*Лекція № **5***
ТЕЗИ

Інтелектуальна власність та ліцензування програмного забезпечення. Тенденції ринку: пропрієтарне прогамне забезпечення та програмне забезпечення з відкитими вихідними кодами (open-source software).

Якщо на минулих лекціях ми говорили спершу про важливість IT стратегії, далі про те ЯК саме повинна організовуватися (на процесному а не функціональному підході), то тепер і надалі говоритимемо про інструментальні засоби і різні практичні аспекти організації IT-інфраструктури на підприємстві.

Інтелектуальна власність

Інтелектуальна власність (ІВ) — це право на нематеріальну власність.
Включає законне право на відсторонення інших від володіння нею (як і матеріальна вл.).

ІВ може бути дуже цінною.
ІВ захищає результати розумової праці.

ІВ поділяють на кілька великих форм. Найпоширеніші:
- ***патент*** (захищає винахідницькі ідеї, які впроваджені на практиці, напр. комп. миш)
- ***авторське право*** (захицає оригінальні "витвори", опубліковані і доступні для сприйняття людиною (книги, програми, музичні твори і т.п.))
- ***професійний секрет*** (захищає комерційну і іншу цінну інформацію, не відому широкому загалу, напр. ????)
- ***торгова марка*** (захищає символіку, під якою розповсюджується товар чи послуга, напр. "Світоч")

Міліарди доларів кожен рік інвестуються в дослідження і розробки.
Середня ціна ІВ є як правло малою, однак окремі екземпляри ІВ можуть коштувати мільйони.
ІВ на сьогоднішній день стала центральним моментом (рушієм) економічного розвитку.

За захист ІВ відповідає **держава** і її уряд. Кожна держава законодавчо регулює права на ІВ по-своєму, однак зараз велике значення також мають міжнародні договори.

Захист ІВ залежить від її форми:
Патент видається в обмін на його розкриття, авторське право — в обмін на публікацію.
Таким чином суспільство отримує вигоду від **розкриття**.
Знайомитися з патентом може кожен, однак використовувати, тільки той, хто оплатив права на використання патенту.
Термін дії патенту і авт. прав як правило обмежується.
Проф секрет не розкривається за означенням. Одну і ту ж інформацію (теоретично) можуть вважати своїм проф секретом різні організації чи навіть сфери діяльності.
Термін дії проф. секрету не обмежений.

Захист торгових марок має дві цілі: захист споживача а також захист інвестицій власника торг. марки.

Патенти бувають різних типів. Чотири головних: патенти на
- корисність (найпоширеніший і як правило найцінніший — напр. додавання коліщатка в комп. миш підлягає патентуванню, а додаткової клавіші - ні)
- дизайн (захищає нефункціональні особливості пристрою, напр. патент на дизайн ергономічної миші, що повторює вигин долоні)
- процес
- рослини

Загальний міжнародний термін дії патентів — 20 років.
В більшості країн існують спеціальні інституції для видачі патентів.
Різною є також процедура розрішення конфліктів: в одних країнах патент видають тому, хто перший подав заявку, в інших — тому, хто зробив винахід.

Права власника патенту теж відрізняються від країни до країни.

Патенти часто об'єднують в патентні пули (пакети). Напр. патент на коліщатко для миші логічно об'єднати з патентом на миш.

Патенти можуть стврювати економічні монополії і тут виникають питання відсутності конкуренції, що теж регулюється законами.

Авторське право не вимагає часто жодних додаткових дій від автора. В більшості країн автор набуває його автоматично, якщо це не оговорено з його працедавцем(видавцем, продюсером і т.п.) додатковими угодами (які теж можуть не мати чинності згідно місцевого законодавства).
Іншими словами авторське право установлюється законодавчо або контрактно (з використанням ліцензій)

Історія авторського права — це в певному сенсі історія технологій: напр. ще зовсім недавно не визнавалось авторське право на бази даних, напр. зараз стоїть питання про визнання авторського права на запахи (парфуми).

Час дії автрського права в більшості країн рівний часу життя автора + 70 років після його смерті.

Проф. Секрет не є ексклюзивним.
Держава його як правило спеціально не захищає — як правило закони про його захист є загальними законами про адміністративні чи кримінальні порушення (кражі напр.)

Торгова марка існує доти, поки використовується в комерційних цілях.
Закони — індивідуальні для країн.

Слід також зазаначити, що закон завжди на крок позаду дійсності: розвиток інтернет показує, що наявні закони захисту ІВ в багатьох моментах недостатні або неефективні. Закони “доганяють” дійсність, тому те, що вчора було легальним, сьогодні може бути вже кримінально-відповідальним.

Чому необхідно використовувати ліцензійне ПО?

Насправді таке питання не повинно навіть виникати.
Однак, за даними Державного комітету зв'язку та інформатизації України, рівень використання піратського ПО в Україні становить коло 80%.
В 2007 році знизився всього лиш на 1%.
Україна входить в 20-ку країн з найвищим рівнем використання піратського ПО.
Загально по світу рівень зріс на 3% і складає коло 40%.
Цифри вражаючі.
Зокрема по Україні втрати в економіці внаслідок цього щорічно складають кого 400 млн. доларів США.

Отже, ЧОМУ потрібно використовувати легальне (ліцензійне) ПО:

1. бо використання неліцензійного протирічить законодавству і тягне за собою кримінальну відповідальність
2. бо використання піратського ПО грозить компанії розривом відносин з як мінімум зарубіжними партнерами і втратою контрактів
3. робота виключно з ліцензійним ПО є необхідною для проходження організацією сертифікації на відповідність стандартам ISO.
4. Ліцензійне ПО дає можливість користуватися технічною підтримкою
5. ліцензійне ПО гарантує відсутність збоїв в роботі з причин зміни вихідних файлів програми (АЛЕ не гарантує відсутність збоїв як таких, нажаль)
6. гроші, потрачені на ліцензійне ПО, сприяють його покращенню.

Особливості ліцензування продуктів Microsoft

Підприємства як правило цікавлять ліцензії на Windows та Office.
Перед покупкою необхідно дізнатися всі деталі у представника.
Тим не менше, фактично всі ліцензії відрізняються, як на мене, доволі “драконівськими” умовами.

Купити ПО Microsoft можна багатьма способами, але завжди покупка супроводжується ліцензією.
Один і той самий продукт, в залежності з якою ліцензією він куплений, можна буде використовувати по-різному.

Види ліц. Microsoft:

- FPP License — Full Package Product (найдорожчий спосіб, необеженеий в термінх, в залізі а також часто влючає право установки на ще один — переносний - комп'ютер)
- OEM License - Original Equipment Manufacturer (для продавців комп. Техніки, не дозволяє заміни материнської плати а часто і більше 3-ох модернізацій комп'ютера взагалі, не є *апгрейдними,* найдешевший спосіб)
- OLP License — Open License Product (для корпоративних клієнтів, для організацій — тут є купа ліцензій, “знижок” і додаткових угод)

Є і інші.

Напр. Wndows Home Edition не можна використовувати на підприємствах та в організаціях.
НЕ можна напр. подарувати чи здати в оренду (напр інтернет-кафе має мати спеціальну угоду окрім професійних ліцензій).

Ліцензії Microsoft (окрім корпоративних) вимагають також зовнішніх атрибутів ліцензування: голографічної наліпки на блоку.
Вимагають також “активації” продукту.

Є також програми легалізації неліцензійного ПО.

Спеціальні ціни є також для освітніх організацій.
http://www.microsoft.com/

Ліцензії GPL, BSD та інші

Але ж існує також “безкоштовне” ПО. ПО, яке не вимагає плати за використання, але поширюється також за певними ліцензіями.

Потрібно розрізняти ПО безкоштовне і т.зв. ***відкрите*** ПО (ПО з відкритими вихідними кодами).
Напр Skype чи ICQ і Jabber — прикладів тисячі.

Ліцензія GPL (GNU GPL) — General Public License - найбільш відома з “відкритих” ліцензій.
Автор — Richard Stallman, GNU — його проект.
Основна мета цієї ліцензії — не допустити “закривання” програм, які раніше були випущені як вільні.
Столлман — історична особа, попри те, що йому зараз 55. В 1985 році заснував Free Software Foundation.
Цікаво, що GNU розроблявся як некомерційна альтернатива в той час дорогому і комерційному UNIX (як зараз помінявся контекст!).

GPL надає право вільно використовувати, модифікувати і поширювати програму при одній умові: разом з програмою мають поширюватися її вихідні коди, включаючи всі зроблені зміни і то за тією ж ліцензією.
Допускається не поширювати коди, якщо можна їх вільно отримати в будь-який момент часу безкоштовно.

Формально безплатність не вимагається.

З GPL зв'язано поняття Copyleft (автор втрачає право на обмеження прав володіння програмою) а також цілий потужний рух за вільне програмне забезпечення.

Цікаво, що GPL первинно виникла як GNU GPL (1983) — Gnu's Not Unix — як ліцензія до ОС GNU (UNIX-подібна ОС Столлмана) на противагу комерційному UNIX.

1991 — версія 2, 2007 — версія 3, на яку ще багато проектів і не перейшли (зокрема ядро Linux — Лінус Торвальдс вважає GPLv2 кращим варіантом).

GPL на сьогоднішній день є найбільш використовуваною з “відкритих” ліцензій.

Ліцензія BSD — програмна ліцензія університету Берклі.

Напевно найпростіша, найкоротші і найдемократичніша ліцензія.

Коротко: робіть з програмою все, що завгодно, але не кажіть, що ви її написали.

Програмні продукти під цією ліцензією можна вбудовувати в пропрієтарне ПО, але необхідно вказувати авторство вихідного коду.

Приклади: стек мережевих з'єднань в OS MS Windows, Mac OS X використовують багато фрагментів коду з BSD ліцензіями.

Вважається, що BSD ліцензія краще захищає розробника, а GPL — користувача.
ПОЯСНИТИ.

Існує велика маса клонів цих двох ліцензій а також інші відкриті ліцензії, напр Apache Software License, Mozilla Public License.

Останні 2 роки характерні спробами притягнути до суду порушників GPL. Зокрема 07.2007 — 05.2008 рік — процес проти Skype в Німеччині, яка випустила бездротовий телефон з прошивкою на базі Linux, але не під GPL ліцензією і з закритими кодами.
В США донедавна прецеденту не було — всі позови закінчувалися мирним врегулюванням (з сумою відступного, яка не розголошується). Однак буквально недавно такий прецедент було зроблено: http://www.opennet.ru/opennews/art.shtml?num=18272
Розробник-ентузіаст відкритого програмного пакету для моделювання роботи мініатюрних залізниць в 2006 році подва в суд на компанію, що випускає такі залізниці і ПО для них за включення його програмного коду в комерційний продукт. Відповідач признав включення коду, а свій захист будував на тезисі непризнання ліцензії недійсною, оскільки її умови неможливо виконати.

Навіщо людям віддавати плоди своєї праці під відкритими ліцензіями:

1. заробіток на підтримці (приклад — RedHat)
2. навчання і здобуття імені
3. неоціненний досвід роботи з спеціалістами всього світу (comunity)
4. альтруїзм, філантропія

Багато великих і серйозних компаній також розробляє ПО з відкритим кодом і частково під відкритими ліцензіями. Приклади: Sun Microsystems (Open Office, MySQL віднедавна), IBM (Eclipse), Nowell (SuSE Linux).
RedHat як особлива компанія, що фактично перша цілком побудувала свою ринкову стратегію на підтримці і розробці GPL продуктів (RedHat Linux, пізніше розділений на два продукти: Enterprise і Fedora).
Вигода від таких проектів для компаній далеко не тільки іміджева.

По-суті використання продуктів, основаних на відкритих чи пропрієтарних ліцензіях носить принциповий характер.
Вибирається глобально ПІДХІД до побудови інформаційних систем, оскільки **на сьогоднішній день** в більшості випадків можна знайти потрібне рішення як на тій так і на іншій ліцензійній основі.

Microsoft використовує великий арсенал маркетингових ходів для підтримки своєї монополії на ринках офісних і десктопних систем.

Одним з таких постійно експлуатованих ходів є поняття про ***сумарну вартість володіння.***
Під сукупною вартістю володіння розуміють затрати на програмне і апаратне забезпечення протягом всього циклу його експлуатації.
(затрати на покупку, на установку, сервісне і гарантійне обслуговування, навчання персоналу і т.д.)
Нещодавно Мікрософт опублікувала результати дослідження вартості програмного забезпечення для використання в навчальному процесі в країнах, що розвиваються, на основі Linux та MS Windows.
Висновок є такий, що "сумарна вартість володіння для комп'ютерів на базі Linux та MS Windows є приблизно однаковою".
Такий висновок зроблено тому, що результати показали великий дефіцит і відповідно дороговизну адміністраторів лінукс в країнах, що розвиваються.
Є, однак інші фактори, які показують, що це не так (напр. Віндовс потребує як правило платного антивіруса, потужнішого "заліза" і т.п.)
Слід також зауважити, що платячи місцевому спеціалісту, компанії підтримують місцеву економіку, а платячи за продукти Мікрософт — в кінцевому результаті виводять гроші зі своєї країни.

Іншим ходом є наприклад угоди з виробниками серійних комп'ютерів (напр. ноутбуків — приклад — нетбуки, де вартість ОС стає суттєвою в порівнянні з "залізом" - виробники отримують значну вигоду від співпраці з Microsoft).

Ще одни хід — боротьба стандартів. Останній приклад — весна цього року боротьба за стандарт офісного формату документу ISO - Open Document Format (ODF) проти Microsoft OOXML. (OOXML спершу було прийнято, потім справедливо відхилено, але ще не остаточно і робота триває).

Ще інший хід — використання прийому "вбудовування" програм в ОС (монополізм, відсутність конкуренції). Приклади — суди по включенню браузера в ОС, з резонансного — по включенню медіа-плеєра в ОС в Європі — мілліонні компенсації + альтернатива.

Відповідальність за установку і використання неліцензійного ПО

Основа — ст. 176 Кримінального Кодексу України та статті Кодексу України про адміністративні правопорушення.
Адміню відповідальність — штрафи від 200 до 1000 неоподаткованих мінімумів, якщо ж сума збитків перевищує 1000 неоподаткованих мінімумів, то кримінальна відповідальність — ув'язнення терміном до 2 років (далі - детальніше).

Для підтвердження ліцензійності ПО підприємство повинно мати відповідні документи як бухгалтерські так і від виробника ПО: рахунок-фактура, накладна, , податкова накладна, угода з виробником, текст ліцензії, голографічні наклейки і т.п.

Окрім того, провіряючі органи можуть вимагати сертифікат компанії, у якої купувалось ПО — підтвердження легальності ввозу ПО в Україну.

Безпосередньо відповідальність за використання неліцензійного ПО несе керівник (адміністративний директор) компанії. Якщо керівництво видає наказ, що така відповідальність покладається на керівника IT відділу, сисадміна чи іншу особу, то відповідальність несе також і він.

Якщо є наказ про відповідальність кожного співробітника, то і кожен співробітник, але директор в будь-якому випадку теж.

Системний адміністратор по змозі повинен написати службову записку директору про використання такого ПО. Це, однак відповідальності з нього не знімає, а є лише пом'якшуючою обставиною, бо доводить, що його дії були зумовлені матеріальною і службовою залежністю.

Хто має право перевіряти ліцензійність ПО?

На сьогодні існують 3 органи, які мають право здійснювати такі перевірки:

1. Державний департамент інтелектуальної власності (е всі співробітника, а лише інспектори з питань інтелектуальної власності)
2. Державна служба по боротьбі з економічною злочинністю МВС України
3. Органи державної податкової інспекції.

Конкретніше **відповідальність:**
За використання неліцензійного ПО а також **за зберігання неліцензійних аудіо та відео та інших файлів** передбачено 2 види відповідальності:

1. **Адміністративна** (кодекс про адміністративні правопорушення)

Стаття 512. Порушення прав на об'єкт права інтелектуальної власності
Незаконне використання об'єкта права інтелектуальної власності (літературного чи художнього твору, їх виконання, фонограми, передачі організації мовлення, комп'ютерної програми, бази даних, наукового відкриття, винаходу, корисної моделі, промислового зразка, знака для товарів і послуг, топографії інтегральної мікросхеми, раціоналізаторської пропозиції, сорту рослин тощо), привласнення авторства на такий об'єкт або інше умисне порушення прав на об'єкт права інтелектуальної власності, що охороняється законом, -

тягне за собою накладення штрафу від десяти до двохсот неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно виготовленої продукції та обладнання і матеріалів, які призначені для її виготовлення.

2. **Кримінільна** (кримінільний кодекс)

Стаття 176. Порушення авторського права і суміжних прав

1. Незаконне відтворення, розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, а так само незаконне відтворення, розповсюдження виконань, фонограм, відеограм і програм мовлення, їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації, або інше умисне порушення авторського права і суміжних прав, якщо це завдало матеріальної шкоди у значному розмірі, -

караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення.

2. Ті самі дії, якщо вони вчинені повторно, або за попередньою змовою групою осіб, або завдали матеріальної шкоди у великому розмірі, -

караються штрафом від тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк від двох до п'яти років, з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення.

3. Дії, передбачені частинами першою або другою цієї статті, вчинені службовою особою з використанням службового становища або організованою групою, або якщо вони завдали матеріальної шкоди в особливо великому розмірі, -

караються штрафом від двох тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до шести років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого та з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувалися для їх виготовлення.

Примітка. У статтях 176 та 177 цього Кодексу матеріальна шкода вважається завданою в значному розмірі, якщо її розмір у двадцять і більше разів перевищує неоподатковуваний мінімум доходів громадян, у великому розмірі - якщо її розмір у двісті і більше разів перевищує неоподатковуваний мінімум доходів громадян, а завданою в особливо великому розмірі - якщо її розмір у тисячу і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Для определения размера ущерба необходимо проведение экспертного исследования. Для этого контролирующие органы должны привлекать к проведению проверки эксперта либо производить изъятие носителей программ (об изъятии смотри ниже).

НО при этом НЕОБХОДИМО отметить, что к ответственности по ст. 176 Уголовного кодекса Украины лицо может быть привлечено только в том, случае, что такие действие совершалось с прямым умыслом, т.е. виновное лицо должно было:
- осознавать, что нарушает авторские либо смежные права;
- предвидело, что автору будет нанесен материальный вред в крупном размере (от 5150,00 грн. на сегодня);
- желало этого (т.е. нарушить авторские либо смежные права и причинить как минимум вред в крупном размере).
Т.е. доказать наличие прямого умысла – достаточно сложное мероприятие, хотя само по себе наличие возбужденного уголовного дела не самое приятное обстоятельство.

ЧТО ПОНИМАЕТСЯ ПОД НЕЗАКОННЫМ ИСПОЛЬЗОВАНИЕМ?
Незаконное использование объекта права интеллектуальной собственности – под ним понимается опубликование, воспроизведение, распространение без согласия автора (собственника патента или свидетельства) литературного или художественного произведения, фонограммы, видеограммы, аудиовизуальных произведений, передач организации вещания, компьютерных программ, баз данных и иных объектов.

Под воспроизведением понимается изготовление одного или более экземпляров произведения, видеограммы, фонограммы в любой материальной форме, а также из запись для временного или постоянного хранения в электронной (в том числе и цифровой), оптической или иной форме, которую может считывать компьютер.

ИЗЪЯТИЕ:
1. В случае составления протокола об административном правонарушении.
В соответствии со ст. 265 кодекса об административных правонарушениях – вещи и документы, которые являются орудием либо непосредственным объектом правонарушения, выявленные во время задержания, личного осмотра либо осмотра вещей изымаются, о чем составляется протокол и делается соответствующая запись в протоколе об административном правонарушении.
2. В случае наличия возбужденного уголовного дела.
В таком случае выемка проводится с соблюдением условий и порядка, предусмотренного ст. 184, 177, 178 Уголовно-процессуального кодекса Украины.
А именно:
Выемка проводиться в случаях, коли имеются точные данные о том, что предметы или документы, которые имеют значение для дела и находятся у определенного лица либо в определенном месте.
Выемка из жилища либо иного владения лица (а офис является как раз иным владением) проводится только по мотивированному постановлению суда. При этом выемка должна проводиться только днем и в присутствии не менее двух понятых.
Кроме того, Верховный суд в своем обобщении по правонарушениям в сфере интеллектуальной собственности от 01.01.2006 года (п. 3.1.) придерживается той позиции, (учитывая положения ст. 420 Гражданского кодекса Украины и ст. 1 закона Украины «Об авторских и смежных правах»), что компьютеры не являются объектами права интеллектуальной собственности, их носителями или предметами, предназначенными для изготовления контрафактных экземпляров, и соответственно не являются объекта административного правонарушения или преступления, а значит, что и изъятию либо выемке они не подлежат. Поэтому в случае выявления нарушения контролирующие органы могут ставить вопрос только о изъятии носителей таких программ (например, жесткого диска), но НЕ КОМПЬЮТЕРНОЙ ТЕХНИКИ.

Учитывая все вышеизложенное, считаю, что самым идеальным вариантом для нас являются совокупность следующих действий:
1. Создать приказ о закреплении за каждым сотрудником определенного компьютера в соответствии с номерами, присвоенными инвентарной описью.
2. Создать приказ о запрете установления сотрудниками на компьютерах нелицензионного программного обеспечения, а так же хранения аудио- , видео- и иных файлов без наличия лицензии на право из использования и хранения.
3. Системному администратору самому проверить все компьютеры в офисе и в случае выявления программ либо файлов, которые нарушают авторские и смежные права, все их немедленно удалить
4. Технически создать запрет на установление самостоятельно пользователем любых программ (что бы ставить любые программы мог только системный администратор). Если это технически возможно, то установить так же невозможность самостоятельно пользователю копировать на компьютер всякого рода аудио- и видеофайлы.

5. Создать на каждый компьютер учетную карточку программ, которые там установлены и приказами закрепить за каждым сотрудником наличие таких программ в их компьютерах и еще раз (дополнительно к приказу из п. 2 этого перечня) запретить устанавливать самостоятельно АБСОЛЮТНО любые программы, а также хранить в компьютере любые аудио- и видеофайлы, кроме тех, которые имеются в учетной карточке.
6. Хотя бы раз в две недели системному администратору проводить аудит всех компьютеров с целью выявления файлов и программ, нарушающих авторские и смежные права
7. Провести собрание всех сотрудников с целью уведомления о наличии, предусмотренной законодательством ответственности (административной, уголовной и гражданской) за нарушение авторских и смежных прав и о возможности предприятия в случае выявления контролирующими органами и наложения любых штрафов взыскивать все эти суммы с сотрудников, в компьютере у которых будут найдены такие программы (а также аудио- и видео файлы). Такое собрание оформить протоколом общего собрания коллектива предприятия.
8. Неофициально (без приказа) установить ответственность в виде штрафа (например, в сумме 500 гривен) в случае нарушение любого из вышеуказанных требований. Думаю, что никто из сотрудников не будет против, понимая серьезность этой ситуации и прежде чем нарушать эти правила, подумает, стоит ли терять из з\п такую сумму. И в случае выявления таких нарушений не жалеть виновного и штраф все-таки накладывать. Думаю, что в случае наличия такого претендента это будет хорошим, а главное запоминающимся уроком не только для виновного, но и для всех остальных.
9. Возложить на системного администратора обязанность (приказом и должностной инструкцией) устанавливать только лицензионное программное обеспечение и контролировать наличие на всех компьютерах файлов и программ, которые нарушают авторские и смежные права, а в случае их обнаружения немедленно их удалять и уведомлять о таком факте директора.
10.

Что на самом деле можно сделать, чтобы обезопасить себя при проверке ПО

Если к вам еще не пришли, но вы опасаетесь этого

В Интернете предлагается множество способов подстраховаться на случай проверки. Вот некоторые из них:

Во-первых, вы можете попытаться изменить внешний вид приложений, замаскировав их под свободно распространяемое ПО. Правда, квалифицированный специалист быстро поймет, что тут к чему на самом деле.

Вариант номер два. Вы можете поставить на своих компьютерах в качестве второй операционной системы свободно распространяемую Linux, а раздел с Windows зашифровать и закрыть с помощью аппаратного USB-ключа. При включении компьютера без USB-ключа будет грузиться Linux, никаких признаков таящейся глубоко в недрах Windows на поверхности видно не будет. Правда, если компьютеры будут конфискованы, это вас не спасет – специалисты все равно обнаружат то, что вами спрятано.

Еще один способ подстраховаться – это перед установкой нелицензионного софта отмотать системную дату таким образом, чтобы в платежных документах значилось, что системные блоки приобретены позже. Тогда в случае проверки вы сможете утверждать, что купили системные блоки такими какие они есть, ничего сами не устанавливали, думали, что оно так и должно быть. Правда, от конфискации и неизбежных проблем это все равно не спасет, да и обратиться с вопросами к фирме, которая продала вам блоки, сотрудникам правоохранительных органов ничто не мешает.

Четвертый вариант, самый лучший, но слегка утопичный – раздать всем сотрудникам флешки, на каждой из которых установлен весь набор необходимых для работы программ, и загружать компьютеры с них. Отдельную флешку отвести под документы. Тогда пришедшие к вам с проверкой сотрудники милиции обнаружат только «голые» компьютеры. Они будут крайне удивлены, но вряд ли смогут что-то сделать. Флешка будет являться частной собственностью конкретного физического лица, и изъята она может быть только по постановлению суда, касающемуся именно этого конкретного физического лица.

Если к вам уже пришли

В первую очередь внимательно проверьте документы проверяющих: постановление прокурора, удостоверения всех проверяющих, паспорта понятых. Запишите все данные.

Если сотрудниками милиции изымается системный блок, на котором предположительно имеется нелицензированная программа, должен быть составлен соответствующий протокол, в котором должны быть отражены следующие факты: должностное лицо, производящее изъятие, место и время изъятия, наличие понятых, разъяснение участникам их прав и обязанностей, какие технические средства обнаружения используются и кем; последовательно описываются действия лица, производящего осмотр, специалистов, обнаруженные объекты, их вид и состояние на момент осмотра, изымаемый предмет и его индивидуальные идентифицирующие признаки (серия, модель, номер). Изъятый предмет должен быть упакован так, чтобы доступ к содержащейся в системном блоке информации был невозможен без повреждения защитных пломб, бирок, печатей (скреплённых подписями понятых), о чём производится запись в протоколе. Таким же образом должно быть оформлено изъятие соответствующих документов. Протокол подписывается всеми участниками осмотра после ознакомления с его текстом, при этом им должна быть предоставлена возможность реализовать своё право сделать замечания или дополнения к протоколу.

Если вы опасаетесь, что сотрудники милиции, конфисковав ваш лицензионно чистый компьютер, «подкинут» в него что-нибудь контрафактное, а потом скажут, что так и было, можете измерить и зафиксировать общий общем данных и количество файлов на жестком диске.

Камеры в офисе также могут быть полезны. Если во время проверки сотрудники правоохранительных органов, по вашему мнению, как-то нарушали закон – видеозапись может служить доказательством их противоправных действий (статьи 74 и 84 УПК РФ).

Чаще всего проверки программного обеспечения проводятся по письменному заявлению представителей правообладателя (1С, «Антивирусная лаборатория Касперского» и т.д.) Также возможен вариант, когда уволенный и недовольный этим фактом сотрудник «стучит» на фирму, сообщая где и что конкретно нелицензионного у нее имеется. В любом случае, никто не станет тратить время и проверять вас просто так. Если вы

лицензионно «чисты» вероятность того, что к вам придут с проверкой, резко уменьшается.

Чтобы застраховаться от несанкционированного появления на ваших компьютерах «пиратских» программ и связанных с их обнаружением неприятностей, придерживайтесь простых принципов:

1. Права на установку и удаление программ должны быть только у системного администратора, рядовые сотрудники не должны иметь такой возможности, она им ни к чему.

2. Необходимо отслеживать процесс поступления программных продуктов в организацию от поставщиков, обеспечить отражение в бухгалтерском и налоговом учёте затрат на приобретение объектов интеллектуальной собственности.

3. Вся документация, касающаяся приобретенных программных продуктов (лицензии, регистрационные карточки и сертификаты, счета-фактуры и т.д.) должна быть сосредоточена в одном месте. Так вы ничего не потеряете и сможете оперативно предъявить все необходимые документы проверяющим.

4. Иногда в магазинах можно увидеть OEM версии различных программ. Да, это легальные копии и продажа их вполне законна. Но они предназначены только для фирм, занимающихся сборкой компьютеров! OEM — это ограниченный вариант лицензии, OEM-версии программ могут быть установлены на компьютер только в процессе его сборки фирмой, которая этим занимается. В случае проверки вам придется документально доказывать, что все происходило именно так. Поэтому не покупайте диски с пометкой «OEM» в магазинах, имеющиеся на них программы нельзя устанавливать на ранее приобретенные компьютеры. Вы только потратите достаточно крупную сумму денег, а результат будет таким же, как если бы вы установили что-то «пиратское». К тому же OEM имеет массу недостатков. OEM привязывается к материнской плате и процессору. Вам придется звонить в Microsoft каждый раз, когда требуется переустановить систему, и объяснять им причину переустановки. Они могут разрешить вам это, а могут и запретить, в этом случае активировать систему вам не удастся.