

200 РОКІВ
ОСВІТНІХ ТРАДИЦІЙ



Том 2

**ТЕЗИ
71-ої наукової конференції
професорів, викладачів, наукових
працівників, аспірантів та студентів університету**



**ПОЛТАВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ
УНІВЕРСИТЕТ ІМЕНІ ЮРІЯ КОНДРАТЮКА**

Міністерство освіти і науки України
Північно-Східний науковий центр НАН України та МОН України
Полтавський національний технічний університет
імені Юрія Кондратюка

Тези

71-ої наукової конференції професорів,
викладачів, наукових працівників, аспірантів
та студентів університету

Том 2

22 квітня – 17 травня 2019 р.

Полтава 2019

УДК 043.2
ББК 448лО

*Розповсюдження та тиражування без офіційного дозволу
Полтавського національного технічного університету
імені Юрія Кондратюка заборонено*

Редакційна колегія:

Онищенко В.О.	д.е.н., проф., ректор Полтавського національного технічного університету імені Юрія Кондратюка
Сівіцька С.П.	к.т.н., доц., проректор з наукової та міжнародної роботи Полтавського національного технічного університету імені Юрія Кондратюка
Агейчева А.О.	к.пед.н., доц., в.о. декана гуманітарного факультету Полтавського національного технічного університету імені Юрія Кондратюка
Винников Ю.Л.	д.т.н., професор, в.о. директора навчально-наукового інституту нафти і газу Полтавського національного технічного університету імені Юрія Кондратюка
Гришко В.В.	д.е.н., професор, директор навчально-наукового інституту фінансів, економіки та менеджменту Полтавського національного технічного університету імені Юрія Кондратюка
Семко О.В.	д.т.н., професор, в.о. директора навчально-наукового інституту архітектури та будівництва Полтавського національного технічного університету імені Юрія Кондратюка
Хоменко І.В.	к.т.н., доцент, в.о. директора навчально-наукового інституту інформаційних технологій та механотроніки Полтавського національного технічного університету імені Юрія Кондратюка

Тези 71-ої наукової конференції професорів, викладачів, наукових працівників, аспірантів та студентів університету. Том 2. (Полтава, 22 квітня – 17 травня 2019 р.) – Полтава: ПолтНТУ, 2019. – 474 с.

У збірнику тез висвітлені результати наукових досліджень професорів, викладачів, наукових працівників, аспірантів та студентів університету.

©Полтавський національний технічний
університет імені Юрія Кондратюка,
2019

ШИФРУВАННЯ ТА ЗАХИСТ ЦИФРОВИХ ДОКУМЕНТІВ ЗА ДОПОМОГОЮ КЛЮЧА СCRYPTO-BOX

Коли йдеться про безпеку програмного забезпечення, генеральні директори й інші особи, відповідальні за захист цінних цифрових активів, їхньої корпоративної інфраструктури та важливого каналу розподілу, повинні відповісти на запитання: чи можна отримати повний захист і яким чином; що захищати та як; чи сприятиме це стратегії, відноsinам як з дистрибуторами, так і з кінцевими користувачами?

Безумовно, найкращим підходом для визначення необхідності захисту цифрових активів є аналіз ризику.

З метою забезпечення збереженості інформації технологічної компанії необхідно:

- виявити активи, що потребують захисту (програми, дані, засоби масової інформації, знання в базах даних і документації, інфраструктуру зв'язку, гроші);
- розглянути види ризиків, які можуть уплинути на залучені активи, наприклад: піратство, крадіжка інтелектуальної власності, крадіжка ідентифікаційних даних, інсайдерські робочі місця, незадоволені працівники, перехоплення даних;
- з'ясувати ймовірність виникнення ризику та спробувати визначити, де можна «отримати найбільшу безпеку для долара».

Програмне забезпечення й захист даних за допомогою ключа CRYPTO-BOX гарантують, що кожен кінцевий користувач внесе плату за продукт. Як відомо, письмові угоди та ліцензії не завжди запобігають несанкціонованому використанню, а їхнє застосування може створити антагоністичні відносини з кінцевими користувачами.

Виробники програмного забезпечення вивчають ті проблеми, які виникають на сьогоднішньому конкурентному ринку. Важливо постійно розробляти інноваційні й зручні для клієнтів продукти, щоб запобігти піратству.

Програмне піратство виявляється у багатьох різних формах. Наприклад, різноманітні веб-сторінки пропонують ліцензії на доступ до програмного забезпечення для отримання від звичайної ринкової ціни. Такі ліцензії часто є підробними, одна ліцензія може продаватися декількома клієнтами. Крім того, клієнт купує тільки одну ліцензію і використовує її на декількох робочих місцях компанії. Часто використовують зламані версії програмного забезпечення.

За даними BSA Global Software Survey, за 2016 рік 39% програмного

забезпечення, встановленого на комп'ютерах 2015 року, не було належним чином ліцензовано.

Такі нелегальні копії програмного забезпечення зменшують прибуток для розвитку компаній, їхньої реклами, маркетингу та продажу (тільки для декількох областей, які отримують удар).

Ключ CRYPTO-BOX або безпосередньо підключений до ПК із захищеним додатком, або додаток може бути захищений на декількох робочих станціях за допомогою одного пристрою в мережі.

AutoCrypt забезпечує швидкий і спрощений захист додатків в Windows, Linux і macOS без необхідності використання вихідного коду чи знань у сфері програмування.

Індивідуальні стратегії ліцензування можуть бути створені й виконані для додатків за допомогою індивідуальної реалізації у вихідному коді за допомогою потужного API Smarx OS, доступного для Windows, Linux, macOS, iOS, Android та інших платформ.

До переваг ключа належать:

- надійний апаратний захист і шифрування з підтриманням затверджених стандартів шифрування AES і RSA;
- швидкий автоматичний захист, а також індивідуальна реалізація у вихідному коді;
- підтримання всіх основних компіляторів / середовища розроблення й операційних систем;
- недорогий захист кількох ліцензій у мережах;
- різні варіанти ліцензування, а саме: обмеження часу, введення окремих параметрів, віддалене оновлення ліцензій (навіть без прямого під'єднання до Інтернету);
- можливість налаштування відповідно до індивідуальних умов і вимог.

Література

1. *SOFTWARE PROTECTION AND LICENSING [Електронний ресурс] – Режим доступу: <https://www.marx.com/en/software-protection>*