ПРОТИДІЯ ЗЛОЧИННОСТІ: ПРОБЛЕМИ ТЕОРІЇ ТА ПРАКТИКИ

УДК 343.533(477)

Джужа О. М. – доктор юридичних наук, професор, головний науковий співробітник відділу організації науково-дослідної роботи Національної академії внутрішніх справ, м. Київ;

ORCID 0000-0003-1347-4937

Топчій В. В. – кандидат юридичних наук, прокурор відділу прокуратури Київської області, м. Київ

Проблеми забезпечення охорони інтелектуальної власності в Україні

Розглянуто нагальні проблеми безпеки та захисту інтелектуальної власності в державі. У сучасному суспільстві зростає потреба в захисті комерційної інформації, оскільки промисловий шпіонаж став поширеним явищем і в нашій країні. Конкурентоспроможність безпосередньо залежить від здатності захистити свою ділову й технологічну інформацію від викрадання, несанкціонованого використання, зміни або знищення.

Високим є рівень розвитку електронних банківських та інших систем. Попри це, втрати від так званих комп'ютерних злочинів, промислового шпигунства та крадіжок комерційних таємниць, обсяг яких протягом двох останніх десятиліть подвоївся, завдають багатомільярдних збитків.

Сформульовано загальні вимоги до організації захисту інформації, що опрацьовують засобами електронно-обчислювальної техніки. Вони передбачають системний аналіз загроз безпеки інформації; комплексне використання засобів захисту; економічну ефективність системи захисту та її безперервність.

Основну частину системи захисту становлять правові (законодавчі, адміністративні, або організаційні) і фізичні заходи захисту. Кожна зі складових доповнює іншу, а недосконаліть однієї з них може призвести до порушення формування й функціонування системи загалом. Для забезпечення її ефективності постає потреба залучення досвідчених фахівців у сфері безпеки.

Для охорони обладнання та носіїв інформації від прямого розкрадання або знищення нерідко вдаються до заходів фізичного захисту. Це різні механічні, електромеханічні й електронні пристрої охорони будівлі та охоронної сигналізації. Фізичні заходи захисту зазвичай застосовують у сукупності з адміністративними заходами.

Важлива для фірми інформація переважно задокументована, тому контроль за документацією – одна з відповідальних ланок системи безпеки.

До технічних заходів захисту належить використання різноманітних механічних, електромеханічних, електронних, оптичних, радіолокаційних та інших пристроїв і систем, які здатні самостійно або в сукупності з іншими засобами виконувати функції захисту інформації. Вони доповнюють фізичні й адміністративні заходи, дають змогу істотно підвищити їхню ефективність.

Морально-етичні норми у сфері захисту інформації – це норми поведінки, які склалися в колективі фахівців конкретної комерційної структури та які не є обов'язковими, як, наприклад, законодавчі норми, проте їх недотримання призводить до втрати авторитету (іміджу) особи, групи фахівців, усієї організації.

Досвід промислово розвинутих країн засвідчує, що найефективніші заходи запобігання кіберзлочинності – це посилення законодавчої складової, взаємодія правоохоронних органів і підрозділів, а також активна співпраця з комерційними службами приватних фірм в Україні.

Ключові слова: інтелектуальна власність; безпека інтелектуальної власності; електронно-обчислювальні машини; локальні обчислювальні мережі; комп'ютерний злочин; програмне забезпечення; прогнозування; захист інформації; авторське право; комерційна таємниця; технічні засоби системи охорони; криптографічні заходи.

Постановка проблеми. Унаслідок переходу від індустріального суспільства до інформаційного інформація стає дедалі важливішим ресурсом, порівняно з матеріальними чи енергетичними. Продукування й обіг інформації стали головним вектором розвитку економіки [1].

Сучасні комерційні структури створюють спеціально для експлуатації нових технологічних досягнень. Держава заохочує таку господарську діяльність, виділяючи кредити для її фінансування [2, с. 81; 3].

Успішно здійснювати виробництво в умовах жорсткої конкуренції можна лише шляхом упровадження нових ідей, які сприяють підвищенню ефективності виробничих витрат.

Рівень конкурентоспроможності безпосередньо залежить від уміння захищати свою ділову і технологічну інформацію від розкрадань, несанкціонованого використання, зміни або знищення. Якщо апаратуру доводиться купувати, то програмне забезпечення може бути не тільки куплено, а й скопійовано. Отже, цей вид інтелектуальної власності потребує посиленого захисту.

У США, наприклад, де функціонують десятки мільйонів ЕОМ, для управління потоками інформації та передання даних використовують локальні обчислювальні мережі, географічно розподілені бази даних, розгалужену мережу телефонного, телексного та факсимільного зв'язку, зокрема через штучні супутники Землі. Високим є рівень розвитку електронних банківських та інших систем. Попри це втрати від так званих

комп'ютерних злочинів [4, с. 50–56], промислового шпигунства та крадіжок комерційних таємниць, обсяг яких протягом двох останніх десятиліть подвоївся, завдають багатомільярдних збитків.

Аналіз останніх досліджень і публікацій. Інтелектуальну власність у широкому значенні слід визначити як цінні комерційні ідеї. Вони можуть стосуватися способу управління виробництвом, хімічної формули, технічного процесу, списку клієнтів, аналізу конкурентоспроможності тощо.

Уперше поняття «інтелектуальна власність» використано 1967 року на Стокгольмській конференції, під час якої створено Всесвітню організацію інтелектуальної власності, до якої приєдналася й Україна.

У сфері охорони інтелектуальної власності в нашій державі допущено низку прорахунків. Зокрема, на виробництво значної кількості лікарських препаратів, розроблених на українських теренах, нині доводиться купувати патенти за кордоном. Японські бізнесмени офіційно подякували журналу «Зроби сам», адже, використовуючи креслення, розміщені в цьому виданні, вони заробили мільйонні статки. Таких прикладів безліч.

Нині вже стало очевидним, що процвітання низки фірм і підприємств ґрунтується на присвоєнні інтелектуальної власності тих установ та інститутів, де нещодавно працювали їхні співробітники. Нерідко для швидкого збагачення таку інформацію продають за кордон. Зарубіжний досвід засвідчує: хто не піклується про безпеку своєї інтелектуальної власності – втрачає до 35–40 % можливого прибутку [5].

Нові ідеї – специфічний товар, що має комерційну вартість. На відміну від матеріальних речей, які постійно мають вартість, скільки разів їх не виробляли б, вартість ідей одноразова (ніхто не буде платити гроші за вже відому інформацію).

Розрізняють два види інтелектуальної власності:

1) промислову інформацію (науково-технічну, технологічну тощо);

2) комерційну інформацію (ділову, фінансову, кредитну тощо).

Кожній із них притаманні певні особливості в способах використання та захисту.

До промислової інформації, яка потребує захисту, належать відкриття, винаходи, методи виробництва, технологія, дизайн. Таємницею фірми може стати хімічна формула будь-якої

речовини (наприклад, як у корпорацій «Кока-Кола» і «Пепсі»). Промислову інформацію становлять:

– конструкторська документація (опис, схеми, креслення) виконаних науково-дослідних, дослідно-конструкторських та інших робіт;

– інформація про наукові винаходи, патенти на стадіях їх розроблення й оформлення;

– програмне забезпечення електронно-обчислювальних машин [6, с. 270];

– електронна схема будь-якого пристрою;

– процес виробництва тканини;

– рецепт виготовлення ліків;

– рецепт приготування страв тощо [7].

На відміну від промислової інформації, сфера застосування комерційної інформації не надто широка. Комерційна інформація допомагає вирішити два питання: як планувати отримання грошей і як їх отримувати. Її предметом можуть бути всі властиві підприємству або діловій людині особливості, індивідуальні деталі комерційної діяльності, ділові зв'язки місця закупівлі сировини й товарів, відомості про постачальників, про передбачуваний прибуток, методи встановлення цін. Володіння такою інформацією надає можливість фірмам успішно конкурувати між собою.

Прикладом комерційної інформації можна вважати:

– відомості про укладені контракти (договори, угоди) або пропозиції щодо їх укладання;

– інформацію про кредити та різноманітні банківські операції;

– плани збуту продукції;

– аналіз конкурентоспроможності;

– систему заходів маркетингу;

– ділове листування;

– бухгалтерські та фінансові звіти;

– заробітну плату співробітників фірми;

– список клієнтів фірми;

– інформацію особистого (приватного) змісту, яку може бути використано проти особи.

Збереження в таємниці цієї інформації від сторонніх осіб, крім податкових і фінансових служб, є обов'язковою умовою для утримання досягнутих у конкурентній боротьбі позицій.

Необхідність захисту такої інформації також зумовлена високим рівнем небезпеки, пов'язаної з рекетом.

Виклад основного матеріалу. Якщо на підставі аналізу доходять висновку, що певна інформація потребує захисту (постійного чи тимчасового), слід негайно розробити програму щодо його забезпечення з метою:

1) запобігання або значного ускладнення розкрадання таємниць фірми;

2) доведення до відома всіх співробітників фірми інформації про важливість таємниць і заходи покарання за їх розголошення.

Зарубіжний досвід у сфері захисту інтелектуальної власності й вітчизняна практика захисту державної таємниці засвідчують, що ефективною може бути лише комплексна система захисту, яка комбінує такі заходи:

1) програмні (застосування спеціальних програм для захисту інформації);

2) законодавчі (використання законодавчих актів, які регулюють питання захисту інтелектуальної власності);

3) морально-етичні (дотримання правил поведінки, що склалися в колективі, порушення яких призводить до втрати авторитету);

4) адміністративні (організація режиму секретності, пропускного та внутрішнього режиму тощо [8, с. 98–99];

5) технічні (застосування електронних та інших пристроїв для захисту інформації);

6) фізичні (створення перешкод для доступу до охоронюваного обладнання й інформації);

7) криптографічні (шифрування інформації).

Не всі компоненти окресленої системи захисту рівноцінні. Здебільшого основну її частину становлять правові (законодавчі, адміністративні, або організаційні) і фізичні заходи захисту. Однак кожна зі складових доповнює іншу, а недосконаліть однієї з них може призвести до порушення формування й функціонування системи захисту. Для забезпечення її ефективності постає потреба залучення досвідчених фахівців у сфері безпеки.

В умовах сьогодення законодавчі заходи можуть захистити тільки науково-промислову інформацію (причому не завжди), а також інформацію у сфері культури й мистецтва (літературні, художні, музичні твори). Для захисту комерційної інформації

застосування законодавчих заходів суттєво ускладнено, тому важливого значення набувають інші системи захисту.

Морально-етичні норми у сфері захисту інформації – це правила поведінки, які склалися в колективі фахівців конкретної комерційної структури та які не є обов'язковими, як, наприклад, законодавчі норми, проте їх недотримання призводить до втрати авторитету (іміджу) особи, групи фахівців, усієї організації. Ці норми можуть бути як неписані (загальноприйняті норми чесності, порядності, патріотизму), так й оформлені у вигляді статуту або відповідних приписів (наприклад, Кодекс професійної поведінки членів Асоціації користувачів електронно-обчислювальних машин США).

Для охорони обладнання та носіїв інформації від прямого розкрадання або знищення нерідко вдаються до заходів фізичного захисту. Це різні механічні, електромеханічні й електронні пристрої охорони будівлі та охоронної сигналізації.

Уживаючи заходів для захисту від несанкціонованого доступу до інформації, не слід прагнути забезпечити захист будівлі цілком, адже це потребує значних затрат і подальших зусиль для здійснення контролю. Доцільно визначити ті місця, у яких необхідно встановити камери прихованого спостереження. За наявності можливості слід територіально відокремити служби, у яких продукують нову інформацію. Для роботи з таємною інформацією мають функціонувати спеціальні ізольовані приміщення, доступ до яких дозволено тільки певним особам.

Фізичні заходи захисту, зазвичай, застосовують у сукупності з адміністративними заходами. До основних груп адміністративних заходів належать: організація відповідного режиму, створення служби безпеки, навчання й інструктаж персоналу тощо. Передусім необхідно визначити найважливіші ділянки й обмежити до них доступ. Доцільно використовувати такі сучасні засоби, як магнітні картки й інші складні системи.

Оскільки важлива для фірми інформація переважно задокументована, контроль за документацією – одна з відповідальних ланок системи безпеки. Документи конфіденційного змісту підлягають ретельному контролю, а значні обсяги нетаємної інформації, сформовані за певною ознакою, також слід контролювати, оскільки саме в сукупності вони набувають цінності.

Створенню системи захисту інформації фірми має передувати вивчення процесу складання циркуляції, зберігання та знищення документів.

Цікавим є досвід зарубіжних фірм, які для обмеження фотокопіювання конфіденційних документів випускають їх оригінали на спеціально пофарбованому папері чи папері, який під час копіювання на ксероксі відтворює інформацію з попередженням, що це копія.

Перевірка (цензура) документів, призначених для публікації, також має важливе значення. Це стосується наукових статей, брошур, прес-релізів і матеріалів, поширюваних на торговельних виставках.

Співробітники фірми завжди є основним каналом витоку інформації. Здебільшого зазначене спричинено їхньою неграмотністю у сфері захисту інформації. Тому в процесі роботи слід навчати персонал належно захищати інтелектуальну власність.

Фахівці радять здійснювати добір кандидатів для роботи у фірмі, ураховуючи вимоги щодо захисту інтелектуальної власності, перевіряти їх благонадійність принаймні шляхом отримання рекомендацій від організацій чи осіб.

Доцільно зобов'язати нового працівника підписати документ про нерозголошення комерційної таємниці фірми. Захист комерційної таємниці залежить від рівня довіри між керівником і співробітниками, тому доцільно такі взаємини обумовлювати положеннями контракту, що передбачає зобов'язання про нерозголошення.

Будь-яка виробнича або комерційна структура має певну специфіку, проте є загальні принципи захисту комерційної таємниці, з-поміж яких – дрібнення комерційної таємниці на окремі елементи. За таких умов повною інформацією володіє обмежене коло співробітників, на яких можна цілком покладатися.

Принципом захисту комерційної таємниці є постійний контроль за найважливішою інформацією. Власну таємну інформацію можна поширювати тільки через контрольовані канали. Періодичного контролю потребує і програма захисту документації.

Важливою складовою безпеки є контроль за відвідувачами установи (офісу).

Групою ризику є співробітники, які здійснюють збут продукції фірми. Вони не повинні володіти інформацією про нові розробки,

які ще не надійшли у виробництво. Із цією метою необхідно не допускати їхніх тісних зв'язків із дизайнерами й інженерами. Слід посилювати заходи захисту під час проведення виставок, ярмарків, демонстрацій продукції.

Під час навчання слід акцентувати увагу персоналу на таких аспектах:

– сутність виробничої та комерційної інформації фірми;

– наявність реальної загрози для цієї інформації;

– методи захисту інформації;

– конкретні зобов'язання кожного співробітника щодо захисту комерційної таємниці.

Навчання співробітників мають проводити фахівці або спеціальні центри підготовки. Чимало іноземних фірм обрали захист інформації основним профілем своєї діяльності.

До технічних заходів захисту належить використання різноманітних механічних, електромеханічних, електронних, оптичних, радіолокаційних та інших пристроїв і систем, які здатні самостійно або в сукупності з іншими засобами виконувати функції захисту інформації. Вони доповнюють фізичні й адміністративні заходи, дають змогу істотно підвищити їхню ефективність.

Технічні засоби призначені автоматизувати охорону приміщення фірми. Без встановлення заборон на використання апаратури опрацювання інформації не можна суттєво знизити або цілком запобігти можливості витоку даних через побічні канали.

Технічні системи охорони містять засоби охоронного освітлення, виявлення, спостереження, сигналізації тощо.

Найпоширенішими є такі технічні засоби й системи охорони:

– акустичні (вібраційні), які надають можливість виявити порушника за вібраціями, створеними внаслідок його дій;

– електромеханічні, принцип дії яких полягає в замиканні або розмиканні електронних ланцюгів чутливих елементів у разі несанкціонованого відкривання дверей, вікон тощо;

– оптичні, які змінюють параметри спеціально створеного оптичного випромінювання ультрафіолетового, видимого й інфрачервоного діапазону для хвиль у разі потрапляння в зону його поширення сторонніх предметів;

– радіотехнічні, параметри електромагнітного випромінювання високої частоти яких у разі появи в його зоні сторонніх об'єктів змінюються;

– магнітометричні, що реагують на наближення до них зміною параметрів магнітного поля;

– ємнісні (індуктивні), що спрацьовують шляхом зміни ємності (індуктивності) чутливих елементів у момент наближення до них людини або сторонніх предметів, транспортних засобів.

Криптографічні засоби захисту інформації дають змогу шифрувати інформацію, щоб її зміст був доступним тільки за умови пред'явлення специфічної інформації (ключа). Фахівці вважають криптографічні закриті інформації найефективнішим і найнадійнішим засобом її захисту.

Значна кількість сучасних іноземних фірм спеціалізується на розробленні апаратури криптографічного захисту інформації. Вони виготовляють і постачають апаратуру, програмне забезпечення, консультують керівників та фахівців фірм з питань захисту тощо. Саме тому проблема збереження комерційної таємниці, яку опрацьовують за допомогою обчислювальної техніки, стає дедалі актуальнішою. По-перше, повсякчас зростає обсяг інформації, яка потребує захисту. По-друге, унаслідок того, що інформацію опрацьовують і зберігають на ЕОМ, вона стає доступною значній кількості людей. По-третє, забезпечення закритості такої інформації вимагає складних процедур і матеріальних затрат.

Активне застосування обчислювальної техніки спричинило формування нової сфери злочинної діяльності – комп'ютерної злочинності. Шкоду від комп'ютерних злочинів обчислюють відсотками національного валового продукту, а протидію їм здійснюють на рівні законодавчих положень.

Висновки. Отже, у цій статті сформульовано загальні вимоги до організації захисту інформації, що опрацьовують засобами електронно-обчислювальної техніки. Вони передбачають системний аналіз загроз безпеки інформації; комплексне використання засобів захисту; економічну ефективність системи захисту та її безперервність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Попередження та викриття злочинів у сфері економіки підрозділами Державної служби боротьби з економічною злочинністю МВС України : навч. посіб. / [Л. П. Скалозуб, М. Г. Вербенський, В. І. Василинчук та ін.] ; за ред. О. М. Джужі. – Київ : РВВ МВС України, 2011. – 520 с.

2. Законодавче забезпечення протидії злочинам у сфері економіки в діяльності підрозділів Державної служби боротьби з економічною злочинністю : зб. підзакон. нормат. актів / [упор.: Л. П. Скалозуб, В. І. Василинчук]. – Київ : ЗУКЦ, 2008. – 258 с.

3. Збірник методичних рекомендацій з документування та викриття злочинів у пріоритетних напрямах та галузях економіки : у 2 ч. / [Л. П. Скалозуб,

В. І. Василинчук, В. Д. Сапсай та ін.] ; за ред. О. М. Джужі. – Київ : Друкарня МВС України, 2008. – Ч. 2. – 512 с.

4. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.] ; за заг. ред. В. В. Коваленка. – Київ : Скіф, 2012. – 728 с.

5. Субъективная-Приказчикова А. Конец эры Audio CD / А. Субъективная-Приказчикова // Upgrade. – № 6. – С. 2–3.

6. Криминология : учебник / под ред. Ю. Ф. Кваши. – Ростов н/Д : Феникс, 2002. – 704 с.

7. Roshen судится из-за «Киевского торта» // Вести. – 2018. – 2 февр. – С. 4.

8. Михальський О. О. Історико-правовий аналіз протидії правопорушенням у сфері інтелектуальної власності / О. О. Михальський // Науковий вісник публічного та приватного права. – 2016. – Ч. 2. – С. 98–103.

REFERENCES

1. Skalozub, L.P., Verbenskyi, M.H., & Vasylynchuk, V.I. (et al.). (2011). *Poperedzhennia ta vykryttia zlochyniv u sferi ekonomiky pidrozdilamy Derzhavnoi sluzhby borotby z ekonomichnoiu zlochynnistiu MVS Ukrainy [Prevention and disclosure of crimes in the field of economy by the units of the State Service for Combating Economic Crime of the Ministry of Internal Affairs of Ukraine].* O.M. Dzhuzha (Eds.). Kyiv: RVV MVS Ukrainy [in Ukrainian].

2. Skalozub, L.P., & Vasylynchuk, V.I. (2008). *Zakonodavche zabezpechennia protydii zlochynam u sferi ekonomiky v diialnosti pidrozdiliv Derzhavnoi sluzhby borotby z ekonomichnoiu zlochynnistiu [Legislative support for counteraction to economic crimes in the activities of the units of the State Service for Combating Economic Crime].* Kyiv: ZUKTs [in Ukrainian].

3. Skalozub, L.P., Vasylynchuk, V.I., & Sapsai, V.D. (2008). *Zbirnyk metodychnykh rekomendatsii z dokumentuvannia ta vykryttia zlochyniv u priorytetnykh napriamakh ta haluziakh ekonomiky [Collection of methodical recommendations on documenting and revealing crimes in priority directions and branches of economy].* O.M. Dzhuzha (Eds.). (Vols. 1-2). Kyiv: Drukarnia MVS Ukrainy [in Ukrainian].

4. Korystin, O.Ye., Butuzov, V.M., & Vasylevych, V.V. (et al.). (2012). *Protydiia kiberzlochynnosti v Ukraini: pravovi ta orhanizatsiini zasady [Countering cybercrime in Ukraine: legal and organizational principles].* V.V. Kovalenko (Eds.). Kyiv: Skif [in Ukrainian].

5. Subektivnaia-Prikazchikova, A. Konec ery Audio CD [End of the Audio CD era]. *Upgrade, 6,* 2-3 [in Russian].

6. Kvasha, Yu.F. (Ed.). (2002). *Kriminologiia [Criminology].* Rostov n/D: Feniks [in Russian].

7. Roshen sudica iz-za "Kievskogo torta" [Roshen sues because of the "Kiev cake"]. *Vesti, Vesti* [in Russian].

8. Mykhalskyi, O.O. (2016). Istoryko-pravovyi analiz protydii pravoporushenniam u sferi intelektualnoi vlasnosti [Historical and legal analysis of counteraction to an offense in the field of intellectual property]. *Naukovyi visnyk publichnoho ta pryvatnoho prava, Scientific Bulletin of Public and Private Law, 2,* 98-103 [in Ukrainian].

Стаття надійшла до редколегії 15.02.2018

Dzhuzha O. *– Doctor of Law, Professor, Chief Research Fellow of the Scientific and Research Work Unit of the National Academy of Internal Affairs, Kyiv, Ukraine;*

ORCID 0000-0003-1347-4937

Topchii V. *– Ph.D in Law, Prosecutor of the Prosecutor's Office Kiev Region, Kyiv, Ukraine*

The Problems of Intellectual Property Security in Ukraine

The article deals with the urgent problems of security and protection of intellectual property in the state. In today's society, there is a growing need for the protection of commercial information, as industrial espionage has laid deep roots in our country as well. The experience of industrialized countries suggests that the most effective measures to prevent cybercrime are the strengthening of the legislative component, the interaction of law enforcement agencies and units, as well as active cooperation with commercial services of private firms in Ukraine.

Successfully engage in production, and even survive in a fierce competition is possible only by acquiring and exploiting new ideas that contribute to increasing the efficiency of production costs.

The level of competitiveness to a large extent depends on the ability to protect its business and technological information from theft, unauthorized use, alteration or destruction.

And if you need to buy the hardware, then the software can be not only bought, but also copied easily. Consequently, this kind of intellectual property is subject to reliable protection.

When taking measures to protect against unauthorized access to information, one should not seek to protect the entire building, as it requires too much money and effort for further control. It is advisable to identify the places where you need to install hidden surveillance cameras. Where it is possible to separate geographically the services in which new information is generated, for example, research departments, laboratories. To work with classified information should be allocated special insulated premises, access to which is allowed only to certain persons.

An important role in protecting information is played by moral and ethical standards. They usually include the rules of conduct that have developed in a team of specialists of a particular commercial structure and which are not mandatory, such as legislative norms,

but their non-compliance leads to the loss of authority (image) of a person, group of experts, the entire organization. These norms may appear as unwritten (generally accepted norms of honesty, decency, patriotism), and are formalized in the form of a charter or corresponding regulations.

The selection, training and organization of the work of the personnel is important. Experts advise to select the candidates for work in the firm, taking into account the requirements of protection of intellectual property, to check their reliability, at least by obtaining recommendations from known organizations or individuals.

Keywords: intellectual property; intellectual property security; electronic computers; local computer networks; computer crime; software; forecasting; information protection; copyright; commercial secrets; technical means of security systems; cryptographic come on.