Етико-правова відповідальність спеціаліста ІТ та основні моральні принципи в контексті неправомірного доступу до комп'ютерної інформації (створення, використання і поширення шкідливих програм для комп'ютерів; порушень правил експлуатації комп'ютерів, комп'ютерних систем або мереж і ін.)

Це питання можна зрозуміти двома чинами: з одного боку, як питання щодо неправомірного доступу до особистих даних користувачів, з іншого боку, щодо порушення правил доступу до інтелектуальної власності. Розглянемо перший варіант, оскільки другий варіант належить до ширшого кола питань про інтелектуальну власність (де важливі не тільки доступ до даних чи експлуатація пропрієтарних систем, а ще й розповсюдження цих даних або коду, та інше).

Важливим правовим регламентом щодо захисту персональних даних є GDPR (General Data Protection Regulation). Вважається, що цей регламент найбільш строго захищає особисті дані, і не зважаючи на те що він діє лише в межах ЄС, майже всі глобальні ІТ-компанії мають враховувати ці правила, аби обслуговувати користувачів з ЄС.

Зазвичай GDPR асоціюють не з технічним захистом персональних даних, а з мінімізацією збору даних *(зокрема питаннями "Do you consent to storing cookies?")*. Але насправді, по-перше, GDPR таки зобов'язує спеціалістів використовувати "відповідні технічні та організаційні методи" для забезпечення захисту даних "by design and by default" (Article 25). По-друге, мінімізація збору даних сама по собі є важливою частиною захисту ІТ-систем: кіберзлочинець не може отримати доступу до даних, які компанія взагалі ніколи не збирала.

Існує ціла сфера етики під назвою "data ethics" (етика даних). Дослідники цієї галузі зазвичай цікавляться big data, проте можна відокремити з цього деякі принципи, важливі саме для нашого питання (неправомірний доступ до комп'ютерної інформації):

1. Власність даних: особисті дані користувача належать користувачу, а не компанії.

2. Прозорість: користувачі мають право знати, які їх дані зберігаються і для чого використовуються
3. Приватність: запобігання зберігання PII (personally identifiable information) якщо для цього немає крайньої потреби

Зокрема принцип прозорості зобов’язує компанії сповіщати користувачів про data breaches (“витоки даних”), тобто кібератаки, в наслідок яких отримано неправомірний доступ до даних користувачів. З правової точки зору, такі закони як GDPR, а також різні відповідні закони США, вимагають сповіщення таких інцидентів: зокрема публічне сповіщення, а в деяких випадках також сповіщення окремих державних органів або команд експертів, за принципом full disclosure. Новини про витоки даних зазвичай публікуються в мас-медіа, що негативно впливає на репутацію компанії та її фінансове становище (не кажучи про можливі штрафи за порушення регламентацій GDPR та ін.)

Також коротко можна зазначити цікавість балансу між 1) захистом комп’ютерної системи від шкідливих програм та неправомірного доступу та 2) свободою користувача щодо запуску програм з різноманітним функціоналом на власному пристрої. Чітким прикладом є явна обмеженість системи Android, де користувачу взагалі не надається прямий доступ до виконуваних файлів APK та даних додатків — проте це вважається етично виправданим, бо значно ускладнює створення шкідливим програм типу ransomware та ін. З іншого боку платформа Windows надає будь-якій програмі доступ до даних будь-якої іншої програми (за окремими винятками), що збільшує свободу користувача (наприклад, можна встановити модифікацію для якоїсь відео-гри), але й ставить його під ризик вкрадення даних та ін.

Основні проблеми авторського права та захист інтелектуальної власності у мережі: вітчизняний та зарубіжний досвід (етичний та соціально-правові аспекти). Навести приклади.

Це питання можна вважати другою половиною загального питання про захист даних.

На відміну від попереднього питання, де несанкціонований доступ до даних приносить безпосередню шкоду користувачам, тут шкода задіюється до видавців, продюсерів, розробників тощо.

Можна вважати, що деяку непряму шкоду отримують і споживачі, оскільки піратство призводить до зниження прибутку розробників, а це призводить до зниження якості/кількості вироблених товарів. За даними різних американських досліджень від 50% до 70% “піратів” вважають, що ця справа шкодить суспільству, проте продовжують порушувати авторські права.

Соціально-правовий аспект вирішення цієї проблеми полягає у впливах двох типів: “негативних”, які спонукають користувачів уникати піратства, та “позитивних”, які спонукають до легального використання даних.

Прикладом негативного впливу може слугувати Закон України «Про авторське право і суміжні права», а саме його оновлена версія, що діє з 1 січня 2023 р.. Зокрема цей закон посилює відповідальність за порушення авторського права не тільки у вигляді розповсюдження, а також і споживання піратського контенту (штрафи від 850 до 5000 грн).

Прикладом позитивного впливу є більш висока надійність та, якщо вірити засновнику Steam Гейбу Ньюеллу, питання зручності сервісу. Для завантаження гри в Steam необов’язково сканувати гру антивірусом (бо ліцензійні відео-ігри, на відміну від піратських, не можуть містити шкідливе ПО), знаходити torrent-трекер, встановлювати torrent-клієнт, маскувати свою IP-адресу тощо.

Поняття “зручності” легального споживання контенту можна розширити до поняття “доступності”, до якого входить не тільки “ціна” в плані витрати часу та зусиль на використання (не-)зручного сервісу, а й власне ціна товару. Зрозуміло, чому піратство значно більш поширене в країнах, що розвиваються.

Тим часом в розвинених країнах все більшу роль відіграють певні моральні цінності, які протистоять поняттю інтелектуальної власності, а власне: право на презервацію даних, як суспільна відповідальність до наступних поколінь; і права та свободи споживачів, якій може шкодити захист авторських прав.

Постають питання щодо технологій DRM (digital rights management), які запобігають використанню програм без авторизації від розробника/видавця. Що робити, якщо видавець став банкрутом, і не може надати авторизацію?

Суперечним питанням є і сама імплементація DRM, яка, з ціллю запобігти неавторизованому використанню ПО, може використовувати технічні засоби, що приносять пряму шкоду споживачу. Прикладом є технологія DRM StarForce, яка встановлює власний CD-ROM драйвер, який виконує перевірку автентичності диску гри; проте в деяких версіях StarForce цей драйвер не видалявся після видалення гри, а сам драйвер міг бути несумісним з деякими CD-ROM reader-ами, спричиняючи сповільнення чи збої гри тощо. В 2006 році це призвело до подання в суду видавця ігор Ubisoft, з вимаганням відшкодування споживачам 5 мільйонів доларів, хоча справу було відкинуто по причині недостатньої кількості доказів.