

– Один раз у рік необхідно колодязь піддавати очищенню.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Кульський Л. А. Основы химии и технологии воды / Л. А. Кульський. – Київ : Наукова думка, 1991. – 568 с.
2. Грабовська Л. Л. Методи очистки і контролю якості води [Електронний ресурс] / Л. Л. Грабовська. – Режим доступу : http://lubbook.net/book_530.html.
3. Новиченко В. Г. Жизнь воды / В. Г. Новиченко, С. В. Шеховцов. – Запорожье : Здоровье, 2010. – 191 с.
4. Дронов В. П. Экономическая и социальная география / В. П. Дронов, В. П. Максаковский, В. Я. Ром. – Справоч. материалы. – М. : Просвещение, 1994. – 208 с.
5. Можаровська О. А. Визначення мінералізації води / Електронний ресурс. Режим доступу: http://www.labprice.ua/zastosuvannya_vimiryuvalnix_priladiv_dlya_vodi_ezodo/viznachennya_mineralizaci_i_vodi

Чернега Аліна Миколаївна, студентка групи ЕКО-16м, інститут екологічної безпеки та моніторингу довкілля, Вінницький національний технічний університет, Вінниця, e-mail : alina.cherneha@gmail.com
Науковий керівник: **Томчук Микола Антонович**, кандидат технічних наук, доцент кафедри БЖДПБ, Вінницький національний технічний університет, Вінниця, e-mail : tomchuk68@mail.ru

Alina M. Chernega, student of group ECO-16m, the Institute of ecological safety and monitoring of environment, Vinnytsia National Technical University. Vinnitsa, e-mail : alina.cherneha@gmail.com
Supervisor: **Nicholas A. Tomchuk**, PhD, department of HSS, Vinnytsia National Technical University, Vinnytsia, e-mail : tomchuk68@mail.ru

УДК 681.3.07

В. М. Чорний
М. А. Томчук

ЗАСОБИ ЗАХИСТУ ПРОГРАМНИХ ПРОДУКТІВ

Вінницький національний технічний університет

В статті розглянуто основні причини захисту програмних продуктів, цілі захисту, захист від впливу людини, апаратури та спеціалізованих програм. Проаналізовано основні технології захисту програмних продуктів та встановлено основні способи захисту продуктів і персональних даних користувачів..

Ключові слова: захист; технології, способи, програмні продукти; бази даних, авторизація, автентифікація.

MEANS OF PROTECTION OF SOFTWARE PRODUCTS

In the article basic reasons of protection of software products, the protection purposes, the protection against influence of the person, an equipment and specialized programs are considered. The main technologies of protection of software products are analyzed and the main methods of protection of products and personal information of users are set.

Keywords: protection; technologies, methods, software products; databases, authorization, authentication.

Захист програмних продуктів – це комплекс заходів, спрямованих на захист програмного забезпечення від несанкціонованого придбання [1], використання, поширення, модифікування, вивчення і відтворення аналогів.

Програмні продукти є важливими об'єктами захисту за цілою низкою причин:

- ПП являють собою продукт інтелектуальної праці фахівців;
- проектування цих продуктів пов'язано зі споживанням значних матеріальних і трудових ресурсів і засноване на застосуванні дорогого комп'ютерного устаткування і наукомістких технологій;

– для відновлення порушеного програмного забезпечення необхідні значні трудовитрати.

Захист програмних продуктів переслідує такі цілі:

- обмеження несанкціонованого доступу окремих категорій користувачів до роботи з ними;
- виключення навмисного псування програм з метою порушення нормальної обробки даних;
- недопущення навмисної модифікації програми;
- перешкоджання несанкціонованому тиражуванню програм;
- виключення несанкціонованого вивчення змісту, структури і механізму роботи програми.

Програмні продукти і бази даних повинні бути захищені за кількома напрямками від впливу:

- людини – розкрадання машинних носіїв і документації програмного забезпечення;
- апаратури – підключення до комп'ютера апаратних засобів для модифікації програм і даних або їх фізичного руйнування;
- спеціалізованих програм – приведення програмного продукту або бази даних в неробочий стан (вірусне зараження), несанкціоноване копіювання програм і бази даних і т.д.

Незважаючи на всі зусилля різних організацій в останні роки продовжується зростання комп'ютерного піратства. В середньому частка піратського ПЗ в глобальному масштабі становить 40%.

З піратством можна боротися різними способами. Основний – легітимний. Тобто злом і незаконне поширення програмного забезпечення повинні бути правильно описані у відповідних законах, і держава повинна здійснювати переслідування піратів і залучати їх до відповідальності.

Ще одним ефективним методом боротьби з піратством – економічний метод [2], коли ціна продукту настільки низька, що може зрівнятися з ціною зламаною продукту, що продається піратами. У більшості випадків, якщо ціна буде однаковою, покупець віддасть перевагу ліцензійному продукту. Проте, економічна конкуренція з піратством справа дуже важка і підходить далеко не всім виробникам програмного забезпечення. Такі виробники звертаються до третього методу – захист програмного забезпечення від злomu і нелегального копіювання.

Технології захисту постійно еволюціонують. Як показує практика, для злomu нової захисту потрібно від декількох днів, до декількох місяців. Також існують поки не зламани захисту, про них мова піде нижче. Найпростіші і найдоступніші спосіб захисту програмних продуктів полягає в обмеженні доступу до них за допомогою:

- авторизації та автентифікації [3] користувача;
- електронного ключа;
- спеціального технічного пристрою, що підключається до порту вводу-виводу комп'ютера.

Для програмних продуктів дієвими захисними заходами є:

- ідентифікація середовища, в якому запускається програма;
- введення обліку числа виконаних санкціонованих інсталяцій або копіювання;
- протидія нестандартному форматування диску;
- закріплення місця розташування програми на жорсткому диску;
- прив'язка до електронного ключа або пристрою, що підключений до порту вводу-виводу.

При захисті програмних продуктів необхідно використовувати і правові методи. Серед них виділяються ліцензування угод і договорів, патентний захист, авторські права, технологічна і виробнича секретність. Патентний захист [4] встановлює пріоритет в розробці і використанні нового підходу або методу, застосованого при розробці програм, засвідчує їх оригінальність.

Статус виробничого секрету для програми обмежує коло осіб, знайомих або допущених до її експлуатації, а також визначає міру їх відповідальності за розголошення секретів. Наприклад, використовується паролний доступ до програмного продукту чи бази даних, аж до паролів на окремі режими (читання, запис, коригування тощо). Програми, як будь-який матеріальний об'єкт велику вартість, необхідно охороняти від крадіжки і навмисних руйнувань.

Ліцензійні угоди поширюються на всі аспекти правової охорони програмних продуктів, включаючи авторське право, патентний захист, виробничі секрети. Найбільш часто використовуються ліцензійні угоди на передачу авторських прав. Авторське право – автору незалежно від його майнових прав належать особисті авторські права (ім'я автора – недоторканність програмного продукту).

Майнові права на програмний продукт або базу даних можуть бути передані частково або повністю іншим фізичним або юридичним особам за договором. Майнові права належать до категорії успадкованих. Якщо програмний продукт або база даних створені в порядку виконання службових

обов'язків, майнові права належать роботодавцю.

Програмні продукти і бази даних можуть використовуватися третіми особами – користувачами на підставі договору з правовласником. Особа, яка правомірно володіє примірником програми або бази даних, має право, без отримання додаткового дозволу правовласника, здійснювати будь-які дії, пов'язані з функціонуванням програмного продукту або бази даних відповідно до її призначення, в тому числі:

- встановлювати один екземпляр, якщо не передбачено інше в угоді з правовласником;
- виправляти явні помилки;
- адаптувати програмний продукт або базу даних;
- виготовляти копії.

Висновок: захист програмних продуктів є необхідним заходом як для розробника так і для користувача цієї програми. Розробник програми зберігає за собою авторство, можливість подальшої модифікації програми та продажу. Користувач програми – отримує гарантію того, що його дані не потраплять в руки зловмисників.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Новичков А. А. Анализ рынка средств защиты от копирования и взлома программных средств / А. А. Новичков, Р. Сардарян – Режим доступу: <http://citforum.ru/security/articles/analis>.
2. Зайцев О. В. Реализация простого механизма активации в приложении / О. В. Зайцев [Електронний ресурс] – Режим доступу: <http://www.z-oleg.com/secur/articles/progprotect.php>
3. Варлатая С. К. Программно-аппаратная защита информации: учебн. пособие / С. К. Варлатая, М. В. Шаханова. – Владивосток : Изд-во ДВГТУ, 2007. – 318 с
4. Защита от пиратства и лицензирование ПО StarForce [Електронний ресурс]. – Режим доступу до ресурса: <http://www.star-force.ru/>.

Чорний Вадим Михайлович, студент, Вінницький національний технічний університет, Вінниця
Томчук Микола Антонович, кандидат технічних наук, доцент кафедри БЖДПБ, Вінницький національний технічний університет, Вінниця, e-mail : tomchuk68@mail.ru

Vadym Chronyi, student, Vinnytsia National Technical University, Vinnytsia
Nicholas A. Tomchuk, PhD, department of HSS, Vinnytsia National Technical University, Vinnytsia, e-mail : tomchuk68@mail.ru

УДК 334.72

О. О. Шамраєва

РОЗВИТОК ОХОРОНИ ПРАЦІ В УКРАЇНІ ЯК ДИСЦИПЛІНИ У НАВЧАЛЬНИХ ЗАКЛАДАХ

Вінницький національний технічний університет

У роботі розглянуто основні аспекти ведення державної політики щодо управління охороною праці в Україні, висвітлено питання стану охорони праці як дисципліни у вищих навчальних закладах.

Ключові слова: охорона праці, нещасний випадок; професійне захворювання, державна політика, управління охороною праці, стан охорони праці.

DEVELOPMENT OF LABOR IN UKRAINE AS A SUBJECT IN UNIVERSITY

The article discusses the main aspects of state policy on safety management in Ukraine and issues of labor status as a discipline in higher education.

Keywords: safety, accident, occupational disease, public policy, safety management, the state of safety.