22%20%5Co%20%22%D0%A1%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%20%D0%BC%D0%BE%D0%B2%D0%B0), активного контенту, і іншого.

ШПЗ класифікують за декількома факторами, на мою думку, основний з них - це за наявністю матеріальної вигоди. Зараз багато хакерів зламують ігрові аккаунти, такі як Origin чи Steam, які мають ліцензовані комп"ютерні ігри, щоб в подальшому продати їх і таким чином заробити певні кошти, але є і ті , які намагаються зламати важливі сервери організацій, для отримання засекречених даних і визнання інших хакерів.

Звісно, завдяки вірусу-жарту або чогось подібного, багато грошей не заробиш і такі віруси дуже легко виявити та знешкодити за допомогою більшості антивірусних програм. Значно шкідливішими є ті, які не проявляють себе, або важкі в виявленні. Зазвичай це такі як: троянський кінь, руткіт, кейлогер, котрі включають утиліту "замітання слідів". Такі віруси не перешкоджають роботі комп'ютера, а викрадають конфіденційну інформацію, наприклад ваші логіни і паролі. Якщо ви звичайний користувач, і всі паролі, які у вас є - це від "Вконтакті" або "Однокласники", то ви не представляєте ніякої зацікавленості для хакерів, але якщо ви - директор багато-міліонної компанії, або високопоставлена особа і на вашому ПК зберігається велика кількість цінної інформації, то вам необхідно серйозно задуматися про її захист.



Одними із найнебезпечніших програм, є руткіти. Руткіт -  [програма](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0) або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі. Це такий спеціальний модуль ядра, який зламувач встановлює на зламаній ним комп'ютерній системі відразу після отримання прав [суперкористувача](https://uk.wikipedia.org/wiki/Su%22%20%5Co%20%22Su).

Про те, що ваш комп'ютер заразився таким ШПЗ можна не знати декілька років, що і робить його найнебезпечнішим. Зламувач буде вичікувати доки ви не помістите на комп'ютер цінні дані і тільки тоді дасть про себе знать.

Кіберзлочинність - це злочинність у так званому «віртуальному просторі». Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера інформаційний, у якому перебувають відомості про особи, предмети, факти, подіях, явищах і процесах, представлені в математичному, символьному або будь-якому іншому вигляді.

«Кіберзлочинність», «хакери», «комп'ютерний злом», «крадіжка машинного часу» - ці терміни вже перестали бути екзотикою. Проблеми протидії злочинам  у сфері використання комп'ютерної техніки активно обговорюється науковцями, досить швидко розвивається практика застосування відповідних норм законодавства про кримінальну відповідальність.

На сьогодні комп'ютерні злочини - це одна з найдинамічніших груп суспільно небезпечних посягань . Швидко  збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.



Історія навчила нас, що розвиток і прогрес, які приносять людям нові блага та можливості, на жаль, завжди супроводжуються негативними явищами.  Так, і масова комп’ютеризація, і стрімкий розвиток цифрових технологій, які максимально спростили людині всі технологічні та виробничі процеси, полегшили її існування та перевернули уявлення про роботу, кар’єру, дозвілля, фінанси і навіть особисте життя, приховують у собі серйозні небезпеки. Я хочу розповісти про одну з найактуальніших.

Сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій. Сьогодні комп'ютери впроваджуються в різноманітні галузі людської діяльності. Усі найважливіші функції сучасного суспільства, так чи інакше, пов’язані з комп'ютерами, комп'ютерними мережами і комп'ютерною інформацією. Останнім часом в світі значно зросла кількість Інтернет користувачів, адже підключення до глобальної мережі стало доступним та зручним. Для багатьох людей інтернет став цілим світом, віртуальним світом. Як і в реальному світі, так і в віртуальному, де панує комп’ютерна інформація, трапляються, злочини, кіберзлочини.

Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем - це далеко не повний перелік подібних злочинів.

Такі злочини характеризуються наступними особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказу в суді подібних справ, транснаціональною складовою в основному з використанням інформаційної мережі Інтернет, високим збитком навіть від одиничного злочину. За деякими оцінками, через кіберзлочинців щорічно світова економіка втрачає $ 114 млрд, повідомляє РБК.

Криміналістична особливість кіберзлочинів заключається в тому, що розслідування та розкриття цих злочинів неможливе без застосування та використання комп’ютерних технологій. Це пов’язано з необхідністю відшукування, фіксування, вилучення та збирання доказів в електронній формі. Також комп’ютерні технології широко використовуються для проведення оперативно-розшукових заходів.

Першою причиною розвитку кіберзлочинності, як і будь-якого бізнесу, є прибутковість, – вона неймовірно прибуткова. Величезні суми грошей з'являються в кишенях злочинців у результаті окремих великих афер, не говорячи вже про невеликі суми, які йдуть просто потоком. Друга причина росту кіберзлочинності як бізнесу - те, що успіх справи не пов'язаний з більшим ризиком. У реальному світі психологічний аспект злочину припускає наявність деяких коштів стримування. У віртуальному світі злочинці не можуть бачити своїх жертв, будь то окремі люди або цілі організації, які вони вибрали для атаки. Грабувати тих, кого ти не бачиш, до кого не можеш дотягтися рукою, набагато легше.