МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ

ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач випускової кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Ільєнко

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ р.

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема: «Методи виявлення та організація системи захисту від кейлогерів»**

Виконавець: студент 241-М групи Янцюк Ярослав Ярославович

(студент, група, прізвище, ім’я, по-батькові)

Керівник: д.ф-м.н. проф., Оксіюк Олександр Глібович

(науковий ступінь, вчене звання, прізвище, ім’я, по-батькові)

Нормоконтролер: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Єгоров С.В

(підпис) (П.І.Б.)

**КИЇВ 2020**

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп’ютерної та програмної інженерії

Кафедра: Комп’ютеризованих систем захисту інформації

Освітній ступінь: Магістр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: 125-01 «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Янцюка Ярослава Ярославовича**

1. Тема роботи «Методи виявлення та організація системи захисту від кейлогерів»

затверджена наказом ректора від «02» жовтня 2019 № 2265/ст.

1. Термін виконання роботи: з 14.10.2019 р. по 06.02.2020 р.
2. Вихідні дані роботи: організувати систему захисту від кейлогерів та створити програмну реалізацію кейлогеру на основі циклічного опитування стану клавіатури.
3. Зміст пояснювальної записки: проведення аналізу існуючої нормативно-правової бази України. Розгляд способів реалізації кейлогерів та методів захисту від них. Створення програмної реалізації кейлогеру на основі циклічного опитування стану клавіатури. Організація системи захисту від кейлогерів.
4. Перелік обов'язкового ілюстративного матеріалу: таблиці, рисунки, графіки.
5. Календарний план-графік

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Завдання | Термін виконання | Підпис керівника |
| 1 | Уточнення постановки задачі | 14.10.2019 | *Виконано* |
| 2 | Аналіз літературних джерел |  | *Виконано* |
| 3 | Обґрунтування вибору рішення |  | *Виконано* |
| 4 | Збір інформації |  | *Виконано* |
| 5 | Аналіз даних та їх класифікація |  | *Виконано* |
| 6 | Дослідження способів реалізації кейлогерів, методів їх виявлення та видалення, аналіз методів захисту від них. |  | *Виконано* |
| 7 | Аналіз існуючих кейлогерів та антикейлогерів, вибір найбільш дієвих програмних продуктів. |  | *Виконано* |
| 8 | Створення програмної реалізації кейлогеру на основі циклічного опитування стану клавіатури |  | *Виконано* |
| 9 | Організація системи захисту від кейлогерів та програмного забезпечення моніторингового типу |  | *Виконано* |
| 9 | Оформлення і друк пояснювальної записки |  | *Виконано* |
| 10 | Оформлення презентації |  | *Виконано* |
| 11 | Отримання рецензій від опонентів |  | *Виконано* |
| 12 | Підготовка до захисту | 09.02.2020 | *Виконано* |

1. Дата видачі завдання: «02» жовтня 2019 р.

Керівник дипломної роботи: Оксіюк О.Г.

(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання*:* Янцюк Я.Я.

(підпис) (П.І.Б)

**РЕФЕРАТ**

Магістерська атестаційна робота складається зі вступу, основної частини, що містить 3 розділи, висновку, списку використаних джерел, додатків. Загальний обсяг роботи – 114 сторінок. Робота містить 43 рисунків, 3 таблиці та 2 додатки. Список бібліографічних посилань використаних джерел включає 34 джерела.

КЕЙЛОГЕР, АНАЛІЗ ДАНИХ, КЛАВІАТУРНА ПАСТКА, ФУНКЦІЯ, МОНІТОРИНГ, ЗАХИСТ ВІД КЕЙЛОГЕРІВ, ДРАЙВЕР, БІБЛІОТЕКА, ЗАХИСТ ІНФОРМАЦІЇ, ЗАХИЩЕНЕ СЕРЕДОВИЩЕ, СИСТЕМА.

Об’єкт дослідження – програми призначені для моніторингу натискання клавіш на клавіатурі та створення журналу активності користувача в системі, кейлогери.

Мета роботи - визначення найбільш дієвих способів виявлення та засобів захисту від кейлогерів, організація системи захисту від них для стаціонарних та бездротових пристроїв, забезпечення безпечного видалення кейлогерів із системи.

Метод дослідження - аналіз існуючих засобів захисту, способів виявлення шпигунського програмного забезпечення за рахунок дослідження технологій їхньої реалізації.

Наукова новизна полягає у тому, що запропонована система передбачає захист від витоку інформації про натискання клавіш на клавіатурах усіх можливих типів: стаціонарних, бездротових, сенсорних, за рахунок комплексного використання засобів захисту.

ЗМІСТ

[Вступ 8](#_Toc536478631)

[Розділ 1](#_Toc536478632). [Нормативно-правова база в сфері захисту інформації 1](#_Toc536478633)0

[1.1. Закон України «Про національну безпеку України» 1](#_Toc536478634)1

[1.2. Закон України «Про інформацію» 1](#_Toc536478635)1

[1.3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» 1](#_Toc536478636)6

[1.4. Концепція технічного захисту інформації в Україні 1](#_Toc536478637)8

[1.5. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення 22](#_Toc536478638)

[1.6. Положення про технічний захист інформації в Україні 2](#_Toc536478639)3

[1.7. НД ТЗІ 3.6-001-00 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу 25](#_Toc536478640)

[1.8. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу 26](#_Toc536478641)

[1.9. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу 27](#_Toc536478642)

[1.10. НД ТЗІ 2.5-004-99 Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу 31](#_Toc536478643)

[1.11.Висновок до розділу 34](#_Toc536478644)

[Розділ 2](#_Toc536478645). [Методи виявлення та захисту від кейлогерів 35](#_Toc536478646)

[2.1. Принцип роботи кейлогера 38](#_Toc536478647)

[2.2. Методи виявлення кейлогерів 40](#_Toc536478648)

[2.2.1.Способи реалізації кейлогерів 40](#_Toc536478649)

[2.2.1.1.Кейлогер на основі клавіатурних пасток 42](#_Toc536478650)

[2.2.1.2.Кейлогер з циклічним опитуванням стану клавіатури 43](#_Toc536478651)

[2.2.1.3.Кейлогер на базі драйверу 44](#_Toc536478652)

[2.2.1.4.Кейлогер з методом перехоплення сигналу радіоінтерфейсу 46](#_Toc536478653)

[2.2.1.5.Кейлогер на базі rootkit 47](#_Toc536478654)

[2.2.1.6.Апаратні кейлогери](#_Toc536478655) 47

[2.2.2.Пошук по сигнатурам](#_Toc536478656) 48

[2.2.3.Евристичні алгоритми](#_Toc536478657) 49

[2.2.4.Моніторинг API-функцій, що використовуються кейлогерами](#_Toc536478658) 49

[2.2.5.Відслідковування драйверів, процесів та сервісів](#_Toc536478659) 49

[2.3. Методи захисту від кейлогерів](#_Toc536478660) 49

[2.3.1.Використовування одноразових паролів/двофакторної автентифікації. 5](#_Toc536478661)2

[2.3.2.Використання систем проактивного захисту](#_Toc536478662) 53

[2.3.3.Використання віртуальних клавіатур](#_Toc536478663) 54

[2.3.4.Програмні рішення](#_Toc536478664) 55

[2.4. Рекомендації щодо захисту](#_Toc536478665) 55

[2.5. Висновки до розділу.](#_Toc536478666) 59

[Розділ 3.](#_Toc536478667) [Тестування способів виявлення та організація системи захисту від кейлогерів 6](#_Toc536478668)1

[3.1. Опис роботи кейлогера, реалізованого на основі циклічного опитування стану клавіатури. 6](#_Toc536478669)1

[3.2. Вибір кейлогерів для тестування. 6](#_Toc536478670)4

[3.3. Опис обраних кейлогерів](#_Toc536478671) 66

[3.3.1.Кейлогер WebWatcher](#_Toc536478672) 66

[3.3.1.1.Інсталяція кейлогеру](#_Toc536478673) 66

[3.2.1.2. Опис роботи кейлогеру 75](#_Toc536478674)

[3.3.2.Кейлогер Jetlogger 78](#_Toc536478675)

[3.3.2.1.Інсталяція кейлогеру 78](#_Toc536478676)

[3.3.2.1.Опис роботи кейлогеру](#_Toc536478677) 68

[3.4. Опис програмного продукту Covert для виявлення кейлогерів 7](#_Toc536478678)5

[3.5. Процес виявлення та видалення кейлогерів](#_Toc536478679) 77

[3.5.1.Кейлогер Jetlogger 77](#_Toc536478680)

[3.5.2.Кейлогер WebWatcher 8](#_Toc536478681)2

[3.5.3.Порівняння способів видалення кейлогерів 88](#_Toc536478682)

[3.6. Зняття інформації з бездротових пристроїв 89](#_Toc536478683)

[3.6.1.Опис пристрою для прийому сигналу 9](#_Toc536478684)0

[3.6.2.Принцип зняття інформації 9](#_Toc536478685)1

[3.6.3.Захист від зняття інформації бездротовим способом 96](#_Toc536478686)

[3.7. Система захисту від кейлогерів](#_Toc536478687) 97

[3.8. Висновки до розділу 10](#_Toc536478688)0

[Висновки 10](#_Toc536478689)2

[Список бібліографічних посилань використаних джерел 1](#_Toc536478689)03

[Додаток А. Фрагмент коду програми 1](#_Toc536478689)06

[Додаток Б. Фрагмент коду для декодування символів 1](#_Toc536478689)08

# ВСТУП

В умовах високого рівня розвитку інформатизації суспільства постійно розвиваються способи несанкціонованого доступу до конфіденційної інформації людини. Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, оскільки найчастіше реалізацією інформаційних загроз є збиток в політичній, військовій, економічній, соціальній, екологічній сферах і т.д.

На теперішній час число шпигунських програм зростає у вигляді тисяч кожного дня, в тому числі клавіатурних шпигунів.

Keylogger - це програма яка безпечна для системи, але небезпечна для користувачів. Ця програма дуже проста, тому сьогодні існують сотні дуже багато клавіатурних шпигунів, що не знаходяться антивірусним програмним забезпеченням.

Шпигун клавіатури не являється вірусом, але являються більшою загрозою для користувачів, оскільки дозволяє зловмисникові відстежувати роботу користувача і може використовуватися для крадіжки конфіденційної інформації, включаючи паролі користувачів. Небезпеки клавіатурного шпигуна можуть значно зрости в поєднанні з технологією RootKit, яка дозволяє маскувати присутність клавіатурного шпигуна. Ще більш небезпечним є троянець, який містить клавіатурний шпигун - його присутність значно розширює функціональність троянця і його небезпека для користувача.

На даний момент найбільша проблема в боротьбі з клавіатурними шпигунами полягає в тому, що велика кількість програм використовує натискання клавіш. Наприклад, багато програм використовують цю функцію для роботи гарячих клавіш в своєму середовищі або для перемикання розкладки клавіатури. Ідентифікація клавіатурних шпигунів - дуже проблематична завдання. Загалом, існує безліч способів реалізації клавіатурних шпигунів, але всі вони мають загальний принцип: вони вводяться в процесі передачі сигналу від натискання клавіші до появи символу на екрані пристрою.

На сьогоднішній день відомі наступні основні типи програмних клавіатурних шпигунів: засновані на пастках клавіатури, засновані на циклічному огляді стану клавіатури, засновані на драйвері. Кожен з перерахованих видів має свої проблеми з виявленням. Як тільки кейлогер виявлений, проблема стає набагато менше, так як видалення кейлогера в теперішніх умовах не є неможливим.

Мета роботи - визначення найбільш дієвих способів виявлення та засобів захисту від кейлогерів, організація системи захисту від них для стаціонарних та бездротових пристроїв, забезпечення безпечного видалення кейлогерів із системи.

Об’єкт дослідження – програми призначені для моніторингу натискання клавіш на клавіатурі та створення журналу активності користувача в системі, кейлогери.

Предмет дослідження - способи реалізації прихованої роботи кейлогерів, методи виявлення, видалення та захисту від них.

Метод дослідження - аналіз існуючих засобів захисту, способів виявлення шпигунського програмного забезпечення за рахунок дослідження технологій їхньої реалізації.

Наукова новизна полягає у тому, що запропонована система передбачає захист від витоку інформації про натискання клавіш на клавіатурах усіх можливих типів: стаціонарних, бездротових, сенсорних, за рахунок комплексного використання засобів захисту.

Під час виконання магістерської атестаційної роботи було проведено дослідження. Була опублікована наукова стаття, по темі дипломної роботи:

* + 1. Янцюк Я.Я. Методи виявлення шкідливих програм та організація захисту / Оксіюк О. Г., Янцюк Я.Я. // «Перспективні розробки науки і техніки»

# РОЗДІЛ 1

# НОРМАТИВНО-ПРАВОВА БАЗА В СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ

Питання забезпечення інформаційної безпеки сьогодні для України стоять на одному рівні із захистом суверенітету і територіальної цілісності, забезпеченням її економічної безпеки. Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз - це нанесення шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо.

За напрямом ураження, загрози інформаційній безпеці держави поділяються наступним чином:

1. Загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України.
2. Загрози інформаційному забезпеченню державної політики України.
3. Загрози розвиткові вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікацій і зв'язку.
4. Загрози безпеці інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються. [1]

* 1. Закон України «Про національну безпеку України»

Цей Закон відповідно до статей 1, 2, 17, 18 і 92 Конституції України визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз.

Цим Законом визначаються та розмежовуються повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони [2].

* 1. Закон України «Про інформацію»

Закон України «Про інформацію» закріплює право громадян України на володіння та розпорядження інформацією, встановлює сутність правових основ інформаційної діяльності та визначає правові форми міжнародного співробітництва в галузі інформації. Згідно зі змістом цього закону, інформація – це документовані або привселюдно оголошені відомості про події і явища, що відбуваються в товаристві, державі або навколишньому природному середовищі.

Закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації [4].

Відповідно до закону основними видами інформації є:

* статистична інформація;
* масова інформація;
* інформація про діяльність державних органів влади й органів місцевого і регіонального самоврядування;
* правова інформація;
* інформація про особистість;
* інформація довідково-енциклопедичного характеру; соціологічна інформація.

Основними принципами інформаційних відносин є:

* гарантованість права на інформацію;
* відкритість, доступність інформації та свобода її обміну;
* об'єктивність, вірогідність інформації;
* повнота і точність інформації;
* законність одержання, використання, поширення та зберігання інформації.

Згідно даного закону, інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. Основними напрямами інформаційної діяльності є: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо. Основними видами інформаційної діяльності є одержання, використання, поширення та зберігання інформації.

Одержання, використання, поширення та зберігання документованої або публічно оголошуваної інформації здійснюється у порядку, передбаченому цим законом та іншими законодавчими актами в галузі інформації [4].

Відомості про режими доступу до інформації та їхні особливості міститься в наведених нижче статтях.

Стаття 28. Режим доступу до інформації

Режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Держава здійснює контроль за режимом доступу до інформації. Завдання контролю за режимом доступу до інформації полягає у забезпеченні додержання вимог законодавства про інформацію всіма державними органами, підприємствами, установами та організаціями, недопущенні необґрунтованого віднесення відомостей до категорії інформації з обмеженим доступом.

Державний контроль за додержанням встановленого режиму здійснюється спеціальними органами, які визначають Верховна Рада України і Кабінет Міністрів України. У порядку контролю Верховна Рада України може вимагати від урядових установ, міністерств, відомств звіти, які містять відомості про їх діяльність по забезпеченню інформацією заінтересованих осіб (кількість випадків відмови у наданні доступу до інформації із зазначенням мотивів таких відмов; кількість та обґрунтування застосування режиму обмеженого доступу до окремих видів інформації; кількість скарг на неправомірні дії посадових осіб, які відмовили у доступі до інформації, та вжиті щодо них заходи тощо).

Стаття 29. Доступ до відкритої інформації

Доступ до відкритої інформації забезпечується шляхом:

* систематичної публікації її в офіційних друкованих виданнях (бюле-тенях, збірниках);
* поширення її засобами масової комунікації;
* безпосереднього її надання зацікавленим громадянам, державним органам та юридичним особам.

Порядок і умови надання громадянам, державним органам, юридичним особам і представникам громадськості відомостей за запитами встановлюються цим Законом або договорами (угодами), якщо надання інформації здійснюється на договірній основі. Обмеження права на одержання відкритої інформації забороняється законом.

Переважним правом на одержання інформації користуються громадяни, яким ця інформація необхідна для виконання своїх професійних обов'язків.

Стаття 30. Інформація з обмеженим доступом

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ – надано статус конфіденційної. Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначається Кабінетом Міністрів України.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до закону про цю інформацію.

Порядок обігу таємної інформації та її захисту визначається відповідними державними органами за умови додержання вимог, встановлених цим Законом. Порядок і терміни обнародування таємної інформації визначаються відповідним законом.

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист.

Стаття 38. Право власності на інформацію

Право власності на інформацію - це врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією.

Інформація є об'єктом права власності громадян, організацій (юридичних осіб) і держави. Інформація може бути об'єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження.

Власник інформації щодо об'єктів своєї власності має право здійснювати будь-які законні дії.

Підставами виникнення права власності на інформацію є:

* створення інформації своїми силами і за свій рахунок;
* договір на створення інформації;
* договір, що містить умови переходу права власності на інформацію до іншої особи.

Інформація, створена кількома громадянами або юридичними особами, є колективною власністю її творців. Порядок і правила користування такою власністю визначаються договором, укладеним між співвласниками.

Інформація, створена організаціями (юридичними особами) або придбана ними іншим законним способом, є власністю цих організацій.

Інформація, створена на кошти державного бюджету, є державною власністю. Інформацію, створену на правах індивідуальної власності, може бути віднесено до державної власності у випадках передачі її на зберігання у відповідні банки даних, фонди або архіви на договірній основі.

Власник інформації має право призначати особу, яка здійснює володіння, використання і розпорядження інформацією, і визначати правила обробки інформації та доступ до неї, а також встановлювати інші умови щодо інформації [4].

* 1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

Закон визначає п'ять основних видів несанкціонованих дій з інформацією:

1. блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;
2. виток інформації - результат дій, внаслідок яких інформація в системі стає відомою або доступною фізичним та/або юридичним особам, що не мають права доступу до неї;
3. знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;
4. порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її зміст.

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації.

Порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її власника в порядку, встановленому законом.

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Стаття 9. Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє уповноважений орган у сфері захисту інформації [5].

* 1. Концепція технічного захисту інформації в Україні

Ця концепція визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами. Технічний захист інформації є складовою частиною забезпечення національної безпеки України. Зростання загроз для інформації, спричинене лібералізацією суспільних та міждержавних відносин, кризовим станом економіки, застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва, поширенням засобів несанкціонованого доступу до інформації та впливу на неї, визначає необхідність розвитку ТЗІ.

Напрями розвитку ТЗІ обумовлюються необхідністю своєчасного вжиття заходів, адекватних масштабам загроз для інформації, і ґрунтуються на засадах правової демократичної держави відповідно до прав суб'єктів інформаційних відносин на доступ до інформації та її захист.

Напрями розвитку ТЗІ обумовлюються необхідністю своєчасного вжиття заходів, адекватних масштабам загроз для інформації, і ґрунтуються на засадах правової демократичної держави відповідно до прав суб'єктів інформаційних відносин на доступ до інформації та її захист.

Приведення інформаційних відносин у сфері ТЗІ у відповідність з міжнародними стандартами сприятиме утвердженню України у світі як демократичної правової держави.

Впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій зумовило поширення великих масивів інформації в обчислювальних та інформаційних мережах на значних територіях. За відсутності вітчизняних конкурентоспроможних інформаційних технологій надається перевага технічним засобам оброблення інформації та засобам зв'язку іноземного та спільного виробництва, які здебільшого не забезпечують захист інформації. Комунікаційне обладнання іноземного виробництва, яке використовується у мережах зв'язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв'язку та змістом повідомлень, які пересилаються.

Прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна легко підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо-, радіотехнічної, оптико-електронної, радіотеплової, акустичної, хімічної, магнітометричної, сейсмічної та радіаційної розвідок.

За таких умов створилися можливості витоку інформації, порушення її цілісності та блокування. Витік інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, – це одна з основних можливих загроз національній безпеці України в інформаційній сфері. Загрози безпеці інформації в Україні зумовлені:

* невиваженістю державної політики в галузі інформаційних технологій, що може призвести до безконтрольного та неправомочного доступу до інформації та її використання;
* діяльністю інших держав, спрямованою на одержання переваги в зовнішньополітичній, економічній, військовій та інших сферах;
* недосконалістю організації в Україні міжнародних виставок апаратури різного призначення (особливо пересувних) та заходів екологічного моніторингу, що може використовуватися для здобування інформації розвідувального характеру;
* діяльністю політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, спрямованою на одержання переваги у політичній боротьбі та конкуренції;
* злочинною діяльністю, спрямованою на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;
* використанням інформаційних технологій низького рівня, що приз-водить до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ та засобів ТЗІ;
* недостатністю документації на засоби забезпечення ТЗІ іноземного виробництва, а також низькою кваліфікацією технічного персоналу у сфері ТЗІ.

Принципами формування і проведення державної політики у сфері ТЗІ є:

* додержання балансу інтересів особи, суспільства та держави, їх взаємна відповідальність;
* єдність підходів до забезпечення ТЗІ, які визначаються загрозами безпеці інформації та режимом доступу до неї;
* комплексність, повнота та безперервність заходів ТЗІ;
* відкритість нормативно-правових актів та нормативних документів з питань ТЗІ, які не містять відомостей, що становлять державну таємницю;
* узгодженість нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України;
* обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях;
* виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту конфіденційної інформації, що не належить державі, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами державних органів, підприємств, установ і організацій;
* покладення відповідальності за формування та реалізацію державної політики у сфері ТЗІ на спеціально уповноважений центральний орган виконавчої влади;
* ієрархічність побудови організаційних структур системи ТЗІ та керівництво їх діяльністю у межах повноважень, визначених нормативно-правовими актами;
* методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;
* скоординованість дій та розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки.

Державна політика у сфері ТЗІ визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз для інформації та здійснюється шляхом виконання положень цієї Концепції, а також програм розвитку ТЗІ та окремих проектів [6].

* 1. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення

Цей стандарт установлює об’єкт, мету, основні організаційно-технічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ.

Джерелами загроз може бути діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб.

Загрози можуть здійснюватися:

* технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;
* каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;
* несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Заходи захисту інформації повинні:

* бути відповідними загрозам;
* бути розробленими з урахуванням можливої шкоди від їх реалізації і вартості захисних заходів та обмежень, що вносяться ними;
* забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

Нормативні документи розробляються в ході проведення комплексу робіт із стандартизації та нормування у галузі ТЗІ. Вони повинні забезпечувати:

* проведення єдиної технічної політики;
* створення і розвиток єдиної термінологічної системи;
* функціювання багаторівневих систем захисту інформації на основі взаємнопогоджених положень, правил, методик, вимог та норм;
* функціювання систем сертифікації, ліцензування й атестації згідно з вимогами безпеки інформації;
* розвиток сфери послуг у галузі ТЗІ;
* установлення порядку розроблення, виготовлення, експлуатації засобів забезпечення ТЗІ та спеціальної контрольно-вимірювальної апаратури;
* організацію проектування будівельних робіт у частині забезпечення ТЗІ;
* підготовку та перепідготовку кадрів у системі ТЗІ [7].
  1. Положення про технічний захист інформації в Україні

Це Положення визначає правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства.

Технічний захист інформації здійснюється щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ, організації.

Матеріально-технічна база системи технічного захисту інформації складається з технічних засобів загального призначення та спеціальних технічних засобів. Технічні засоби загального призначення повинні мати документ, що засвідчує їх відповідність вимогам нормативно-правових актів з технічного захисту інформації, одержаний у порядку, що встановлюється Адміністрацією Держспецзв'язку України і Державним комітетом України з питань технічного регулювання та споживчої політики.

Техніко-економічне обґрунтування, проектування будівництва та реконструкції об'єктів, проведення наукових досліджень та створення інформаційних систем, зразків озброєнь, військової та спеціальної техніки, критичних і небезпечних технологій виконуються за завданнями, до яких включаються вимоги з технічного захисту інформації, якщо під час виконання передбачених завданням робіт та у процесі функціонування зазначених об'єктів, систем, зразків і технологій циркулюватиме інформація, охорона якої забезпечується державою.

Під час віднесення замовником таких робіт до особливо важливих та створення інформаційних систем державних органів завдання та результати приймання їх етапів погоджуються з Адміністрацією Держспецзв'язку України. Фінансування створення цих систем здійснюється після такого погодження. Оцінювання захищеності інформації здійснюється шляхом атестації або експертизи комплексів технічного захисту інформації та інспекційних перевірок. За результатами атестації або експертизи комплексів технічного захисту інформації визначається можливість введення в експлуатацію об'єкта, де циркулюватиме інформація, охорона якої забезпечується державою.

Розроблення, впровадження, атестація та експлуатація комплексів технічного захисту інформації для власних потреб здійснюються відповідними підрозділами органів, щодо яких здійснюється ТЗІ, або військовими частинами, підприємствами, установами, організаціями, на які в установленому порядку покладено забезпечення технічного захисту інформації, за наявності у них відповідного дозволу.

До виконання цих робіт можуть бути залучені суб'єкти підприємницької діяльності, що мають відповідні ліцензії.

Результати атестації на державних об'єктах, віднесених замовником до особливо важливих, погоджуються з Адміністрацією Держспецзв'язку України [8].

* 1. НД ТЗІ 3.6-001-00 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу

Цей нормативний документ (НД ТЗІ) встановлює єдині вимоги до порядку створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу (НСД) в комп’ютерних системах та захищених від несанкціонованого доступу компонентів обчислювальних систем.

Дія НД ТЗІ поширюється на апаратні, програмні та програмно-апаратні засоби ТЗІ, призначені для використання в комп’ютерних системах, де обробляється, накопичується, зберігається та передається інформація, що підлягає технічному захисту.

НД ТЗІ призначений для розробників та виробників (впроваджувальних організацій), споживачів (замовників, користувачів) засобів ТЗІ, а також для органів, що здійснюють функції оцінювання засобів ТЗІ на відповідність вимогам НД ТЗІ.

Згідно з Положенням про технічний захист інформації в Україні в КС, де обробляється інформація, яка є власністю держави або захист якої гарантується державою, повинні використовуватись засоби ТЗІ, які мають документ, що засвідчує їх відповідність вимогам нормативних документів з питань технічного захисту інформації (експертний висновок та/або сертифікат відповідності). Засоби криптографічних перетворень, які є складовою частиною засобів ТЗІ, повинні відповідати вимогам нормативних документів з питань криптографічного захисту інформації. Модернізація засобів ТЗІ в комп’ютерних системах здійснюється у відповідності з окремим ТЗ або доповненням до основного ТЗ на створення засобу ТЗІ. ТЗ (доповнення до основного ТЗ) розробляється та оформляється відповідно до чинних ДСТУ з урахуванням вимог НД ТЗІ 3.7-001-99 [9].

* 1. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу

Цей документ установлює терміни і визначення понять у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

Обчислювальна система; ОС (computer system) – сукупність програмних-апаратних засобів, призначених для обробки інформації.

Комплексна система захисту інформації; КСЗІ – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Доступ до інформації (access to information ) – вид взаємодії двох об’єктів КС, внаслідок якого створюється потік інформації від одного об’єкта до іншого і/або відбувається зміна стану системи.

Захист від несанкціонованого доступу; захист від НСД (protection from unauthorized access) – запобігання або істотне ускладнення несанкціонованого доступу до інформації.

Комп’ютерний вірус (computer virus) – програма, що володіє здатністю до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування КС і/або зумовити порушення політики безпеки.

Програмна закладка (program bug) – таємно впроваджена програма або недокументовані властивості програмного забезпечення, використання яких може призвести до обходу КЗЗ і/або порушення політики безпеки.

Визначення властивостей інформації:

Конфіденційність інформації (information confidentiality) – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

Цілісність інформації (information integrity) – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

Доступність (availability) – властивість ресурсу системи (КС, послуги, об’єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Спостереженість (accountability) – властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії [10].

* 1. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

Цей нормативний документ технічного захисту інформації (НД ТЗІ) визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:

* визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;
* створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;
* оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів. Впливи, які призводять до зниження цінності інформаційних ресурсів, називаються несприятливими. Потенційно можливий несприятливий вплив називається загрозою.

Захист інформації, що обробляється в АС, полягає в створенні і підтримці в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Іншими словами, захист інформації спрямовано на забезпечення безпеки оброблюваної інформації і АС в цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації і АС, що її обробляє. Система зазначених заходів, що забезпечує захист інформації в АС, називається комплексною системою захисту інформації.

Істотна частина проблем забезпечення захисту інформації в АС може бути вирішена організаційними заходами. Проте, з розвитком інформаційних технологій спостерігається тенденція зростання потреби застосування технічних заходів і засобів захисту.

Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення). Інформація зберігає доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу. Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації. Кінцевою метою всіх заходів щодо захисту інформації, які реалізуються, є забезпечення безпеки інформації під час її обробки в АС. Захист інформації повинен забезпечуватись на всіх стадіях життєвого циклу АС, на всіх технологічних етапах обробки інформації і в усіх режимах функціонування. Життєвий цикл АС включає розробку, впровадження, експлуатацію та виведення з експлуатації.

Інформація в КС існує у вигляді даних, тобто представляється в формалiзованому вигляді, придатному для обробки. Під обробкою слід розуміти як власне обробку, так і введення, виведення, зберігання, передачу і т. ін. Інформація для свого існування завжди вимагає наявності носiя. Як носiй інформації може виступати поле або речовина. В деяких випадках у вигляді носiя інформації може розглядатися людина. Втрата інформацією своєї цінності (порушення безпеки інформації) може статися внаслідок переміщення інформації або зміни фізичних властивостей носiя.

При аналізі проблеми захисту від НСД інформації, яка може циркулювати в системі, як правило, розглядаються лише інформаційні об'єкти, що служать приймальниками/джерелами інформації, і інформаційні потоки (порції інформації, що пересилаються між об'єктами) безвідносно до фізичних характеристик їх носiїв.

Із всієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації.

Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікацiї (видалення). Інформація зберігає доступність, якщо зберігається можливість ознайомлення з нею або її модифікацiї відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу. Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації.

Створення додаткових потоків інформації може бути зумовлене: модифікацією атрибутів доступу користувача, процесу або пасивного об'єкта; створенням нових об'єктів (включаючи копіювання існуючих); експортом або імпортом об'єктів.

Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін «політика безпеки» може бути застосовано щодо організації, АС, ОС, послуги, що реалізується системою (набору функцій), і т. ін. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальніше стають правила. Далі для скорочення замість словосполучення «політика безпеки інформації» може використовуватись словосполучення «політика безпеки», а замість словосполучення «політика безпеки інформації, що реалізується послугою» — «політика послуги» і т. ін.

Політика безпеки інформації в АС є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації. Для кожної АС політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама АС може реалiзувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій АС буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси АС, що потребують за-хисту, зокрема установлювати категорії інформації, оброблюваної в АС. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз.

Як складові частини загальної політики безпеки інформації в АС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Відповідальність персоналу за виконання положень політики безпеки має бути персонiфікована.

Політика безпеки інформації, що реалізуються різними КС будуть відрізнятися не тільки тим, що реалізовані в них функції захисту можуть забезпечувати захист від різних типів загроз, але і в зв'язку з тим, що ресурси КС можуть істотно відрізнятись. Так, якщо операційна система оперує файлами, то СУБД має справу із записами, розподіленими в різних файлах.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступу.

Під НСД слід розуміти доступ до інформації з використанням засобів, включених до складу КС, що порушує встановлені ПРД.

Несанкціонований доступ може здійснюватися як з використанням штатних засобів, тобто сукупності програмно-апаратного забезпечення, включеного до складу КС розробником під час розробки або системним адміністратором в про-цесі експлуатації, що входять у затверджену конфігурацію КС, так і з використанням програмно-апаратних засобів, включених до складу КС зловмисником.

До основних способів НСД відносяться:

* безпосереднє звертання до об'єктів з метою одержання певного виду доступу;
* створення програмно-апаратних засобів, що виконують звертання до об'єктів в обхід засобів захисту;
* модифікація засобів захисту, що дозволяє здійснити НСД;
* впровадження в КС програмних або апаратних механізмів, що порушують структуру і функції КС і дозволяють здійснити НСД [11].
  1. НД ТЗІ 2.5-004-99 Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу

Цей нормативний документ — установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

Критерії надають:

* порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах;
* базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

* вимоги до функцій захисту (послуг безпеки);
* вимоги до гарантій.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги треба шукати в розділі “Критерії конфіденційності”. В цьому розділі описані такі послуги (в дужках наведені умовні позначення для кожної послуги): довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні (експорті/імпорті).

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі “Критерії цілісності”. В цьому розділі описані такі послуги: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги треба шукати у розділі “Критерії спостереженості”.

Результатом оцінки є рейтинг, що являє собою упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Комбінації упорядковуються в порядку опису послуг в критеріях. Для того, щоб до рейтингу комп'ютерної системи міг бути включений певний рівень послуги чи гарантій, повинні бути виконані всі вимоги, перелічені в критеріях для даного рівня послуги або гарантій.

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної КС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації).

Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, цей документ містить критерії гарантій, що дозволяють оцінити коректність реалізації послуг.

Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. В цих Критеріях вводиться сім рівнів гарантій (Г-1, ..., Г-7), які є ієрархічними.

Ієрархія рівнів гарантій відбиває поступово наростаючу міру певності в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи [12].

* 1. Висновок до розділу

В даному розділі дипломної роботи було викладені основні правові положення у сфері захисту інформації.

Розглянуто Закони України пов’язані з темою дипломної роботи "Про основи національної безпеки", "Про інформацію", "Про захист інформації в інформаційно-комунікаційних системах",

Проаналізувавши дані можна сказати, що у галузі інформаційної безпеки законодавство України регулює широке коло питань та проблем. В описаних нормативних документах, заходи захисту інформації передбачають усі можливі типи інформаційних загроз, розроблені з урахуванням можливої ​​шкоди від їх реалізації та вартості заходів та обмежень безпеки, забезпечують необхідну ефективність захисту інформації на встановлених рівенях за необхідний проміжок часу.

# РОЗДІЛ 2

# МЕТОДИ ВИЯВЛЕННЯ ТА ЗАХИСТУ ВІД КЕЙЛОГЕРІВ

Кейлогер - це програмне забезпечення або апаратний пристрій, що реєструє різні дії користувача - натискання клавіш на клавіатурі комп'ютера, руху і натиснення клавіш миші і т. д. Належить він до небезпечного програмного забезпечення типу spyware. На даний час великою проблемою боротьби з кейлогерами є велика кількість програм використовує перехоплення натискань клавіш

Видалення кейлогерів є досить складною проблемою, враховуючи, що їх сьогодні дуже багато. Метод пошуку кейлогерів безпосередньо залежить від способу його здійснення та, відповідно, від технології відстеження клавіатури.

В теперішній час багато кейлогерів не тільки записують натискання клавіш, а також і закріпляють натискання клавіатури до певного вікна, з певною частотою робити знімки екрана; слідкувати за вмістом буфера обміну, запущені додатки та програми, підключати носії та генерувати звіти, які містять інформацію та надсилаються електронною поштою або через протоколи призначення ftp / http призначення.

В останні роки видно швидке збільшення кількості шкідливого програмного забезпечення, які мають функції кейлогера. Дослідницький документ проводився під час написання дипломної роботи, і кількісне збільшення відомих кейлогерів було виявлено щороку з 2003 року. Зверніть увагу, дані є приближеними, так як неможна оцінити ступінь програмного забезпечення, яке ще не було виявлено. Статистика показана у вигляді графіка на рисунку. 1.1. Судячи з даних, можна вирішити, що кейлогери є поширеним засобом несанкціонованого видалення інформації, що швидко набирає популярність. Таким чином, за останні два роки кількість відомих кейлогерів збільшилась більш ніж удвічі, що вимагало втручання у розробку нових систем безпеки проти них.

Рис. 2.1. Кількість кейлогерів, що з'явилися за останні десятиліття

Метод використання кейлогерів (включаючи апаратні чи програмні продукти, що включають кейлогери як модуль) дає можливість побачити межу між порушеннями безпеки та управлінням безпекою.

Несанкціоноване використання - установка кейлогера відбувається без відома власника (адміністратора безпеки) автоматизованої системи або без відома власника конкретного персонального комп'ютера . Несанкціоновані використовувані кейлогери (програмне чи апаратне забезпечення) називаються шпигунськими або шпигунськими програмами. Самовільне використання зазвичай пов’язане з незаконною діяльністю. Зазвичай несанкціоноване встановлене шпигунське програмне забезпечення має можливість конфігурувати та отримувати пакетний виконуваний файл, який під час встановлення не відображає жодних повідомлень та не створює вікон на екрані, а також має вбудовані засоби доставки та віддаленої установки для комп'ютера користувача , тобто установка процесу відбувається без прямого фізичного доступу до комп'ютера користувача і часто не потребує привілеїв системного адміністратора.

Санкціоноване використання - установка кейлогера проходить з дозволу власника (адміністратора безпеки) автоматизованої системи або від власника певного персонального комп'ютера. Авторизовані кейлогери (програмне чи апаратне забезпечення) називають програмним забезпеченням для моніторингу (програмне забезпечення для моніторингу працівників, програмне забезпечення батьківського контролю, програмне забезпечення контролю доступу, програми особистої безпеки тощо). Як правило, авторизовані програмні продукти потребують фізичного доступу до комп'ютерів. Користувач і адміністратор вимагають прав на конфігурацію та встановлення.

Санкціоноване застосування кейлогерів дозволяє власникові (адміністраторові безпеки) автоматизованої системи або власникові комп'ютера:

* виявити всі випадки набору на клавіатурі критичних слів і фраз, передача яких завдасть матеріальної шкоди третім особам;
* мати можливість доступу до інформації, що зберігається на жорсткому диску комп'ютера, в разі втрати логіна та пароля по будь-якої причини (хвороба працівника, умисні дії персоналу і т. д.);
* ідентифікувати (локалізувати) всі випадки спроб доступу до паролю;
* контролювати можливість використання персональних комп'ютерів в неробочий час і дізнаватися, що друкувалося на клавіатурі в кожен конкретний момент;
* розслідувати комп'ютерні інциденти;
* проводити наукові дослідження, пов'язані з визначенням точності, оперативності і адекватності реагування персоналу на зовнішні впливи;
* відновити важливу інформацію після збою комп'ютерних систем.

Використання модулів, які включають кейлогер розробниками комерційного програмного забезпечення дозволяє останнім:

* створювати системи швидкого пошуку слів (електронні словники, електронні перекладачі);
* створювати програми для швидкого пошуку по іменах, компаніям, адресами (електронні книги)

Несанкціоноване використання клавіатурних шпигунів дозволяє зловмисникові:

* перехоплення чужої інформації на клавіатурі;
* отримувати несанкціонований доступ до логінів і паролів в різних системах, в тому числі в системах «банк-клієнт»;
* отримати несанкціонований доступ до систем криптографічного захисту інформації користувача комп'ютера - пральних фраз;
* отримати несанкціонований доступ до інформації авторизації кредитної картки [13].

## Принцип роботи кейлогера

Клавіатурні пастки (так звані "хукі")

У середовищі Windows хук означає перехоплення системних повідомлень за допомогою програмного механізму Win32Api. Для більшості клавіатурних шпигунів за основу береться хук WH\_Keyboard, іноді - WH\_JOURNALRECORD. Різниця в тому, що в другому випадку немає залежності від динамічних бібліотек (DLL).

Опитування стану клавіатури

Досить простий спосіб, що не вимагає впровадження програми в графічний інтерфейс системи, однак, має серйозний недолік - ресурсомісткість. Цей недолік призводить до спрацьовування антивірусного і антишпигунського ПО.

Кейлогери на базі драйвера

Сенс методу в тому, щоб впровадити захоплення натискання клавіш прямо в драйвер клавіатури.

Rootkit-шпигуни

Впроваджуються в процес csrss.exe і перехоплюють усі дані при обміні між клавіатурою і цим самим процесом. У більшості випадків, від кейлогеров такого типу не може захистити навіть екранна клавіатура Windows, яку всі рекомендують використовувати для захисту від крадіжки даних [32].

Графічно схему роботи кейлогера зображено на Рис. 2. 2.

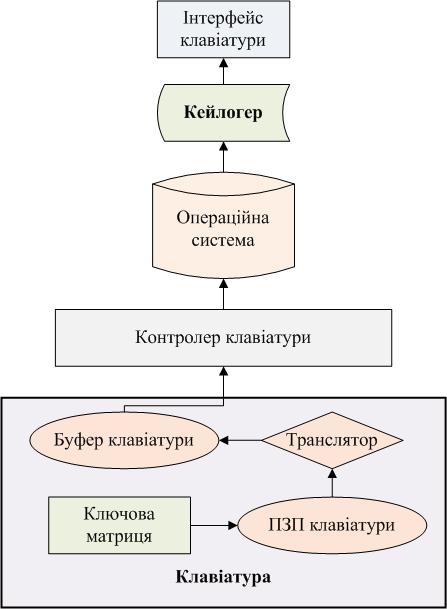


Рис. 2. 2. Схема роботи кейлогера

## Методи виявлення кейлогерів

На теперішній час, знаходження кейлогерів є дуже проблемним завданням. Так як антивірусне програмне забезпечення не визначає його як вірус або троянське програмне забезпечення, тому багато захисних програм, які не мають розширеної бази даних та модулів, не розглядають кейлогери як шкідливі програми.

Шукаючи кейлоггери, вам потрібно врахувати ряд їх особливостей:

1. програми цього типу завантажуються під час входу, тобто вони можуть бути прив’язані до захищеного додатку (як віруси), який ігнорується антивірусним інструментом;
2. час від часу аналізувати поточний стан клавіатури;
3. отримана інформація (журнали) певним чином надсилається зловмиснику або зберігається на диску. Тому система постійно контролюється, а тимчасовий буфер час від часу містить велику кількість інформації, і лише після її заповнення вона завантажується на диск [14].

### Способи реалізації кейлогерів

Способів реалізації кейлогерів є багато, вони поділяють загальний принцип: вони вводяться в процесі передачі сигналу від натискання клавіші до появи символу на екрані пристрою.

Поділяються на програмні та апаратні засоби.

Програмні кейлогери належать до групи програмних продуктів, які контролюють діяльність користувача ПК. Спочатку цей тип програмного забезпечення призначався виключно для запису інформації про натискання клавіш на клавіатурі, включаючи системні натискання клавіш, у спеціалізований журнал (файл журналу), який згодом вивчався особою, яка встановила програму. Файл журналу можна надсилати через мережу на мережевий диск, на FTP-сервер в Інтернеті, електронною поштою тощо. На сьогодні програмні продукти, які зберегли це ім'я, виконують багато додаткових функцій - він перехоплює інформацію з Windows, перехоплює кліки миша, захоплення буфера обміну, знімки скріншотів та активних вікон, відстеження всієї отриманої та відправленої електронної пошти, активність файлів моніторингу, реєстр системи моніторингу, черга завдань моніторингу, надіслана на принтер, захоплення аудіо з мікрофона та відео веб-камери, підключеної до комп’ютер тощо. е., що вони фактично належать до зовсім іншого класу програмного забезпечення, а саме програмного забезпечення для моніторингу.

Апаратні кейлогери - це мініатюрні пристрої, які можна підключити між клавіатурою та комп'ютером або інтегрувати в саму клавіатуру. Вони записують усі натискання клавіш, зроблені на клавіатурі. Процес реєстрації абсолютно непомітний для кінцевого користувача. Апаратні кейлогери не вимагають, щоб на комп'ютері була встановлена ​​будь-яка програма для успішного перехоплення всіх натискань клавіш. Якщо приєднаний апаратний кейлогер, не має значення, у якому стані комп'ютер увімкнено чи вимкнено. Час його роботи не обмежений, оскільки для його роботи не потрібно додаткового джерела живлення [15].

За місцем зберігання Log файлу

* жорсткий диск
* пам'ять
* реєстр
* розшарений, тобто загальнодоступний (shared) мережевий диск

За методом відправки Log файлу

* e-mail
* ftp
* http (https)
* будь-який варіант бездротового зв'язку (радіодіапазон, інфрачервоний діапазон, Bluetooth, Wi-fi і тому подібне)

На сьогоднішній день відомі такі основні типи програмних кейлогерів:

* на основі пасток клавіатури;
* на основі огляду циклу клавіатури;
* на основі водія;
* Кейлогери, що перехоплюють сигнал, що передається через радіоінтерфейс пристрою.

Вище приведені методи реалізації кейлогерів доста відомі. Новим методом, є радіоперехоплення пристрою через велику кількість використовуваних радіостанцій та пристроїв Bluetooth. Бездротові технології, такі як клавіатури, миші та навушники - це поширена технологія передачі інформації по радіо. Пристрої використовуються для зчитування електронних цифрових підписів, які ідентифікують людину за сигналом [33].

На рисунку 2.3 зображено відсоткове розподілення цих типів в існуючих реалізаціях.

Рис. 2. 3. Розподілення типів кейлогерів

#### Кейлогер на основі клавіатурних пасток

Дана методика є класичною для клавіатурних шпигунів, а суть її полягає в застосуванні механізму пасток (hook) операційної системи. Пастки дозволяють спостерігати за повідомленнями, які обробляються вікнами інших програм. Установка і видалення пасток виробляються за допомогою добре документованих функцій бібліотеки user32.dll (функція SetWindowsHookEx дозволяє встановити пастку, UnhookWindowsHookEx - зняти її). При установці пастки вказується тип повідомлень, для яких повинен викликатися обробник пастки. Зокрема, існує два спеціальних типи пасток: WH\_KEYBOARD і WH\_MOUSE - для реєстрації подій клавіатури і миші відповідно. Пастка може бути встановлена ​​для заданого потоку і для всіх потоків системи, причому останнє дуже зручно для побудови клавіатурного шпигуна.

Код обробника подій пастки повинен бути розташований в DLL. Ця вимога пов'язана з тим, що DLL з обробником пастки проектується системою в адресний простір всіх GUI1-процесів. Цікавою особливістю є те, що проектування DLL відбувається не в момент установки пастки, а при отриманні GUI-процесом першого повідомлення, що задовольняє параметрам пастки.

На доданому до журналу компакт-диску є демонстраційний клавіатурний шпигун, побудований на основі пастки. Він реєструє клавіатурний введення у всіх GUI-додатках і дублює текст, що вводиться на своєму вікні. Даний приклад можна використовувати для тестування програм, які протидіють клавіатурним шпигунам.

Методика пасток вельми проста і ефективна, але у неї є ряд недоліків. Одним з них можна вважати те, що DLL з пасткою проектується в адресний простір всіх GUI-процесів, що може застосовуватися для виявлення клавіатурного шпигуна. Крім того, реєстрація подій клавіатури можлива тільки для GUI-додатків - це легко перевірити за допомогою демонстраційної програми [34].

#### Кейлогер з циклічним опитуванням стану клавіатури

Дана методика заснована на періодичному опитуванні стану клавіатури. Для опитування стану клавіш в системі передбачена спеціальна функція GetKeyboardState, що повертає масив з 255 байт, в якому кожен байт містить стан певної клавіші на клавіатурі. Даний метод вже не вимагає впровадження DLL в GUI процеси і в результаті шпигун менш помітний.

Однак зміна статусу клавіш відбувається в момент зчитування потоком клавіатурних повідомлень з його черги, і в результаті подібна методика працює тільки для стеження за GUI додатками. Від цього недоліку вільна функція GetAsyncKeyState, що повертає стан клавіші на момент виклику функції.

На компакт-диску є демонстраційний «клавіатурний шпигун», побудований на основі циклічного опитування клавіатури - додаток KD2.

Недоліком клавіатурних шпигунів такого типу є необхідність періодичного опитування стану клавіатури з досить високою швидкістю, не менше 10-20 опитувань в секунду [34].

#### Кейлогер на базі драйверу

Цей метод навіть більш ефективний, ніж описані вище. Існує як мінімум два варіанти реалізації цього методу - написання і установка драйвера клавіатури в систему замість звичайного або установка драйвера фільтра. Використання драйвера фільтра, на нашу думку, є найбільш правильним методом.

Фільтр драйверів

Робота клавіатурних шпигунів цього типу заснована на установці драйвера, який підключається до драйверу клавіатури в якості фільтра. Приклад реалізації фільтра клавіатури представлений в DDK, і цей шпигун є одним з найпростіших з точки зору реалізації та виявлення.

Цей тип кейлогер може бути побудований одним з двох способів:

Фільтр драйвера в поєднанні з керуючим додатком, яке встановлює, завантажує і налаштовує драйвер. Драйвер передає інформацію про натиснутих клавішах в управління додаток, яке обробляє і реєструє одержані дані;

Повністю автономний драйвер самостійно записує події. В цьому випадку вам потрібно тільки виконати початкову установку драйвера в системі, після чого додаток, яке встановило драйвер, може самознищитися. Рішення також можливо без додатка-установника - в цьому випадку драйвер встановлюється з використанням файлу INF.

Під час завантаження драйвер повинен підключитися до стека драйверів клавіатури за допомогою функцій IoCreateDevice і IoAttachDevice. У більшості відомих реалізацій фільтр підключений до стека пристроїв «\\ Device \\ KeyboardClass0», який є драйвером класу і реалізує загальні функціональні можливості для клавіатур різних типів.

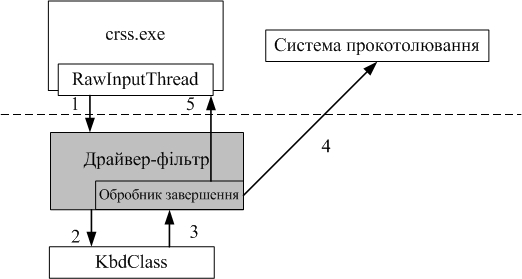


Рис. 2. 4.Загальна функціональність для клавіатур різних типів

Для клавіатурного шпигуна не матимуть значення переривання типу IRP\_MJ\_READ, оскільки на основі їх аналізу можна отримати коди клавіш. Джерелом цих IRP-запитів є процес csrss.exe, а точніше - що належить цьому процесу потік необробленого введення RawInputThread. Посилається цим потоком переривання спочатку потрапляє до драйверу-фільтру шпигуна (крок 1), який встановлює свій обробник завершення за допомогою функції IoSetCompletionRoutine і передає IRP драйверу Kbdclass (крок 2). Той, в свою чергу, позначає IRP як очікує завершення і ставить в чергу. При виникненні клавіатурних подій Kbdclass витягує з черги очікує завершення IRP, вносить в його буфер інформацію про натиснутих клавішах і завершує IRP. А оскільки в IRP встановлений адреса обробника завершення, то буде проведений виклик цього обробника (крок 3). Оброблювач може проаналізувати вміст буфера і передати міститься там інформацію системі протоколювання (крок 4). Далі IRP повертається в потік RawInputThread, а потім весь процес повторюється. Природно, що наявність коректно написаного драйвера-фільтра ніяк не позначається на роботі додатків і забезпечує глобальний перехоплення клавіатурного введення.

Виявлення описаного шпигуна не представляє особливої ​​складності, - для його пошуку досить вивчити стек клавіатурного драйвера на предмет наявності невпізнаних драйверів-фільтрів.

Підміна драйвера клавіатури

Даний метод в дійсності заснований на підміні драйвера Kbdclass або одного з низькорівневих драйверів клавіатури драйвером власної розробки. Складність реалізації зазначеного методу полягає в тому, що заздалегідь невідомий тип застосовуваної користувачем клавіатури, а тому підміну драйвера порівняно просто виявити. Внаслідок цього подібний метод практично не зустрічається [18].

#### Кейлогер з методом перехоплення сигналу по радіоінтерфейсу

Останнім часом поняття кейлогерів дещо розширилося, і до цієї категорії почали віднести програмне забезпечення для зчитування інформації з таких популярних пристроїв, як Bluetooth-передавачі, клавіатури та миші, які працюють, передаючи сигнал через радіоінтерфейс.

Також швидкими темпами розвивається система управління будинком під назвою розумний дім. Його суть полягає в забезпеченні безпеки, збереження ресурсів та комфорту для всіх своїх користувачів. Всі пристрої в будинку підключені один до одного бездротово, тобто вся інформація про їх взаємодію зберігається в одному сховищі. Доступ до цієї інформації обмежений паролями та біометричними системами розпізнавання обличчя.

Звичайно, система захисту даних для користувачів розумних будинків є досить надійною на цьому етапі свого розвитку, але відомі також випадки незаконного викрадення інформації з цих систем, тому твердження про стовідсоткову безпеку цих пристроїв є помилковим. .

#### Кейлогер на базі rootkit

Rootkit - це технологія, яка включає набір програмних засобів, які допомагають маскувати об’єкти, керувати ними та збирати системні дані. Кейлоггери такого типу не можуть бути виявлені анти-кейлоггерами. Вони можуть перехоплювати інформацію, введену навіть на екранній клавіатурі, коли вони читають інформацію про події клавіатури через повідомлення Windows. Такий кейлоггер можна протиставити лише анти-руткітом. Визначення засноване на аналізі можливостей обміну повідомленнями бібліотеки user32.dll.

Існує два типи технологій руткітів, які використовуються кейлоггерами:

* використання методів приховування режиму користувача;
* з використанням методів приховування ядра ОС.

Принцип використання шпигунських програм на основі rootkit в режимі користувача досить простий: за допомогою будь-якої з відомих технологій rootkit перехоплюється одна або кілька функцій для отримання контролю над інформацією, що вводиться з клавіатури. Найпростіше - перехопити функції GetMessage та PeekMessage (Рис. 2. 5)

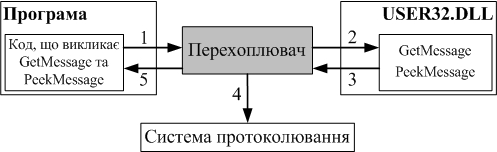


Рис. 2. 5. Перехоплення функцій GetMessage та PeekMessage

Робота шпигуна організована так. Додаток викликає функцію PeekMessage, щоб перевірити, чи є повідомлення вказаного типу в черзі. Цей виклик перехоплюється за принципом руткіта (техніка в цьому випадку не має значення). Потім перехоплювач викликає реальну функцію PeekMessage від user32.dll і аналізує повернуті результати. Якщо функція повертає значення true, це означає, що повідомлення було поставлено в чергу і що воно було вилучене в буфер, до якого передається покажчик як перший параметр функції. У цьому випадку перехоплювач перевіряє повідомлення в буфері для виявлення повідомлень типу WM\_KEYDOWN (натискання клавіші), WM\_KEYUP (випуск ключа), WM\_CHAR (надіслане вікно після обробки WM\_KEYDOWN за допомогою TranslateMessage). Якщо ви знайдете таке повідомлення, ви можете дізнатися код ключа та передати його в систему реєстрації та аналізу (крок 4). Потім управління повертається до програми (крок 5), яка не знає про наявність перехоплювача.

Такий шпигун клавіатури дуже небезпечний, оскільки:

- Схоже, це не стандартні методи пошуку шпигунських програм;

- можливо реалізувати перехоплювач за певних умов, в результаті чого він реалізується не у всіх GUI-процесах, а в строго визначених (наприклад, в браузерних процесах або в додатку типу WebMoney);

- марно використовувати електронні клавіатури та інше антишпигунське програмне забезпечення;

На додаток до перехоплення функцій PeekMessage та GetMessage, функції копіювання інформації можуть бути перехоплені при використанні буфера обміну (OpenClipboard, CloseClipboard, GetClipboardData, SetClipboardData), опитування стану клавіатури (GetKeyState, GetAsyncKeyState, GetKeyboardState) та інших функцій. та функції Capture, як CreateWindow, дозволяють відстежувати створення вікон [18].

Принцип роботи шпигунських програм в робочому режимі зі схованням ОС ядра схожий з UserMode, але в цьому випадку одна або кілька функцій win32k.sys перехоплюються. Як і у UserMode, PeekMessage та його однолітки представляють найбільший інтерес для перехоплювача, оскільки він дозволяє контролювати та змінювати абсолютно всі повідомлення, отримані програмою, не встановлюючи пастку чи фільтр.

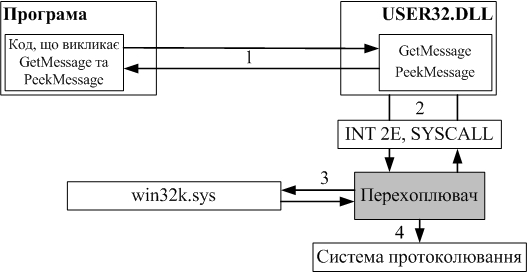


Рис. 2. 6. Схема роботи перехоплювача в режимі ядра ОС

Рис. 2. 6 перехоплювач показаний умовно, оскільки існують різні способи його встановлення, зокрема:

Перехоплення SY SYSCALL та INT 2E;

Function функція перехоплення зі зміною адреси у відповідній комірці таблиці KeServiceDescriptorTableShadow. Єдина складність для шпигунської атмосфери - це пошук цієї таблиці, яка не експортується ядром або документально підтверджується. Однак існують відомі способи подолання цієї проблеми, і засоби для цього можна знайти в Інтернеті;

модифікація машинного коду win32k.sys. Пошук таблиці KeServiceDescriptorTableShadow також необхідний. Можлива цікава ситуація: функцію вже можна перехоплювати (наприклад, анти-кейлоггером), і тоді машинний код перехоплювача буде змінений, що ще більше ускладнить виявлення шпигуна.

Алгоритм шпигунських програм досить простий. Додаток викликає функцію бібліотеки user32.dll (крок 1; розглянемо виклик PeekMessage як приклад). Функція PeekMessage в user32.dll за своєю суттю є адаптером, і в кінцевому підсумку SYSCALL в Windows XP або INT 2E в Windows NT та Windows 2000 зателефонує до функції ядра (крок 2). Цей виклик буде перехоплений шпигуном (розташування перехоплювача залежить від способу перехоплення). Перехоплювач, у свою чергу, викличе реальну функцію (крок 3) та проаналізує повернуті до неї результати [18].

Якщо повідомлення успішно видалено з черги, тип шпигунських програм буде аналізувати його та записувати результати (крок 4). Робота шпигуна абсолютно непомітна для всіх програм та користувачів, і його можна виявити лише за допомогою спеціальних програм, які здійснюють пошук перехоплень та модифікацій машинного коду модулів ядра [18].

На рис. 2.7 показано приблизний розподіл використання цих технологій порівняно з кейлоггерами, які не використовують технології руткітів.

Рис. 2. 7. Реалізація кейлогерів на основі технології rootkit

#### Апаратні кейлогери

Інший вид - апаратні кейлоггери. Якщо ви користуєтесь домашнім комп'ютером, достатньо переконатися у відсутності кейлогерів, але у випадку з корпоративною мережею потрібно перевірити відсутність обладнання, призначеного для запису вводу на клавіатуру.

Апаратні кейлоггери (пристрій запису натискань клавіш, апаратний кейлоггер тощо) - це мініатюрні пристосування, які можна приєднати між клавіатурою та комп’ютером або вбудувати у саму клавіатуру. Вони фіксують усі натискання клавіш. Цей процес повністю непомітний для користувача.

Апаратні кейлоггери не вимагають встановлення будь-якої програми на комп'ютері користувача для успішного перехоплення всіх натискань клавіш. Такий пристрій може бути таємно підключений до ПК будь-ким - колегою, прибиральницею, відвідувачем тощо. Якщо апаратний кейлоггер підключений, не має значення, у якому стані комп'ютер увімкнено чи вимкнено, оскільки він підключений до за межами ПК.

Потім зловмисник може в будь-який час видалити пристрій і, коли це зручно, завантажити його вміст (записані натискання клавіш). Внутрішня ємність зберігання цих пристроїв дозволяє записувати до 10 мільйонів натискань клавіш. Приєднати цей пристрій до комп'ютера користувача дуже просто. Зовнішній вигляд цих пристроїв настільки різноманітний, що навіть фахівець іноді не в змозі визначити їх наявність під час проведення інформаційного аудиту.

KeyKatcher, KeyGhost, MicroGuard, Hardware Апаратні кейлоггери KeyLogger особливо відомі на ринку і виробляються Alien Concepts, Inc., Amecisco, KeyGhost, Ltd., MicroSpy, Ltd.

Апаратні кейлоггери поділяються на зовнішні та внутрішні.

Зовнішні апаратні кейлоггери підключаються між звичайною клавіатурою ПК та комп'ютером і записують кожен натискання клавіш. Їм не потрібні ні акумулятори, ні програми, і вони можуть працювати на будь-якому ПК. Ви можете підключити їх до одного комп'ютера для запису інформації, а потім до іншого для відтворення. Сучасні апаратні кейлоггери - це гаджети, схожі на апаратне забезпечення ПК.

Найважче - це виявити (і налагодити) внутрішній апаратний кейлоггер, який має в корпусі клавіатури апаратний модуль натискання клавіш. Це вбудований невеликий пристрій, розміщений в розриві шнура клавіатури і покритий ізоляційним матеріалом.

Щоб знайти шпигунське програмне забезпечення на домашньому комп’ютері, достатньо переконатися у відсутності кейлогерів. Але у корпоративному середовищі, наприклад, комп’ютерах, що використовуються для банківської справи, електронної комерції чи обробки секретних документів, існує небезпека використання апаратних засобів, призначених для запису інформації, що вводиться з клавіатури. Розглянемо основні канали витоку інформації з точки зору використання обладнання (рис. 2. 8).

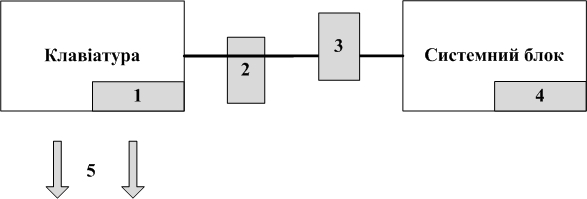


Рис. 2. 8. Можливі місця перехоплення введеної інформації

Апаратні кейлоггери можуть бути реалізовані кількома способами:

1. Закладка обладнання на клавіатурі (рис. 2. 8). Клавіатуру користувача можна встановити вручну або спеціалізованим контролером. В даний час існує велика кількість клавіатур такого типу, які можна придбати в спеціалізованих магазинах. На будь-якій клавіатурі зазвичай багато порожнин, розмір яких досить великий, щоб вмістити невелику дошку. Пристрій працює, і інформацію можна видалити, безпосередньо підключившись до друкованої плати контролера клавіатури. Закладку обладнання можна встановити вручну або промисловим способом. Цій закладці можна протиставити лише фізичну розбирання пристрою та його герметизацію [15].
2. Зчитування даних з кабелю клавіатури безконтактним методом. Ця методика передбачає зчитування інформації за допомогою безконтактного датчика. Встановлення такого пристрою не вимагає ні відкриття клавіатури, ні підключення будь-якого пристрою до зазору кабелю. Безконтактний апаратний кейлоггер повинен мати автономне джерело живлення, а його конструкція набагато складніше, ніж у випадку прямого підключення. За зовнішнім виглядом такий пристрій може виглядати як знімний перешкодний фільтр, який одягається на кабель. Метод контрзаходу: Безконтактне зчитування є найбільш ефективним при розташуванні датчика в безпосередній близькості від кабелю клавіатури (а ще краще - навколо цього кабелю), тому під час перевірки завдань переконайтесь, що поблизу кабелю клавіатури чи безпосередньо на ньому немає ніяких невідомих предметів.
3. Підключення пристрою до обриву кабелю. Шпигуни клавіатури такого типу є найпоширенішими та простіми в установці та виявленні. Апаратний кейлоггер виконаний як невеликий пристрій, який підключається до порту PS / 2 або USB комп'ютера, а клавіатура підключається до роз'єму на корпусі кейлоггера. Ця операція не вимагає кваліфікації, і підключення брелока до USB-клавіатури можна здійснити без вимкнення комп'ютера. Існує ряд комерційно доступних пристроїв, таких як апаратні кейлоггери KEYKatcher, які випускаються двох типів - для клавіатур PS / 2 та USB. Інший приклад - KeyGhost. Апаратний кейлоггер може бути схожим на фільтр перешкод або адаптер. Пристрій складається з вхідних схем, призначених для фільтрації перешкод і захисту пристрою від перенапруги, мікроконтролера з низьким споживанням енергії та флеш-пам'яті, призначених для зберігання зібраної інформації. Флеш-пам’ять становить від 32 Кб до десятків мегабайт; типовий об'єм - від 128 КБ до 2 Мб. Техніка протидії: періодичний огляд робочого місця на предмет наявності сторонніх пристроїв, що входять до обриву кабелю клавіатури. Штекер клавіатури досить простий для захисту наклейки, яка ламається при вийманні штекера з розетки.
4. Закладка апаратури всередині системного блоку. Цей шпигун принципово не відрізняється від пристроїв типу 1 і 3, але розміщується всередині системного блоку. Встановити його може тільки фахівець, і це зажадає відкриття корпусу. Спосіб протидії: герметизація корпусу системи наклейками. Перед герметизацією необхідно вивчити вміст системного блоку та переконатися у відсутності сторонніх пристроїв (з'єднання за замовчуванням - материнська плата; підключення здійснюється паралельно з роз'ємом клавіатури).
5. Захопити електромагнітне випромінювання клавіатури досить важко на відстані (хоча теоретично це можливо), але захопити акустичні шуми на порядок простіше. Навіть розмовляючи по телефону, іноді можна чітко почути людину, яка вводить інформацію на клавіатурі. Дослідження експертів із безпеки показують, що кожна клавіша видає певний звук при натисканні, щоб виявити натиснуті клавіші. Найвідоміша робота в цьому напрямку була проведена вченими Каліфорнійського університету в Берклі, які прийшли до висновку, що за звичайним записом можна розпізнати від 60 до 96% символів. Без використання спеціалізованих програм аналізу можна просто встановити кількість символів, набраних паролем, та наявність дублікатів символів. Техніка протидії: основним способом захисту від витоку інформації шляхом аналізу акустичних сигналів є постійний та систематичний інструктаж персоналу [18].

### Пошук по сигнатурам

Даний метод не відрізняється від типових методик пошуку вірусів. Сигнатурний пошук дозволяє однозначно ідентифікувати клавіатурні шпигуни, при правильному виборі сигнатур ймовірність помилки практично дорівнює нулю. Однак сигнатурний сканер зможе виявляти заздалегідь відомі і описані в його базі даних об'єкти, так що ця база повинна бути великою і її потрібно постійно оновлювати [24].

### Евристичні алгоритми

Це методики пошуку клавіатурного шпигуна по його характерним особливостям. Евристичний пошук носить імовірнісний характер, і він найбільш ефективний для пошуку клавіатурних шпигунів найпоширенішого типу - заснованого на пастках, проте подібні методики дають багато помилкових спрацьовувань. Деякі дослідження показали, що існують сотні безпечних програм, які не є клавіатурними шпигунами, але встановлюють пастки для стеження за клавіатурним введенням і мишею. Найбільш поширені приклади - програма Punto Switcher, програмне забезпечення від мультимедійних клавіатур і миш.

### Моніторинг API-функцій, що використовуються кейлогерами

Дана методика заснована на перехопленні ряду функцій, що застосовуються клавіатурним шпигуном, зокрема, функцій SetWindowsHookEx, UnhookWindowsHookEx, GetAsyncKeyState, GetKeyboardState. Виклик цих функцій будь-яким додатком дозволяє вчасно підняти тривогу, однак проблеми численних помилкових спрацьовувань будуть аналогічні методу евристичного алгоритму [24].

### Відслідковування драйверів, процесів та сервісів

Це універсальна методика, застосовна не тільки проти клавіатурних шпигунів. У найпростішому випадку можна застосовувати програми типу Kaspersky Inspector, які відстежують появу в системі нових файлів [24].

## Методи захисту від кейлогерів

Для виявлення та видалення програмного забезпечення для моніторингу, які можна встановити без відома користувача ПК, зараз використовуються програми, які за допомогою аналізу підписів забезпечують більш-менш ефективний захист лише від відомих шпигунських програм. Для того, щоб цей тип програми працював ефективно, вам потрібно отримати зразок шпигунських програм, витягнути з нього підпис і включити його у свою базу даних. Під час оновлення бази даних підписів користувачі персональних комп'ютерів отримують можливість розібратися з переданою версією шпигунських програм. Багато відомих виробників антивірусного програмного забезпечення працюють над цим принципом.

Що може користувач персонального комп’ютера протидіяти шпигунській програмі? Вирішення цієї проблеми можливе лише у використанні комплексу програмних продуктів.

Програмний продукт №1 - це той, який використовує евристичні механізми захисту, створені фахівцями з більшим досвідом боротьби зі шпигунським програмним забезпеченням. Його захист безперервний, поки він не використовує жодних підписів.

Програмний продукт №2 - це антивірусний програмний продукт, який використовує постійно оновлювані бази даних підписів.

Програмний продукт №3 - персональний брандмауер, який керує доступом до Інтернету з персонального комп’ютера на основі налаштувань самого користувача.

Ця послідовність вибирається з причини.

Антивірусний програмний продукт вдається реагувати на проникнення вірусів за допомогою модуля керування журналами, коли інформація вже перехоплена, оскільки база даних вірусів ще не встигла поповнитися новою інформацією, а відповідно, та оновитись на комп'ютері користувача.

Особистий брандмауер задає багато питань, на які навіть дуже навчений користувач може відповісти неправильно, тим самим налаштувавши його неправильно. Наприклад, деякі комерційні програми моніторингу використовують процеси програмних продуктів, яким навмисно дозволяється доступ до Інтернету (браузери, клієнти електронної пошти).

А це призводить до того, що інформація, яка вже була викрадена при повній бездіяльності антивірусної програми, буде спокійно передана в Інтернет за Інтернет-адресою, заздалегідь підготовленою хакером (або кимось іншим). І лише програмний продукт першого типу працює безшумно, не задаючи користувачеві зайвих запитань, і виконує свою роботу постійно у фоновому режимі.

У світі існує дуже багато антивірусних програм, що використовують постійно оновлювані бази даних підписів (AVP, Dr.Web, Panda Antivirus, Norton Antivirus та багато інших). Є ще більше персональних брандмауерів (Norton Internet Security, BlackICE Defender, брандмауер GuardianPro, мініатюрний персональний брандмауер та інші).

І представлені сьогодні програми безпеки першого типу блокують роботу шпигунських програм без використання баз даних підписів. Це стало можливим завдяки тому, що були знайдені рішення та були розроблені алгоритми, що дозволили відрізнити роботу шпигунських програм від будь-якого іншого додатка, який встановлений у системі.

Програма першого типу повинна включати модулі, які забезпечують:

* захист від перехоплення натискань клавіш на клавіатурі;
* захист від перехоплення тексту з вікон;
* захист від зйомки зображення на робочому столі;
* захист від захоплення зображення активними вікнами.

А також для власного захисту від зовнішнього згубного впливу шпигунських програм програма повинна мати систему контролю цілісності та інші захисні функції.

Методи протидії апаратним кейлогерам.

Жодна програмна продукція не в змозі визначити наявність встановлених апаратних пристроїв, які забезпечують перехоплення натискань клавіш користувачем персонального комп’ютера.

На сьогодні існує лише два способи протидії апаратним кейлогерам при роботі на звичайному персональному комп’ютері:

* фізичний пошук та усунення апаратного кейлогера;
* використання віртуальних клавіатур для введення критичної інформації (логіни, паролі, коди доступу, PIN-коди кредитної картки).

### Використовування одноразових паролів/двофакторної автентифікації

У випадку, якщо вам потрібно захистити доступ до певних акаунтів у соціальних мережах, до своїх банківських рахунків, на різних сайтах тощо, найбільш ефективним методом було б використання одноразового пароля. Такі паролі не можна перехоплювати за допомогою кейлогера, шпигувати або підслуховувати, оскільки вони працюють лише один раз. Їх схема реалізована за допомогою специфічного криптографічного алгоритму, їх можна генерувати на основі поточної дати та часу, створених за допомогою конкретного секретного ключа. Також можуть використовуватися інші алгоритми, єдиною вимогою є те, що обидві сторони (сервер та користувач) повинні знати, який алгоритм та які умови застосовуються. Ще однією перевагою такого пароля є те, що він діє протягом певного періоду часу, після якого він стає неактивним. Зараз існує безліч програмних та апаратних засобів, які можна використовувати для отримання одноразового пароля, наприклад спеціальний калькулятор або алгоритм для генерування цього пароля [23].

Одноразовий пароль можна надіслати через SMS на номер мобільного телефону, зареєстрований у системі.

Двофакторна аутентифікація - досить надійний спосіб. До факторів аутентифікації належать:

Автентифікація за допомогою знань. Вони можуть бути паролем або парольною фразою, PIN-кодом;

Аутентифікація ктори за власністю. Це може бути фізичний ключ, магнітна смужка або чіп-карта, маркер або ключ USB, який використовується для ідентифікації власника;

Аутентифікація за характеристикою. До них відносяться відбитки пальців, малюнок сітківки, голос [24].

### Використання систем проактивного захисту

Системи проактивного захисту є частиною антивірусного програмного забезпечення. Щодо захисту від келоугерів, вони працюють за принципом запобігання зараженню системи, не шукаючи відомих кейлогерів [25]. Такі системи включають описаний вище евристичний аналіз. Ці системи попереджають користувача про встановлення або активацію програмних келоггерів.

Методи проактивного захисту включають:

пісочниця - метод, заснований на виконанні потенційно небезпечного ПО в обмеженій середі виконання, який пропонує контакт з потенційно небезпечним ПО з ОС;

Ips стегна - метод контролю за діяльністю, заснований на перехопленні звернень до ядра ОС та блокуванні виконання потенційно небезпечних дій програмного забезпечення, що працює в режимі користувача, виконуються без відома користувача;

vips - метод управління активними, заснованими на моніторингу виконаними операціями ПО, встановленими на ПК та блокованими виконаннями потенційно небезпечних діючих ПО, виконаних без відома користувача.

Методи поведінкового аналізу:

Методи емуляції системних систем - метод визначення тимчасового ПО шляхом аналізу діючого та / або ланцюгів діючого з підтримкою виконання ПО в спеціально обмеженій середі (що використовується емулятор коду), імітуючої реальної апаратури;

поведений блокатор - метод, заснований на методах IPS, аналіз у реальному часі ланцюгів діючого ПО та блокованого виконання дійсно небезпечних алгоритмів у реальному часі;

Сканер цілісності - постійно контролює ядро ​​ОС, щоб виявити зміни, які можуть бути викликані шкідливим програмним забезпеченням. У разі виявлення змін, внесених шкідливим програмним забезпеченням, користувач отримує відповідне сповіщення та, якщо можливо, відшкодування дій, що виконуються шкідливим програмним забезпеченням;

«Емулятор NX-біта» здійснює моніторинг сучасної оперативної пам’яті. У випадку виявлення спроби, що входять до складу критичних вимірів, містяться в оперативній пам'яті, дія блокується. [26].

Недолік в тому, що існує потреба в постійному залученні користувачів до роботи програми: потрібно вибрати, що робити з програмою, яка підозріла в цій системі. Але мінімізуючи участь користувачів, кейлогер може бути пропущений через жорстку політику безпеки системи.

### Використання віртуальних клавіатур

Віртуальна клавіатура представляє собою програму, демонструючи на екрані зображення звичайної клавіатури, в якій за допомогою миші можна «наживити» конкретні клавіші [27].

У цілому, екранній клавіатурі плохого застосування для обману кейлогерів, так як вона створила не як засоби захисту, як спосіб допомоги людям з обмеженими можливостями, і передає дані після введення з допомогою даної клавіатури, може бути дуже просто перехоплюється тимчасовою програмою.

Екранна клавіатура може бути використана для того, щоб скористатися кейлогером, однак, вона повинна бути розроблена спеціальною системою, що дозволяє переключити введені дані на будь-яких стаціонарних введення і передачі (як правило, застосовується алгоритм зразків позицій кнопок і цифр, а так само шифрування конкретного рішення) [24].

### Програмні рішення

Наступні програмні рішення включають такий тип захисту кейлогера:

1) Антивірусні продукти. Їх використання доцільне, але оскільки кейлогери не є вірусами, антивіруси в цьому питанні не є абсолютно ефективними.

2) Сигнатурні та евристичні пошукові утиліти.

3) Спеціальне ПЗ для пошуку та знищення кейлогерів [28].

## Рекомендації щодо захисту

На сьогоднішній день кейлогери є досить великою проблемою, оскільки вони не потребують попередньої інформації про комп'ютер користувача для встановлення. Вирішення цієї проблеми можливе лише у використанні комплексу програмних продуктів.

Програмний продукт №1 використовує евристичні механізми захисту, створені експертами з більшим досвідом роботи зі шпигунським програмним забезпеченням. Його захист є безперервним, і він не використовує жодних баз даних пошуку підписів.

Програмний продукт №2 - це антивірусний програмний продукт, який використовує постійно оновлювані бази підписів.

Програмний продукт №3 - це персональний брандмауер, який керує доступом до Інтернету з персонального комп’ютера на основі налаштувань користувача.

Така послідовність обрана не просто.

Антивірусне програмне забезпечення вдається реагувати на проникнення вірусу за допомогою модуля клавіатури, коли інформація вже перехоплена, оскільки база даних вірусів ще не встигла поповнитися новою інформацією, а відповідно, та оновитись на комп'ютері користувача .

Особистий брандмауер викликає багато питань, на які навіть дуже навчений користувач може відповісти неправильно, тим самим неправильно налаштувавши його. Наприклад, деякі комерційні програми моніторингу використовують програмні процеси, які свідомо дозволяють отримати доступ до Інтернету (браузери, поштові клієнти). І це призводить до того, що інформація, яка вже була викрадена при повній бездіяльності антивірусної програми, буде спокійно передаватися в Мережу хакеру (або комусь іншому), заздалегідь підготовленому за допомогою Інтернет-адреси. І лише перший тип програмного забезпечення працює безшумно, не задаючи користувачеві зайвих запитань, і виконує свою роботу постійно у фоновому режимі.

Існує багато антивірусних програмних продуктів, які використовують постійно оновлювані бази даних підписів (AVP Dr.Web, антивірус Panda Antivirus Norton та багато інших). Створено більше брандмауерів (Norton Internet Security, BlackICE Defender, GuardianPro Tiny Personal Firewall тощо).

З апаратними кейлогерами ситуація дещо інша. Жоден програмний продукт не в змозі виявити наявність встановлених апаратних пристроїв, які дозволяють користувачеві клавіатури перехоплювати клавіатури.

На сьогодні існує лише два способи протидії апаратним кейлогерам при роботі на звичайному персональному комп’ютері:

Пошук фізичного пошуку та видалення апаратного кейлогера;

Використовуйте віртуальні клавіатури для введення особливо важливої ​​інформації (логіни, паролі, коди доступу, PIN-коди кредитної картки).

На відміну від спаму та іншого небажаного програмного забезпечення, кейлогери мають функціональні можливості, які можуть порушувати конфіденційні дані. Потенційними результатами діяльності цих програм є значне уповільнення продуктивності чи складності комп’ютера під час відвідування будь-якого веб-сайту, зниження продуктивності співробітників та інформаційна безпека.

В даний час відставання виявлення та видалення шпигунських програм від вимог до централізованого управління цією продукцією є досить гострим, а швидкість розробки заходів безпеки значно нижча, ніж швидкість створення шпигунських програм. Зараз ця проблема вирішується зусиллями як малого, так і середнього бізнесу та великих постачальників антивірусних програм, доповнених лінійкою рішень шпигунських програм.

Жодне із існуючих на ринку антишпигунських рішень не забезпечує стовідсотковий захист. Навіть у повністю закритому програмному середовищі зараження може статися, якщо спочатку програмний модуль був присутній у програмному забезпеченні, до якого було дозволено встановити програмне забезпечення. Шпигунське програмне забезпечення займає №2 у списку загроз безпеці мережі - після вірусів, хробаків та троянців. Основним заходом захисту є «освіченість» користувачів: вони повинні добре знати ризики та фінансові збитки, які шпигунське програмне забезпечення приносить із собою, а також вживати запобіжних заходів. Багато програм-шпигунських програм потрапляють на комп'ютери легально: користувач встановлює їх самостійно.

За даними Trend Micro, існує шість основних наслідків атак шпигунських програм:

* залучення мережевих обчислювальних ресурсів;
* Зниження продуктивності користувачів на час;
* Зменшення пропускної здатності мережі;
* Завантаження шкідливих програм;
* втручання в конфіденційність.

Для початку давайте визначимо конкретні шляхи проникнення шпигунських програм. Деякі ми вже згадували (CD та інші медіа, оновлення). Але найчастіше це вільне програмне забезпечення. Іншим джерелом можуть бути функції Інтернет-браузера, які забезпечують завантаження без участі користувача: вони служать інструментом для завантаження небажаного програмного забезпечення. Ви можете використовувати ActiveX Control, який реалізує запит на підтвердження завантаження, для управління такими завантаженнями, зробленими, наприклад, за допомогою ActiveX. Працюйте в Інтернеті за наявності виявлених вразливих місць ОС або Інтернет-браузерів

Перш за все, і найголовніше, повинна існувати політика безпеки, яка регулює правила доступу користувачів в Інтернеті. Персонал повинен регулярно проходити навчання за правилами Інтернету, щоб усі були в курсі поточної інформації про існуючі Інтернет-загрози. Таке навчання рекомендується проводити на конкретних, зручних для користувача прикладах, а не у формі загальної теорії. Якщо користувач не знає, що може загрожувати завантаженню «цікавої» програми з Мережі, то регуляторні заходи не дадуть очікуваних результатів.

Друге рішення - централізувати реалізацію керованого антишпигунського рішення, в рамках якого політики встановлюються адміністратором безпеки, сервісами клієнтських ПК, автоматизовано збирання інформації про інциденти та звітування. У той же час слід використовувати профілактичні шпигунські технології, які можуть видалити підозрілі програми до їх встановлення на комп’ютері.

Таким чином, кейлогери часто використовуються хакерами для крадіжки паролів, номерів кредитів та іншої конфіденційної інформації.

Ось кілька порад, які допоможуть захистити ваш комп’ютер від кейлогерів:

1. Використання надійного антивірусу. Хоча це не є гарантією того, що кейлогер не буде встановлений на вашому комп'ютері, встановлення антивірусу - це перший крок для захисту від кейлогерів та інших загроз з Інтернету. Антивірусні бази даних повинні постійно оновлюватися.

2. Встановлення менеджера паролів. Автозаповнення корисно для захисту кейлогера. Якщо пароль автоматично заповнюється без будь-яких натискань клавіш, клавішник прийме пароль лише при першому введенні. Усі веб-браузери мають цю функцію, але є деякі програми, які дозволяють запам’ятати всі паролі, а автозаповнення відбувається лише тоді, коли ви входите в один і той же додаток, для чого потрібен логін та одноразовий пароль [23].

3. Часта зміна пароля. Зміна паролів допомагає мінімізувати ймовірність атак Keylogger. Зазвичай при їх викраденні паролі використовуються не відразу, якщо тільки конкретний користувач не був об'єктом зловмисника. Коли ви зміните свої паролі, вкрадена інформація кожні два тижні може більше не бути актуальною.

4. Використовуючи лише надійний комп'ютер (наприклад, на комп’ютерах в Інтернет-кафе можуть бути встановлені KeyLoggers, які збирають вашу особисту інформацію).

Для захисту від кейлогерів рекомендується працювати в безпечному середовищі. Для збереження паролів рекомендується використовувати програми запам'ятовування паролів. Створюючи нову базу даних паролів, програма пропонує ввести пароль, вибрати режим шифрування даних, функцію їх шифрування, спосіб стиснення файлів, встановити максимальну кількість паролів у цій базі даних, дату та час пароля змінити.

## Висновки до розділу

У другому розділі описана суть кейлогерів, їх найпоширеніші типи, способи розповсюдження та створення, приховування себе під час використання комп'ютера та їх поточний стан.

Провівши аналіз та получивши інформацію, можна сказати, що кейлогери - це потужний інструмент, який не завдає шкоди самій системі, вони спрямовані на отримання конфіденційної інформації користувача, наприклад, ім’я користувача, пароль, номер телефону, банківську карту тощо. Деякі кейлогери використовуються як законні програми , може бути створено на замовлення уряду або для компаній, які відстежують дії своїх працівників.

Виявлення технології keylogger не відрізняється від інших шкідливих програм або загроз, які потребують регулярного моніторингу системи. Основне завдання користувача - усвідомлювати, що існують загрози, такі як кейлогери, знати, як вони використовуються та як їх можна виявити. Актуальним аспектом зараз є те, що користувачі не повинні забувати, що бездротові клавіатури не безпечніші, а навпаки, можуть передавати інформацію по повністю незахищеному каналу. Однак в організаціях виявлення брелоків повинно бути частиною плану реагування на інциденти.

Для захисту кейлогерів слід використовувати багаторівневу безпеку, таку як використання антивірусного програмного забезпечення, проактивний захист та віртуальні клавіатури або системи одноразового пароля, а також двофакторну автентифікацію.

# РОЗДІЛ 3

# ТЕСТУВАННЯ СПОСОБІВ ВИЯВЛЕННЯ ТА ОРГАНІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ВІД КЕЙЛОГЕРІВ

## Опис роботи кейлогера, реалізованого на основі циклічного опитування стану клавіатури

Для ілюстрації принципу кейлогера був реалізований демонстраційний програмний продукт. Цей кейлогер реалізований принципом циклічного моніторингу функцій API. Ця програма працює у фоновому режимі, після включення вікно програми приховано, завдання відсутнє на панелі завдань, функція приховування в диспетчері завдань не передбачена. Ця програма перехоплює коди клавіш і кнопок миші. Усі букви перекладені англійською мовою, імена активних вікон видаляються. Результати записуються у текстовий файл, ім'я якого складається з поточної дати та часу у форматі .log.

Програмний код містить визначення необхідних бібліотек та функцій. Оскільки програма була створена під Windows, використовується спеціальна основна функція програми WinMain. Модифікатор ApiEntry використовується разом із цією функцією для правильного запису аргументів у стек. Виглядає так:

int APIENTRY WinMain(HINSTANCE hInstance,HINSTANCE hPrevInstance,LPTSTR lpCmdLine,int nCmdShow)

Далі створюється .log файл, ім'я якого складається з поточної дати та часу. Цей файл записуватиме всю отриману інформацію. Для цього використовуються функції *strftime, sprintf*.

strftime(filename, 100, «%Y-%m-%d\_%H-%M-%S», timeinfo);

sprintf(filepath, «%s\\%s%s», basepath.c\_str(), filename, FILEEXT);

Потім відображається поточна інформація про вікно. Для цього за допомогою функції GetForegroundWindow () отримує дескриптор цього вікна, а за допомогою функції GetWindowText () визначає назву активного вікна. HWND hwndHandle = GetForegroundWindow();

GetWindowText(hwndHandle, title, 1023);

Наступна частина полягає у визначенні натискань клавіш і записує їх у файл: перераховуються можливі натискання клавіш, що варіюються від 1 до 255. За допомогою функції GetAsyncKeyState видаляється поточний стан клавіатури. Якщо цю клавішу натиснути в даний момент, її стан блокується, а інформація відображається в документі.

for(unsigned char c = 1; c < 255; c++){

SHORT rv = GetAsyncKeyState(c);

if(rv & 1){ string out = ««; …}

Після отримання коду сканування, клавіша визначається, яка саме клавіша натискається наступним чином:

if(c == 1)

out = «[ЛіваМ]»;

else if(c == 2)

out = «[ПраваМ]»;

Нижче наведено список можливих натискань клавіш: [ЛіваМ], [ПраваМ], [СередняМ], [Enter], [Shift], [Ctrl], [Alt], [AltGr], [Backspace], [Tab], [Esc], [PageUp], [PageDown], [End], [Home], [ВлівоСтр], [ВверхСтр], [ВправоСтр], [ВнизСтр], [Ins], [Del], [Win], [Num 0-9], [Num /], [Num +], [Num -], [Num ,], [Num], [+], [,], [-], [.], [#], [<], [>], [F1-12], [PrtSc], [Вимкнення звуку], [Зменшення звуку], [Збільшення звуку], [Наступний трек], [Попередній трек], [Зупинити/включити музику]. Усі інші клавіші визначаються за кодом, вивід якого оформляється наступним чином:

out = «[Клавіша \\» + intToString(c) + «]»;

Щоб отримати поточний каталог, використовуйте функцію GetCurrentDirectory (), щоб отримати повний шлях до активного файлу GetModuleFileName ().

Результат програми такий. Після запуску програми її приховали і запустили у фоновому режимі. Журнал подій під назвою "Рік-місяць-день\_ Години-секунди.лог" був створений з датою та часом запуску програми (рис. 3. 1).



Рис. 3. 1. Лог файл створений кейлогером

Закрити дану програму можна тільки за допомогою Диспетчера задач.



Рис. 3. 2. KStroker у диспетчері задач

Цей кейлогер не вимагав ігнорувати антивірусні програми, тому Eset Nod 32 негайно видалив його при спробі записувати інформацію. Коли завантажений кейлогер під час вимкнення антивіруса, він не був заблокований після ввімкнення антивірусу до відкриття менеджера завдань. Windows Defender не відповів на KStroker у системі.

## Вибір кейлогерів для тестування

Після вибору кейлогерів було розглянуто ряд їх характеристик:

1) кейлогери повинні фіксувати натискання клавіш з різними принципами роботи;

2) вони повинні були відповідати мінімальним вимогам приховування: браузер не повинен був блокувати процес завантаження кейлогера; антивірус повинен був дозволити доступ до веб-сайту завантаження Keylogger; інсталятор не повинен був видаляти антивірус відразу після завантаження;

3) Програмне забезпечення повинно бути ефективним, сучасним та не відомим (не всі антивіруси повинні містити інформацію про них у своїх базах даних).

Під час відбору було протестовано кілька кейлогерів: Jetlogger, Elite Keylogger, The Rat!, Ardamax Keylogger, SC-KeyLog, Radar Spy, WebWatcher, Mipko.

Не всі перераховані вище програми відповідали заявленим вимогам. Кейлогер Radar Spy був негайно заблокований браузером, коли ви намагалися завантажити його на комп'ютер. Ardamax Keylogger - не має прихованого режиму, призначеного для домашнього відстеження процесів. SC-KeyLog - антивірус видалив інсталятор при спробі завантажити його. Щур! - Антивірус видалив GUI Keylogger після його встановлення, унеможлививши його відкриття, хоча сам кейлогер збирав та записував інформацію про сеанси. Міпко та Еліт Кейлогер були надто відомими, щоб брати участь у тестуванні.

Перші два кейлогери, WebWatcher та Jetlogger, найкраще відповідали заявленим стандартам, тому вони були обрані для роботи.

Кейлогери WebWatcher 8.2.49 та Jetlogger 1.9 відносно рідкісні на сьогоднішній день, але досить надійні та мають усі необхідні функції кейлогера. У таблиці 3.1 наведено порівняння функцій, що виконуються цими кейлогерами.

Таблиця 3.1.

Порівняння функцій WebWatcher 8.2.49 та Jetlogger 1.9

|  |  |  |
| --- | --- | --- |
| **Функція** | **WebWatcher 8.2.49** | **Jetlogger 1.9** |
| Віддалене підключення | + | - |
| Доставка звітів на електронну адресу | + | + |
| Невидимий режим спостереження | + | + |
| Спосіб спостереження | Драйверний, використання dll бібліотек | API-моніторинг |
| Статистика загального часу активності користувача | - | + |
| Збереження скріншотів | + | + |
| Збереження буферу | + | + |
| Перехоплення електронної пошти | + | + |
| Моніторинг мережевих протоколів | POP3, HTTP, SMTP | SMTP, HTTP |
| Розділення клавіатурного набору від набору паролів | + | - |
| Комбінація клавіш для відкриття інтерфейсу за замовчуванням | unhide | Ctrl+Alt+Shift+J |
| Створення прихованої папки для логів | + | - |
| Запис відео та аудіодзвінків | - | + |
| Відстежування по радіоканалу | - | - |

Отже, було використано два кейлогери. Нижче наведено короткий опис кожного.

1. WebWatcher позиціонується як інструмент батьківства та управління, але в 2016 році компанія-розробник подала позов до суду за витік особистих даних багатьом користувачам. На базі водія, виробництво США не є поширеним в Європі.

2. Jetlogger - позиціонується як корпоративне програмне забезпечення для відстеження. Працює на основі моніторингу api-функцій, програми російського виробництва.

## Опис обраних кейлогерів

### Кейлогер WebWatcher

#### Інсталяція кейлогеру

Установка WebWatcher не відрізняється від встановлення стандартного додатка WebWatcher. Щоб завантажити інсталятор, потрібно увійти до системи. Після завантаження браузер повідомляє, що файл може містити потенційні загрози, що є першим недоліком програми. Ця програма може бути встановлена в невидимому або видимому режимі. Невидимий режим включає такі компоненти, як драйвер низького рівня та прихований переглядач журналу, захищений паролем. У цьому випадку користувач не підозрює, що на його комп'ютері встановлений кейлогер.

У видимому режимі програма створює свої ярлики в меню "Пуск", на робочому столі, додається до списку об'єктів у "Додавання та видалення програм". Цей режим призначений для видимого моніторингу журналів. Наступним кроком є вибір списку встановлених компонентів (рис. 3. 3). У нашому випадку вказаний лише один компонент.

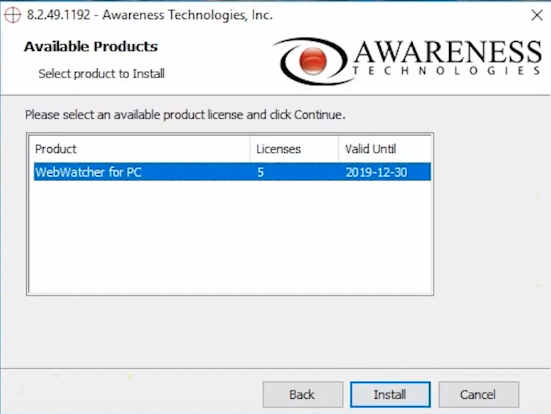


Рис. 3. 3. Перелік встановлюваних компонент WebWatcher

Наступним кроком є вибір періоду часу для видалення програми з комп'ютера, після чого необхідні параметри будуть завершені і розпочнеться процес встановлення програми. Після її завершення рекомендується перезавантажити комп'ютер та запропонувати видалити файл завантаження та записати з історії веб-переглядача.

Після перезавантаження системи відображається коротка інструкція щодо виклику програмного інтерфейсу (рис. 3. 4).

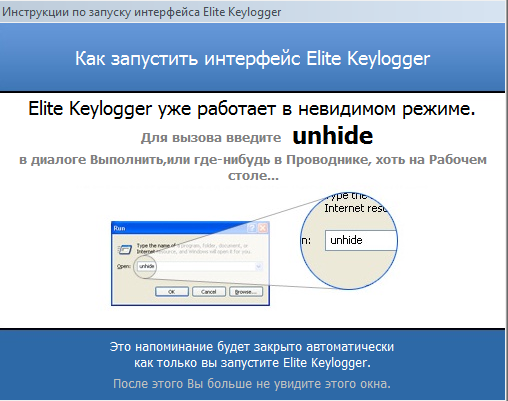


Рис. 3. 4. Інструкція щодо відкриття кейлогеру

#### 3.2.1.2. Опис роботи кейлогеру

Щоб відкрити вікно інтерфейсу, ви повинні ввести слово unhide у вільному просторі, а потім, при першому завантаженні, вас попросять ввести пароль, щоб відкрити вікно. На рис. 3.5 показано домашнє вікно WebWatcher.

На головній панелі ви бачите, що цей кейлогер призначений для ведення журналу натискань клавіш, знімків екрана, відвідуваних сайтів та пошукових запитів, запущених програм та додатків, буфера обміну, історії електронної пошти, історії друку та клацань миші. Крім того, ви можете включити фільтрацію в окремий файл введених паролів у налаштуваннях. Можна переглянути журнали на певну дату.

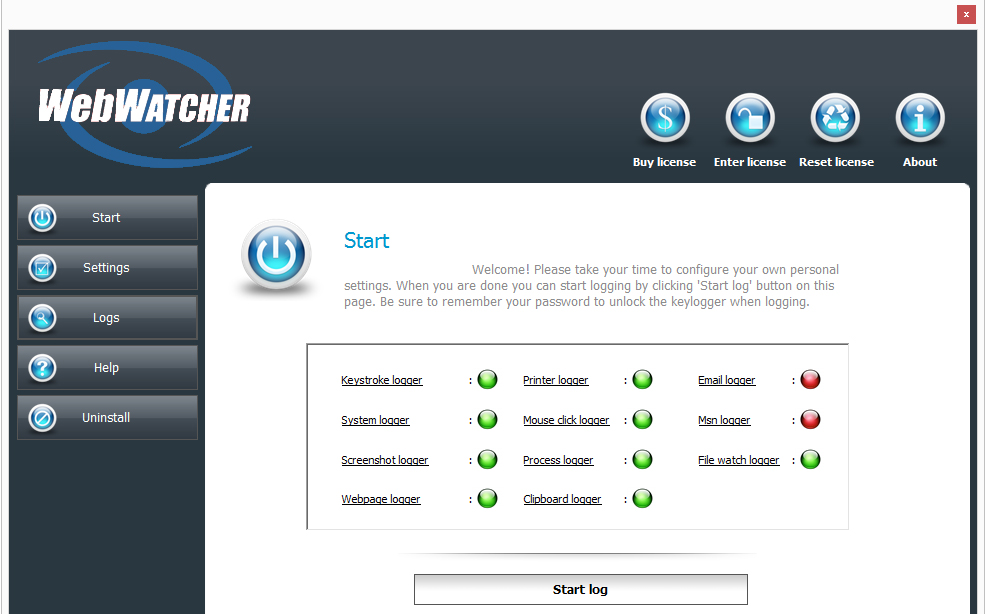


Рис. 3. 5. Домашнє вікно WebWatcher

WebWatcher показує скріншоти, створені кожні три хвилини. Для цього виберіть у меню знімки екрана.

При переході на модуль Журнали відкриється додаткове вікно, де відображається список вкладок із створеними журналами. Кожна вкладка виглядає як таблиця з датою створення запису, назвою процесу, вікнами та суттю запису. За замовчуванням відкривається вкладка клавіш. У розділі Інтернет-активності відображається перелік адрес відвідуваних сайтів із часом та датою.

WebWatcher підтримує кілька інших типів журналів:

Діяльність на основі активності, що визначають дату та час запуску, ім'я користувача або систему, повний шлях до файлу EXE;

 Дані буфера обміну. WebWatcher надає дані про розмір даних у буфер обміну, додаток, з якого дані розміщувались у буфері обміну, а самі дані копіювали;

Addresses адреси електронної пошти, на які надсилалися листи (“Пошта”), їх зміст;

 список кліків миші ("Клацання мишкою"), де відображається назва вікна, на кнопки якого натискаються, значення цього клацання;

List Список принтерів, де ви можете знайти дату та час друку, кількість сторінок та програму.

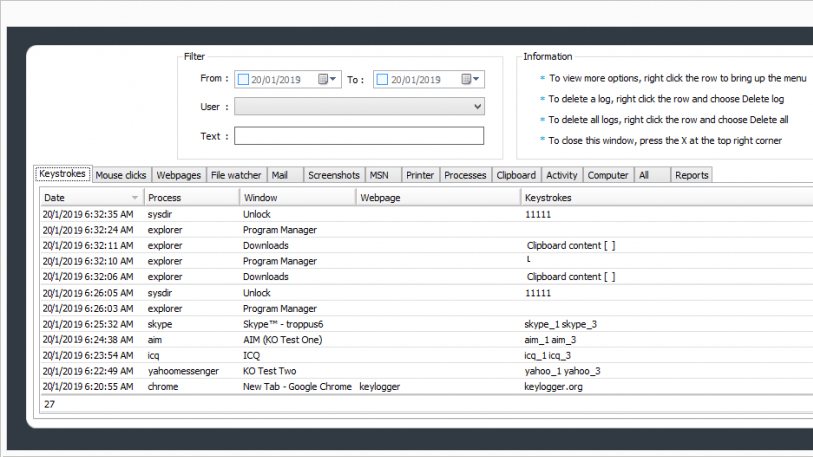


Рис. 3. 6. Логи WebWatcher

У налаштуваннях можна вибрати користувача, який може переглядати журнали клавіатури, вказувати пароль та / або ключове слово, встановлювати інтервал збереження знімків екрана та їх якість, вказувати способи збереження кожного з журналів окремо тощо (рис. 3. 7).

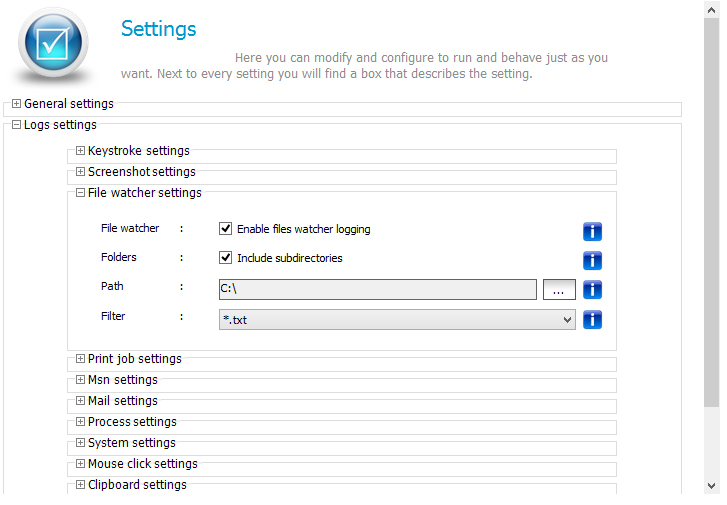


Рис. 3. 7. Вікно налаштувань WebWatcher

WebWatcher також надає можливість відстежувати активність користувачів на плановій основі. Автоматичне очищення колод проводиться, коли вони перевищують розмір 300 Мб, цей параметр також налаштований. Доступна функція надсилання журналів на вказану адресу електронної пошти.

### Кейлогер Jetlogger

#### Інсталяція кейлогеру

Jetlogger встановлюється нестандартно: його файли розміщені у прихованій папці на диску «C: \ ProgramData», він не відображатиметься у списку встановлених програм та при запуску. Автоматичний запуск Jetlogger спочатку не призначений, але він налаштований всередині програми або безпосередньо під час фази інсталяції. Установка програми дуже проста, запускати її потрібно лише в тому випадку, якщо параметри за замовчуванням підходять користувачеві (рис. 3. 8). Після запуску установки запускається лише програма.



Рис. 3. 8. Встановлення Jetlogger

Спочатку для запуску програми призначається ярлик на робочому столі. Після вивчення специфіки Jetlogger та гарячих клавіш, відкриття її ярликів на робочому столі відповідно знищується. Але перед тим, як розпочати вивчення програми, потрібно виконати певну роботу над системою.

На наступному кроці, після встановлення програми, потрібно додати папку шляху до списку виключень (він же білий аркуш) антивірусу:

C:\ ProgramData\JetProject

#### Опис роботи кейлогеру

Загальний інтерфейс програми представлений на Рис. 3. 9.

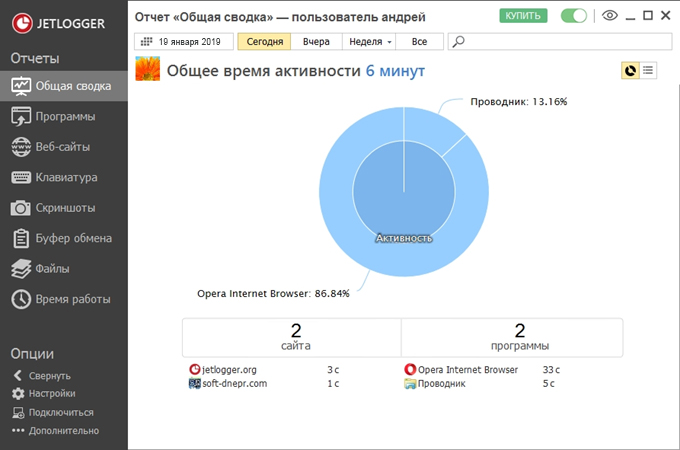


Рис. 3. 9. Домашнє вікно Jetlogger

Jetlogger є більш складним, ніж програми батьківського контролю, оскільки він працює безперебійно для користувача і дозволяє відслідковувати його дії в найтонших деталях. Програма виконує такі завдання:

 збирає інформацію про всі програми, що працюють на комп’ютері (рис. 3. 10 (а)), ігри, відкриті сайти (рис. 3. 10 (b)), монітори, що вводяться в пошуки;

 обчислює час, витрачений на конкретні програми, ігри та сайти;

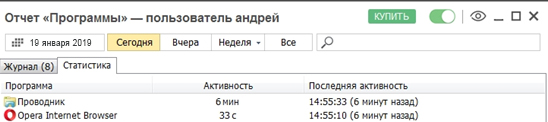
Є фіксує загальний час роботи за комп’ютером (рис. 3. 9);

 запам'ятовує набраний текст на клавіатурі (рис. 3. 10 (с));

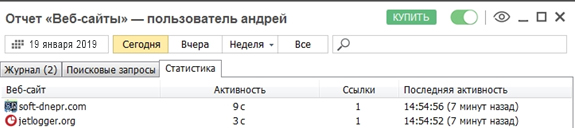
 контролює буфер обміну, створені та відредаговані файли;

 знімає скріншоти на весь екран та фотографії з веб-камери через певний проміжок часу (рис. 3. 10 (d));

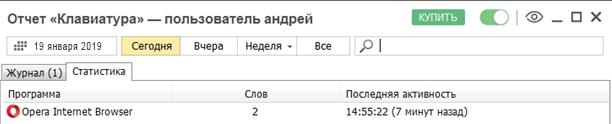
 забезпечує 4 механізми доставки звітів про роботу, а також режим віддаленого доступу з моніторингом дій користувачів у режимі реального часу [23].



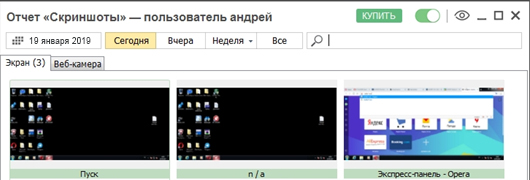
а)



б)



в)



г)

Рис. 3. 10. Логи Jetlogger а) Запущені програми; б) Відвідані веб-сайти; в) Натиснуті клавіші; г) Скріншоти

У розділі "Налаштування" (рис. 3. 11) у першій вкладці "Основні" ми можемо призначити автозапуск, якщо ця функція не була включена під час фази встановлення та змінити гарячі клавіші за замовчуванням для відкриття програми. Будь-які зміни, внесені в налаштування, повинні бути додатково підтверджені опцією збереження в нижній частині вікна.

Друга вкладка "Моніторинг" призначена для коригування окремих типів даних моніторингу - скріншоти, фотографії з веб-камери, використовувані програми, відвідувані веб-сайти, керовані файли тощо. Будь-який тип фіксованих даних може бути відключений, якщо це не представляє інтересу. або споживає занадто багато системних ресурсів. Деякі типи даних настроюються. Так, для знімків веб-камер та скріншотів можна змінити умови їх створення. Останні, залежно від можливостей комп’ютера, можуть бути створені в поганій або кращій якості. Зберігання знімків може бути обмежено певною кількістю дискового простору.

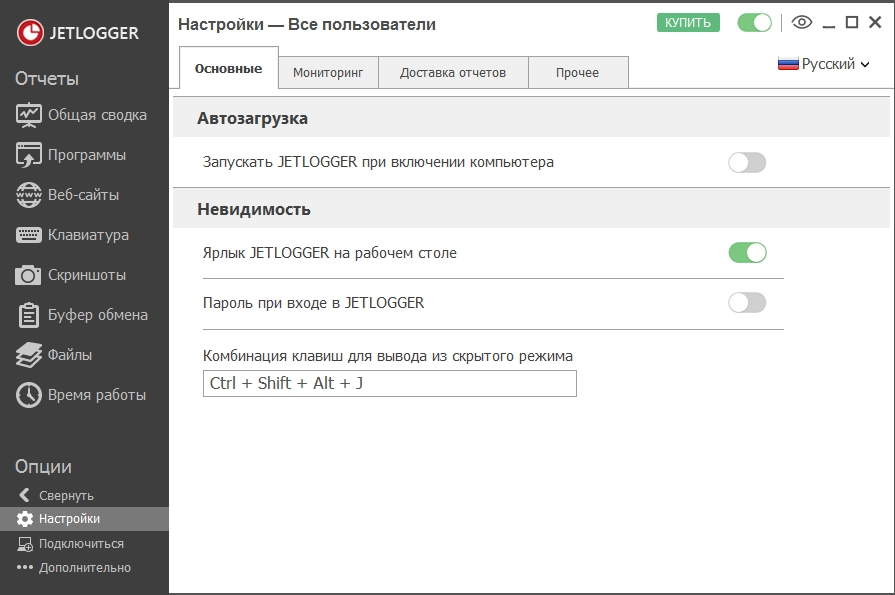


Рис. 3. 11. Вікно налаштувань Jetlogger

Операції відстеження файлів передбачають можливість відмовитись відслідковувати окремі дії, такі як створення, видалення, модифікація, перейменування. Ви можете налаштувати ярлики швидкої клавіші для збору даних, введених з клавіатури.

* 1. Опис програмного продукту Covert для виявлення кейлогерів

Традиційне антивірусне та антишпигунське програмне забезпечення не захищає знімки екрана та відео від скріншотів, оскільки ця дія не заборонена і невідома користувачем або тим, хто її переглядає. Аналогічна ситуація і з захистом від кейлогерів. Існує багато програм, які перехоплюють натискання клавіш для виконання певних функцій. Наприклад, ярлики до програм. Це юридична дія, яку не заважають антивірусні програми. Найуспішнішою, згідно з опитуванням, наразі є програма Covert.

Перелік функціональних можливостей програми:

1. Захищена платформа. Увійти та вийти з платформи одним клацанням утруднює доступ до облікового запису користувача.

2. Мережевий монітор. Відображає список програм, які отримують доступ до Інтернету в поточний час, має в порядку загрози базу даних загроз (шкідливе або небажане програмне забезпечення). Доступні для поповнення користувачем дані перевіряються розробниками, після чого вирішено додати цю програму / бібліотеку до списку шкідливих програм.

3. Монітор водія. Відображає список активних та прихованих драйверів в операційній системі, тим самим дозволяючи користувачеві приймати власні рішення щодо доцільності його роботи в системі.

4. Системні процеси. Надає інформацію про процеси (запущені програми), що відбуваються на вашому комп'ютері (подібно до диспетчера завдань Windows).

5. Системні послуги. Використовується для відображення списку запущених служб, монітора прихованих процесів. Це особлива функція, яка використовується для виявлення та відображення руткітів.

6. Режим внутрішнього захисту. Існує три режими захисту для управління запуском програм всередині платформи, з можливістю додавання їх до так званого білого списку винятків.

7. Кнопки запуску програми, ідентифікатор входу на платформу для створення декількох платформ безпеки, масштаб завантаження процесора, масштаб завантаження платформи, масштаб завантаження буфера обміну.

8. Аварійний вихід з програми та всіх платформ із закриттям усіх програм.

9. Відрегулюйте гучність гучномовців та мікрофонів усередині захищеної платформи. Дозволяє заблокувати мікрофон, щоб захистити зону прослуховування комп'ютера.

10. DLL-монітор. Використовується для відображення списку завантажених DLL-файлів на екрані під час роботи маски

11. Буфер обміну [30].

Інтерфейс програми має вигляд, зображений на Рис. 3. 12.

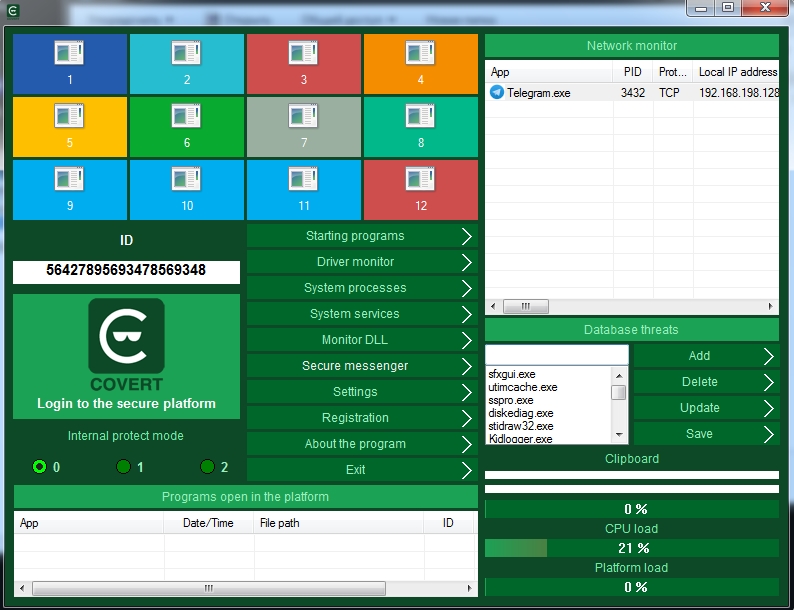


Рис. 3. 12. Інтерфейс програми Covert

## Процес виявлення та видалення кейлогерів

### Кейлогер Jetlogger

Цей кейлогер був виявлений за допомогою Covert. Після встановлення кейлогера його приховали. У Covert є способи, якими ви можете

повідомлення всіх запущених драйверів, системних процесів, служб та бібліотек dll.

Розробники Jetlogger стверджують, що програма призначена для обчислення робочого часу співробітників, при цьому заявляючи, що вона залишає далеко позаду різні кейлогери та шпигунські програми, максимально фіксуючи інформацію про роботу користувачів за комп’ютером і працює в самому невидимому режимі для користувачів. Саме ця заява є першою причиною, чому ця програма включена до переліку небезпечних кейлогерів, оскільки програми моніторингу ефективності робочого часу не потребують максимально прихованого режиму. На рис. 3. 13 показані всі підозрілі, на думку захисника програми, водії. Програма має можливість перевірити особу водіїв певних програм, після чого виявлено програму, яка володіє цими підозрілими драйверами, її безпеку було підтверджено. Тож у водійському полі все безпечно.

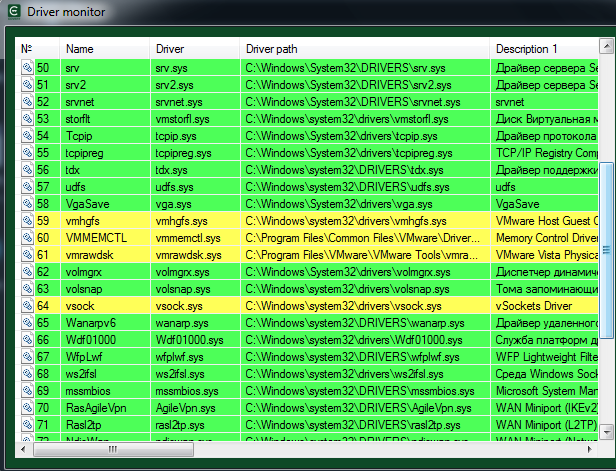


Рис. 3. 13. Драйверний монітор Covert

Далі перевірено системні процеси. Для цього було відкрито монітор системних процесів. У запущених процесах програма не виявила слідів програми-шпигуна. Наступним кроком було відображення прихованих процесів системи (рис. 3. 14).

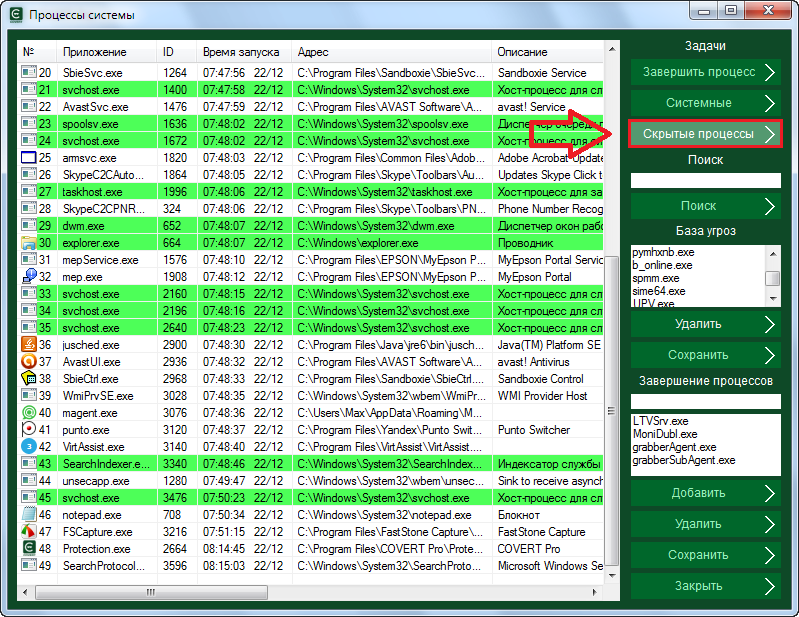


Рис. 3. 14. Монітор «Процеси системи» програми Covert

Коли відображаються приховані процеси, у системі з’являється підозріла активність: процес JetGUI.exe виділяється червоним кольором (мал. 3. 15). Тобто ця програма маскується таким чином, що вона розміщує свої процеси в списку систематично прихованому списку. На необхідних процесах клацніть правою кнопкою миші та виберіть пункт меню «Завершити процес».

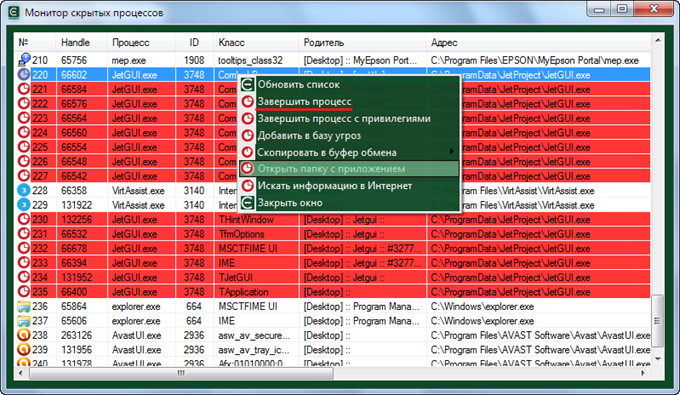


Рис. 3. 15. Монітор «Приховані процеси» програми Covert

Остання спроба - дослідити бібліотеки dll. У головному меню виберіть DLL Monitor. Відкриваючи вікно, ми помічаємо червону виділену рядок під назвою FRLib32.dll, яка допомагає приховати шпигунське програмне забезпечення на вашому комп’ютері. Клацання правою кнопкою миші на процесі відкриє швидке меню та вибере пункт меню «Відключити».

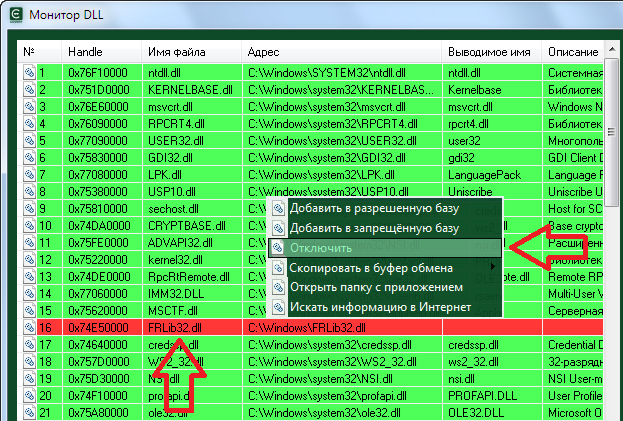


Рис. 3. 16. «Монітор DLL» програми Covert

Щоб позбутися від Jetlogger, вам потрібно знайти цю програму на своєму комп’ютері. Для цього клацніть правою кнопкою миші на рядку з назвою небезпечного процесу та виберіть пункт меню «Відкрити папку з додатком» (як показано на рис. 3. 15). Після цього в цьому ж меню виберіть пункт «Завершити процес» і видаліть папку з усім її вмістом.

Аналогічно у контекстному меню вікна DLL Monitor виберіть пункт Відключити, підтвердіть наші дії та перезавантажте комп'ютер. Після перезавантаження ОС Jetlogger буде видалено. Якщо ви не видалите Jetlogger, але перейдете на захищену камуфляжну платформу, то всі дії, які виконуються всередині (введення тексту, відвідування сайтів, перегляд відео тощо), шпигунськими програмами не будуть записані. Вхід на платформу здійснюється натисканням кнопки головного меню «Увійти в платформу захисту». Відкривши програму, ви побачите, що шпигунські журнали порожні та не мають інформації про всі дії, які були виконані всередині платформи.

Щоб перевірити реакцію звичайного антивіруса, потрібно виконати ці кроки перед видаленням програми. Оскільки бібліотека недоступна, але небезпечний процес не був виявлений, логічним кроком було б перевірити список антивірусних винятків, до яких, звичайно, вже була папка C: \ ProgramData \ JetProject, що містить інсталятор keylogger додано. Ім'я папки дає підказку щодо імені кейлогера: JetLogger. Після видалення програми з білого аркуша антивірусу вона негайно почала реагувати на свою активність у системі (рис. 3. 17)

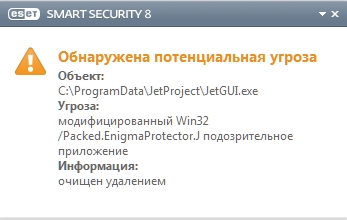


Рис. 3. 17. Реагування Eset Nod 32 на кейлогер

Доцільно використовувати утиліту JetDetecting для повного видалення компонентів програми, зокрема для видалення блокнота JetLogger, який підходить до його функцій та безпечний у використанні.

Після видалення кейлогера ми проведемо останній тест: перевірку інформації в антивірусних базах даних про небезпеку файлу JetGUI.exe (рис. 3. 18). Результати показують, що 7 з 39 доступних антивірусних програм вважають цю програму небезпечною для користувача, що є хорошим результатом, оскільки для небезпечних кейлогерів позначки можуть досягати нуля.

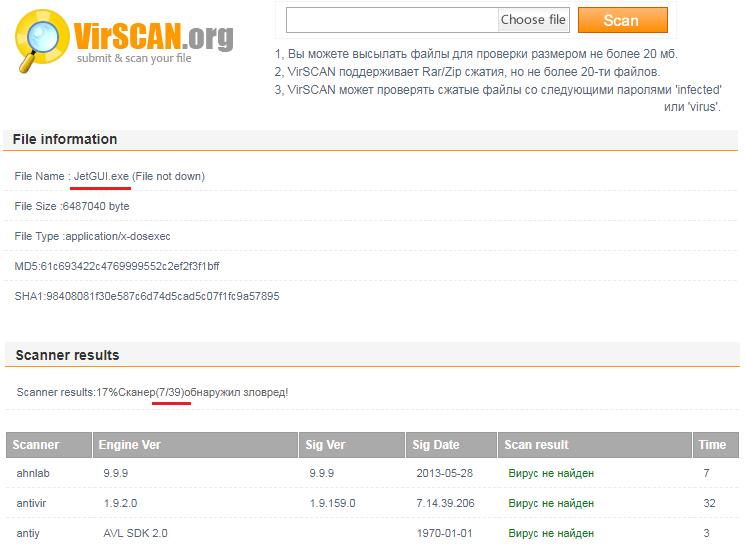


Рис. 3. 18. Реакція антивірусів на файл JetGUI.exe

### Кейлогер WebWatcher

WebWatcher, як і попередня програма, позиціонується як інструмент для моніторингу дітей та співробітників. Ця позиція допомагає вам не потрапляти в бази даних антивірусних підписів і працювати на комп’ютерах непомітно. Хоча величезний негативний вплив на його репутацію мав скандал із витоком особистих даних користувачів, які, схоже, зберігаються не лише локально на комп’ютерах, але й на віддалених серверах розробників.

WebWatcher був виявлений аналогічним чином. Після перевірки моніторів системних служб, системних процесів та моніторів драйверів результати виявилися невдалими: прихований не виявив жодних небезпечних запущених процесів. Більшість шпигунських програм легко виявляється в Мережевому моніторі маскара під час передачі інформації в Інтернет. Але WebWatcher працює набагато тонше. Він використовує для цього помилкові процеси, які жодним чином не пов’язані із записом інформації. Перший процес - iexplore.exe (веб-браузер Micosoft Internet Explorer), другий - svchost.exe (основний системний процес для завантажуваних та динамічних бібліотек). Обидва процеси належать до операційної системи, і не рідко вони знаходяться в мережевому моніторі (рис. 3. 19).

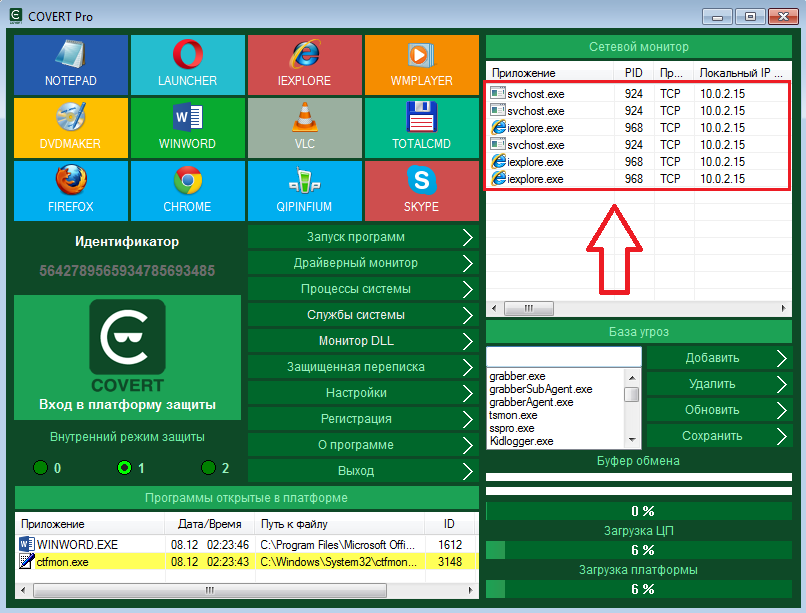


Рис. 3. 19. «Мережевий монітор» програми Covert

Спробуємо знайти шпигуна за допомогою модулів "DLL Monitor" та "File file svchost.exe".

По-перше, відкрийте DLL Monitor і відключіть контроль облікового запису UAC, якщо він включений (UAC - це контроль облікових записів користувачів Windows, ця функція запобігає несанкціонованим змінам системних файлів вашого комп'ютера). Covert має адміністративні права, а також усі його монітори. Більшість кейлогерів не мають такої можливості. Тому для детального вивчення та виявлення в системі програм моніторингу ми відключаємо UAC під час системного аналізу (рис. 3. 20). Потім потрібно перезавантажити комп’ютер, щоб зміни вступили в силу. Після дій у модулі DLL Monitor у списку завантажених бібліотек ми бачимо три бібліотеки mcsc\_wqjhqb.dll, shim\_hkcuob.dll та mcapp\_dehbkb.dll, виділені жовтим кольором, які знаходяться в папці \ \ qtqhdt32 \ \ \ \ \ \ qtqhdtg ”(рис. 3. 20). Це файли WebWatcher. Тепер давайте визначимося, кому належать файли: для цього зателефонуйте в контекстне меню на жовтому рядку та виберіть «Шукати інформацію в Інтернеті».

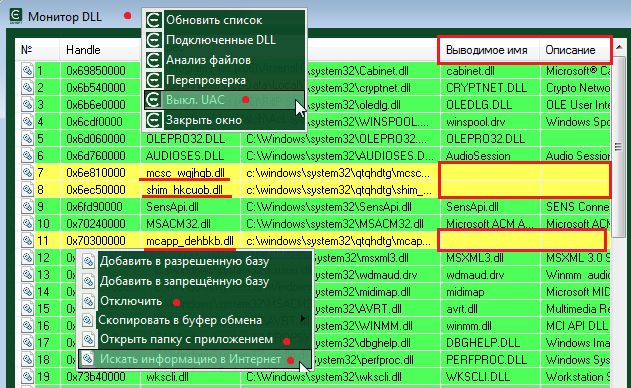


Рис. 3. 20. «Монітор DLL» програми Covert

Інформацію про дані бібліотеки не вдалося виявити, так як вони не належіть ні операційній системі Майкрософт, ні будь-якій іншій відомій компанії (Рис. 3. 21).

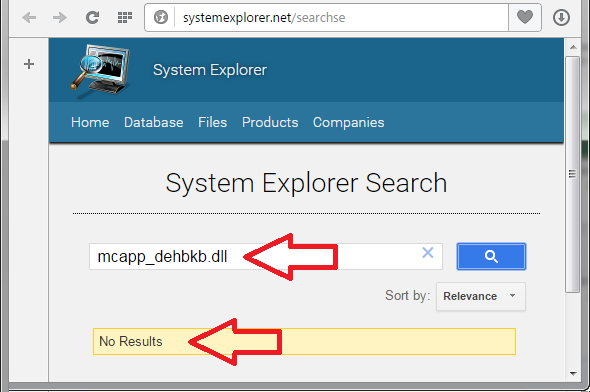


Рис. 3. 21. Інформація щодо приналежності dll- бібліотек

Ці бібліотеки не включають ім'я, опис та назву компанії розробника. Ця ситуація вимагає видалення невідомих DLL-файлів. Тепер потрібно запустити модуль системних служб, потім відобразити "Приховані сервіси" та вибрати в контекстному меню пункт "Аналізувати svchost.exe". Ця функція була спеціально розроблена для виявлення шпигунських програм, які замасковані системними процесами. У вікні системні сервіси та бібліотеки, які працюють через процес svchost.exe, виділені зеленим кольором. Жовтим кольором відображаються ті, які замасковані під системний процес. У нашому випадку ми відразу бачимо сервіс WebWatcher з назвою svcboot\_yvnhea, що працює як системний процес, з динамічно підключеною бібліотекою svcboot\_yvnhea.dll (рис. 3. 22). І це той самий шлях, що і бібліотеки-шпигуни, які були виявлені раніше.



Рис. 3. 22. Монітор "Приховані служби" програми Covert

Щоб видалити шпигунське програмне забезпечення WebWatcher, відкрийте вікно "Монітор DLL" у головному вікні маскиратора, у контекстному меню рядка модуля шпигунських програм виберіть "Відключити". Цю операцію потрібно виконати на всіх шпигунських файлах. Якщо зробити все правильно, шпигунські програми почнуть сіріти, і з’явиться повідомлення про успішну операцію.

Потім перейдіть до "Приховані служби" та виберіть "Аналіз файлів svchost.exe" у контекстному меню. У контекстному меню рядка із доданим файлом із шпигунських програм у розділі «Змінити службові завдання» натисніть «Вимкнути DLL». Якщо операція успішна, рядок з номером DLL, ім'ям та адресою стане сірим. Потім перезавантажте комп'ютер. Бібліотеки, що використовуються програмою шпигунських програм, будуть відключені. Щоб видалити папку файлів кейлогера та його інформацію, у вікні прихованих служб виберіть елемент, де зберігається інформація про шпигунське програмне забезпечення, а в контекстному меню виберіть "Відкрити папку служб", а потім "DLL". Папку разом із її вмістом потрібно видалити, а потім у підменю «Змінити службові завдання» натисніть «Очистити систему».

Після виконання вищезазначених кроків кейлогер буде видалений. Щоб замаскувати спостереження, ви повинні працювати через захищену платформу Covert.

Щоб перевірити реакцію звичайного антивіруса, перед тим, як видалити програму, необхідно перевірити список виключень антивірусу, які не мають підозрілих винятків. Тобто, антивірус не може бути виявлений антивірусом Keylogger WebWatcher.

Після видалення кейлогера ми знову перевіримо на наявність інформації в антивірусних базах даних про небезпеку файлу svscboot\_yvnhea.dll (рис. 3. 23). Результати показують, що 6 з 39 доступних антивірусних програм вважають цю програму небезпечною для користувача, що є невтішним результатом для такого небезпечного програмного забезпечення.

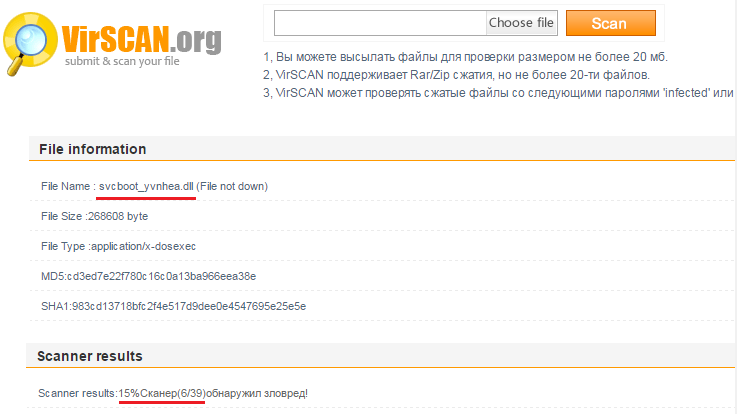


Рис. 3. 23. Реакція антивірусів на файл svscboot\_yvnhea.dll

Існує альтернативний варіант, коли цей кейлогер буде видалений із системи. Кейлогер, як програма, при своїй установці вносить зміни до багатьох частин системи, залежно від принципу її роботи. Однак для всіх програм, а також для кейлогера незмінно, він вносить певні своєрідні зміни до свого реєстру. Редагування реєстру здійснюється за допомогою редактора реєстру regedit. Щоб виявити пошкодження в реєстрі, значення реєстру порівнюються з правильними значеннями реєстру іншого комп’ютера, що призводить до ряду дефектів потенційно зараженого комп'ютера Keylogger. Ключі видаляються з реєстру, щоб видалити остаточні файли брелоків. Для кейлогерів WebWatcher це такі ключові значення:

Необхідно врахувати, що при ручному редагуванні реєстру можна видалити необхідні системі файли, після чого успішно завершити процес видалення кейлогеру можна буде лише шляхом перевстановлення Windows. Після вдалого редагування реєстру в процесному моніторі відображаються процеси, що належать кейлогеру, які необхідно завершити.

### Порівняння способів видалення кейлогерів

Існувало два способи видалення кейлогерів: приховане та редагування реєстру. Короткий опис наведено в таблиці 3.2.

Таблиця 3.2.

Порівняння способів видалення кейлогера

|  |  |  |
| --- | --- | --- |
| **Показник** | **Видалення за допомогою програми Covert** | **Ручне видалення** |
| Безпека даних | Безпечно | Можна видалити необхідні дані з реєстру або системні файли |
| Надійність видалення | 95% | 60%, не можна дізнатися, чи видалився кейлогер повністю |
| Наявність слідів кейлогеру у диспетчері процесів | Немає | Немає |

Тому зрозуміло, що для видалення кейлогера доцільно використовувати спеціалізоване програмне забезпечення, або, якщо ви можете відкрити сам кейлогер, краще видалити його через графічний інтерфейс, який назавжди видалить усі його файли та компоненти.

У таблиці 3.3 показано ефективне порівняння кейлогерів після їх використання та інформація про них.

Таблиця 3.3.

Порівняння кейлогерів

|  |  |  |
| --- | --- | --- |
| **Показник** | **Jetlogger** | **Elite Keylogger** |
| Необхідність вимикання антивірусу при встановленні | Необхідно | Необхідно |
| Наявність процесів та служб в диспетчері задач | Немає | Немає |
| Наявність у «Встановленні та видаленні програм» | Немає | Немає |
| Додавання виключень до реєстру | Вручну | Автоматично |
| Вплив на продуктивність комп’ютеру | Непомітний для системи | Дуже великий вплив |
| Поширеність утиліт для видалення | Середня | Висока |

## Зняття інформації з бездротових пристроїв

Зараз бездротові пристрої набувають популярності. Це миші, клавіатури, дзвінки, навіть розетки. Більшість з них підключається до комп'ютера за допомогою радіо. Часто розробники використовують протоколи записів на своїх пристроях, не замислюючись про безпеку. На сьогоднішній день дуже мало клавіатур, на яких вбудований модуль шифрування даних, тому ця зона є дуже спокусливою для зловмисників. Перехоплення радіохвиль таке:

3. Антена, приєднана до приймача, приймає сигнали з повітряної хвилі.

4. Виділяється ділянка ефіру, що починається у заздалегідь заданій точці, його ширина за замовчуванням становить 3 МГц, чіп E4000 посилює даний розділ.

5. Чіп приймача оцифровує цей розділ і передає його через USB на комп'ютер.

6. Програма (GnuRadio, HDSDR та ін.) Налаштовує на вибрану частоту в межах вибраного раніше 3 МГц, виконує демодуляцію у визначеному порядку і передає отриманий звук на звукову карту. Він також надсилає команди мікросхем E4000 для перенастроювання в інший діапазон.

### Опис пристрою для прийому сигналу

HackRF One зазвичай використовується для прийому сигналу, свого роду унікального пристрою, який не тільки приймає, але і передає радіосигнали в діапазоні 1 МГц-6 ГГц з пропускною здатністю до 20 МГц. Але оскільки інформація потрібна лише для отримання даних, можна використовувати її бюджетну версію, DVB-тюнер RTL-SDR, який працює в діапазоні 60-1700 МГц, який буде використовуватися в цьому тесті.

Для налаштування програмного забезпечення для Windows вам потрібно завантажити інсталятор, що містить драйвер для RTL2832, плагін для програми Gqrx та саму програму Gqrx. Після цього Zadig починає встановлювати драйвер WinUSB. Зазвичай тюнер називається "Bulk-In, інтерфейс 0". Після установки програма запускається. Перший раз, коли ви відкриєте вікно, відкриється плагін RTL2832. Після налаштування приймача потрібно натиснути кнопку «Пуск» у головному вікні. Після запуску буде показаний перший записаний радіосигнал.

Зчитування інформації відбувається з бездротової клавіатури Logitech MCU3492364.

### Принцип зняття інформації

Принцип роботи цього способу є єдиним для всіх пристроїв. Тільки інтерфейс програми або спосіб підключення пристрою можуть відрізнятися. Давайте докладніше розглянемо кожен етап.

1. Визначення параметрів пристрою.

Кожен пристрій (клавіатура, миша, навушники тощо) має свій унікальний ідентифікатор, за допомогою якого можна знайти інформацію про пристрій. Дуже популярним ресурсом є https://fccid.io/, де інформація, отримана ідентифікатором, може надати інформацію, необхідну для зловмисника, таку як допомога щодо типу та частоти модуляції. На задній панелі клавіатури зазвичай міститься наклейка з основною інформацією про клавіатуру. З цього списку користувач цікавиться ідентифікаційним номером FCC, який пробивається на описаному вище сайті, а потім отримує цікаву інформацію (рис. 3. 24).

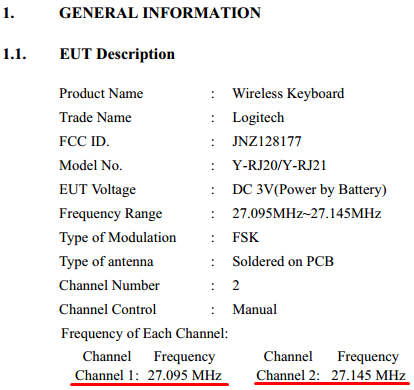


Рис. 3. 24. Інформація про частоту і вид модуляції

Дані показують, що клавіатура працює на 2 частотах: 27.095 МГц і 27.145 МГц, залежно від обраного каналу. Очевидно також, що цей пристрій використовує модуляцію FSK.

2. Пошук сигналу.

Утиліта Gqrx найчастіше використовується для контролю частотного спектру на частоті, виявленій під час OSINT. Після налаштування на необхідну частоту при використанні пристроїв з незахищеним кабелем USB спектр може бути дуже галасливим, тому виділення сигналу з клавіатури може бути майже неможливим завданням. Для цього на стандартному кабелі HackRF встановлюються феритові сердечники. Після цього спектр стає безшумним, інформаційний сигнал відображається правильно (рис. 3. 25).



Рис. 3. 25. Незашумлений частотний спектр сигналу

3. Запис та аналіз сигналів.

Для запису сигналу використовується проста схема в GNU Radio Companion. Схема включає джерело сигналу джерела осмокома та блок File Sink, необхідний для запису сигналу у файл. Сигнал джерела осмокому налаштований на середню частоту 27,08 МГц для екранування джерела живлення постійного струму. Ви можете скористатися утилітою Inspectrum для аналізу записаного сигналу. Використовуючи його (інструмент управління курсором), ви можете вибрати необхідні символи з існуючого сигналу та обчислити швидкість передачі даних.

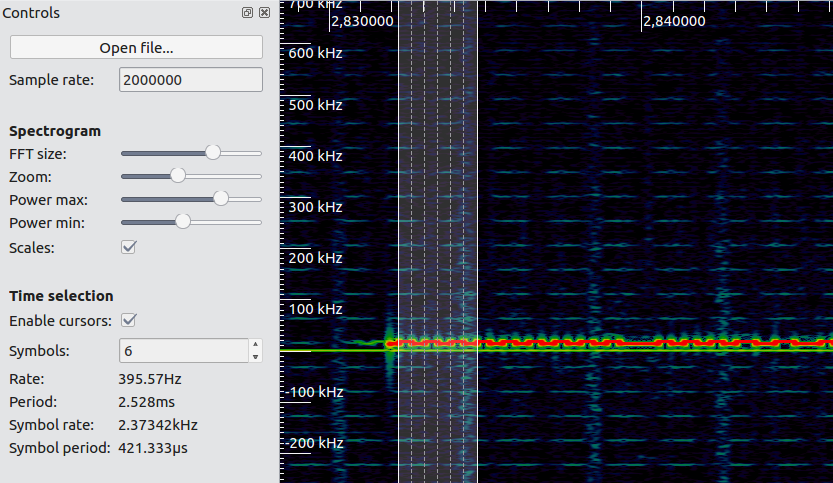


Рис. 3. 26. Аналіз сигналу в inspectrum

4. Демодуляція сигналу.

Визначивши частоту, з якою передається сигнал, швидкість передачі даних та тип модуляції, необхідно використовувати отримані значення та демодулювати сигнал для отримання інформації з нього.

З цією метою до схеми додається квадратурний блок демодуляції для демодуляції сигналу, а тип вхідного блоку File Sink змінюється на Float; додається фільтр низьких частот з частотою відсікання 50 кГц і пропускною здатністю 20 кГц. Цей фільтр передає частотний спектр сигналу нижче заздалегідь заданої частоти і пригнічує все вище.

Потім файл із записаним сигналом відкривається за допомогою утиліти Baudline, яка визначає швидкість вибірки та формат декодування. Вікно форми хвилі містить демодульований сигнал. Це призведе до шумів, які не будуть декодувати сигнал. Щоб видалити їх у існуючу схему, потрібно додати кілька блоків: блок живлення Squelch, який не пропускає сигнали, амплітуда яких нижче заданої точки, та інший фільтр низьких частот. На рис. 3. 27 ми можемо визначити амплітуду сигналу та рівень, нижчий за який користувачеві лише зайвий шум.

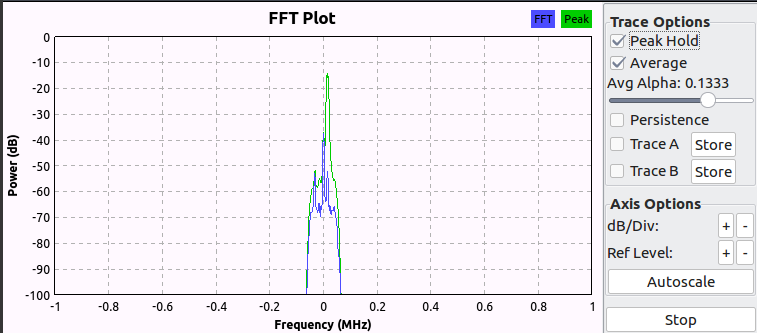


Рис. 3. 27. Амплітуда корисного сигналу

На малюнку видно, що корисний сигнал знаходиться нижче -35 дБ. Тож ви можете вирізати все нижче. Для цього встановлено значення Порогової потужності - Поріг –35 дБ. Після описаних етапів виходить чистий демодульований сигнал (рис. 3. 28).

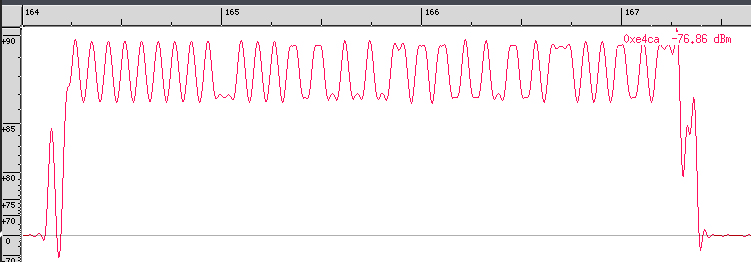


Рис. 3. 28. Демодульований сигнал

5. Розшифровка (декодування) сигналу.

Для перетворення сигналу в послідовність нулів і одиниць потрібно додати в ланцюг блок Binary Slicer. Цей блок перетворює елементи зі значеннями, що перевищують нуль, до нуля, а негативні - до нуля. Для цього додайте абсцису до сигналу за допомогою блоку Add Const (рис. 3. 29).

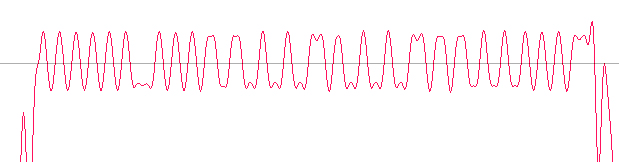


Рис. 3. 29. Підготовлений сигнал

Після отримання кінцевого варіанту схеми, необхідно відкрити файл в будь-якому hex-редакторі та визначити період сигналу, використовуючи методики коду Міллера.

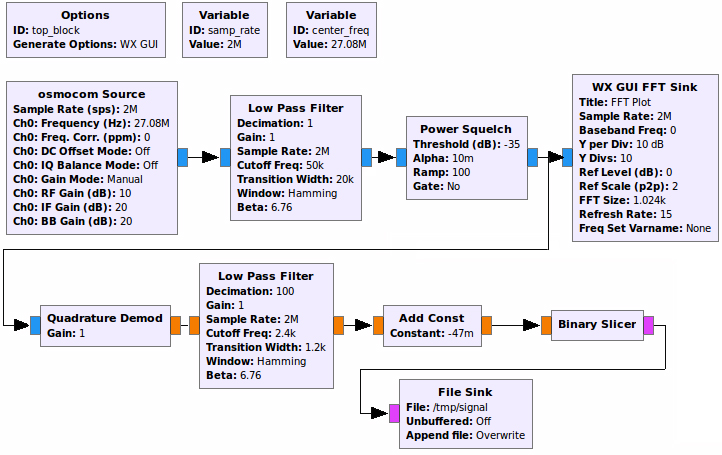


Рис. 3. 30. Схема перехоплення сигналу по радіоінтерфейсу

6. Вилучення символів.

Для вилучення символів з отриманого сигналу використовується письмовий кейлогер, вхід якого отримується нулями, а їх - блоком TCP Sink. Як правило, кейлогер використовує заздалегідь написаний скрипт (додаток В), який прослуховує порт TCP, записує всі вхідні значення та порівнює їх із складеним словником. Після одночасного запуску кейлогера та кінцевої блок-схеми символи, введені користувачем, відображаються на консолі. Таким чином, ця техніка досить проста і дозволяє перехопити сигнал з бездротового пристрою та відновити натиснуті користувачем клавіші.

Описаний найпростіший варіант, хоча найчастіше реалізується програмне забезпечення, яке надсилає натискання клавіш на віддалений комп'ютер і команди [31].

Такі атаки можливі через відсутність механізмів захисту передачі даних між бездротовим пристроєм та приймачем. Дані натискання клавіші передаються відкрито, на одній з двох частот, погоджених пристроями під час з'єднання.

### Захист від зняття інформації бездротовим способом

Таким чином, перехоплення радіоінформації та відновлення користувацьких ключів не є складним завданням. Такі атаки можливі, оскільки будь-які механізми захисту при передачі даних між клавіатурою та приймачем віддалені. Дані радіо передаються у відкритій формі на одній з двох частот, погоджених пристроями на момент з'єднання.

Для забезпечення передачі інформації рекомендується використовувати пристрої шифрування даних. Найбезпечнішою на сьогоднішній день є технологія Bluetooth 5.0. кілька пристроїв використовують технологію генерації ключів Kinit, ключ зв'язку Kab та процес аутентифікації.

Клавіша Kinit використовує алгоритм E22, який обробляє такі значення, як унікальна MAC-адреса пристрою, його пін-код, його довжина та ключ від 8 до 128 біт. Цей ключ дозволяє встановити отриману надійність шифрування відповідно до законодавства кожної країни. Тому слід зауважити, що належним чином налаштовані пристрої Bluetooth не можуть бути підключені випадково, тому випадковий витік важливої ​​інформації третім сторонам неможливий.

Залежно від виконуваних завдань специфікація Bluetooth має три режими захисту, які можна використовувати окремо або в різних комбінаціях:

1. У першому режимі мінімальний (який є типовим параметром) не вживаються кроки для безпечного використання пристроїв Bluetooth. Дані кодуються відкритим ключем і можуть прийматися будь-яким пристроєм без обмежень.

2. У другому режимі реалізується захист на рівні пристрою, тобто заходи безпеки, засновані на процесах аутентифікації та авторизації. Цей режим визначає різні рівні довіри для кожної послуги, пропонованої пристроєм. Рівень доступу можна вказати безпосередньо в мікросхемі, і відповідно пристрій буде отримувати певні дані від інших пристроїв.

3. Третій режим - це безпека на рівні сеансу, де дані кодуються 128-бітовими випадковими номерами, що зберігаються в кожній парі пристроїв, що беруть участь у певному сеансі зв'язку. Цей режим вимагає розпізнавання та використовує систему шифрування.

Зазвичай другий і третій режими використовуються одночасно. Ось чому неможливо видалити інформацію через переданий радіосигнал, оскільки всі канали зашифровані. Для забезпечення додаткового рівня захисту доцільно використовувати адаптер Bluetooth, здатний приймати та надсилати дані. Найпоширенішим на сьогоднішній день є адаптер Bluetooth 2 в 1 Vention 4.2 (NABBO). Це адаптер, який дозволяє організувати з'єднання в обох напрямках по бездротовому каналу. За допомогою цього пристрою, який працює як для передачі, так і для прийому сигналу, можливо підключити бездротові пристрої до систем, що не мають бездротового модуля. Недоліком способу є те, що всі пристрої Bluetooth працюють на акумуляторних батареях і мають обмежену ємність, тому тривале використання стає неможливим.

## Система захисту від кейлогерів

Актуальним є питання несанкціонованого видалення інформації про користувачів, таких як дані авторизації, особисті дані користувача, державна або особиста конфіденційна інформація тощо. Провівши ряд досліджень, можна констатувати, що пристрою, який би був на 100% захищений від усіх каналів збору інформації, не існує. Ось чому існує потреба в організації системи захисту від такого шпигунського програмного забезпечення, як кейлогери. На сьогодні найкращим інструментом для локально встановлених кейлогерів було програмне забезпечення Covert Pro. За допомогою цієї програми ви можете виявити, видалити або відключити майже будь-який інструмент для моніторингу активності користувачів. Бази даних цієї програми постійно оновлюються залежно від виявлення нових типів шкідливого програмного забезпечення. Однак це програмне забезпечення захищає від відомих комерційних програмних модулів. Якщо користувач є єдиною ціллю зловмисника, вдруге буде непросто створити новий програмний продукт, який не буде відомий жодним анти-кейлогерам і антивірусним базам даних.

З цієї причини рекомендується працювати в безпечному середовищі для захисту даних авторизації від кейлогерів. Для збереження паролів рекомендується використовувати програми запам'ятовування паролів, такі як KeePass. Створюючи нову базу даних паролів, ця програма пропонує ввести пароль, вибрати режим шифрування даних, функцію їх шифрування, спосіб стиснення файлу, встановити максимальну кількість паролів у цій базі даних, дату та час зміна пароля (рис. 3. 31). У цьому випадку, коли ви потрапите на комп'ютер користувача келоггера, всі дані вже будуть міститися в єдиній базі даних, до якої можна отримати доступ за допомогою ключа Bluetooth, що містить електронний цифровий підпис або дані біометричного доступу користувачів.

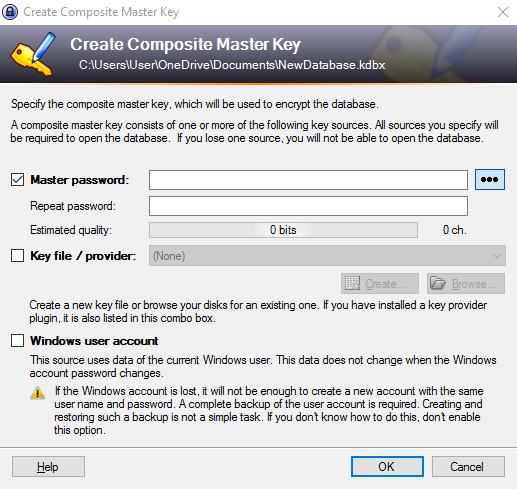


Рис. 3. 31. Створення паролю для програми KeePass

Процес додавання нового паролю на Рис. 3. 32.

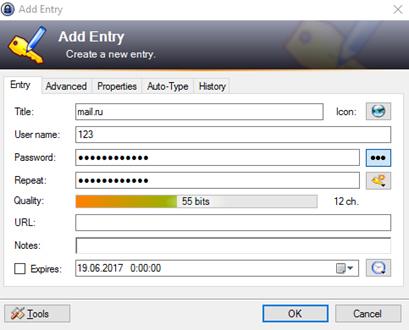


Рис. 3. 32. Додавання паролю до бази даних KeePass

Після цього в базі даних створюється база даних, яка дає можливість скопіювати у буфер обміну логін або пароль або необхідну інформацію облікового запису. Ви також можете використовувати додатки веб-переглядача, такі як програма PassChesk Google Chrome. Щоб увійти в цю програму, ви повинні ввести пароль, і тоді всі логіни та паролі, що зберігаються в ній, автоматично будуть вставлені в необхідні поля.

Для критично важливої ​​інформації доцільно використовувати віртуальні операційні системи. Переважна більшість кейлогерів пов'язана з поточною операційною системою, незалежно від того, чи вони базуються на драйверах чи на пастці.

Бездротові пристрої повинні використовувати додаткові адаптери Bluetooth на основі технології 5.0, які забезпечують зашифрований канал даних.

Тобто реалізована система захисту кейлогерів складається з таких компонентів:

1. Остання версія Covert Pro з оновленими базами даних.

2. Програмне забезпечення KeePass для створення єдиної бази даних авторизації.

3. Використання віртуальних операційних систем для створення, передачі та обробки конфіденційної інформації.

4. Використання адаптерів Bluetooth на основі технології 5.0 для бездротових пристроїв.

Також слід пам’ятати про наявність апаратних кейлогерів. Щоб захистити їх, слід періодично перевіряти комп'ютер на предмет підозрілих пристроїв, що містяться між USB-роз'ємом та виходом, наприклад.

* 1. Висновки до розділу

У цьому розділі описані найпоширеніші кейлогери, їх специфіка, функціональність, особливості установки. Переглядається приховане програмне забезпечення для моніторингу стану робочого середовища, драйверів, системних процесів та послуг. Розглянуто два можливі способи видалення кейлогерів та аналізу загроз, виявлених програмою. Окреслено можливі варіанти захисту від видалення інформації про конфіденційні, конфіденційні та особисті дані користувачів.

Тепер кейлогери фіксують інформацію не тільки про натискання клавіш, як спочатку передбачалося, але й роблять скріншоти, знімки з веб-камери, відстежують активність в Інтернеті, окремо в пошукових системах, відрізняють введення пароля від іншої інформації, копіюють вміст буфера обміну, поштова кореспонденція, тобто вони беруть на себе всі функції систем моніторингу. Виявлення кейлогерів безпосередньо залежить від способу їх реалізації: пошук драйверів кейлогерів слід шукати в процесах і списках драйверів, кейлогери на основі пасток клавіатури повинні виявлятися за допомогою моніторингу бібліотек DLL,

Для захисту кейлогерів використовується різноманітне програмне забезпечення. Але з розвитком програм безпеки царство шпигунських програм не вийшло. Так, за останній рік кількість відомих кейлогерів подвоїлася. Більше того, слід враховувати, що не всі вони відомі. Державне програмне забезпечення, інформація про розкриття якого не є загальнодоступним, становить велику небезпеку.

На сьогоднішній день на ринку програмного забезпечення для боротьби з кейлогерами представлено широке розмаїття систем. Великий відсоток програм оплачується, але це не завжди означає, що поточна доступність баз даних цих програм відповідає заявленій вартості, тому ви повинні нести відповідальність за вибір програмного забезпечення для захисту свого комп’ютера.

# ВИСНОВКИ

При виконанні дипломної роботи було виконано ряд завдань:

Досліджено методи виявлення та захисту від кейлогерів

Створено програмне забезпечення простої версії кейлогерів на основі циклічного опитування стану клавіатури для демонстрації перехоплення функцій API та створено систему для створення захищеного від кейлогерів середовище

Проаналізовано існуючі методи впровадження кейлогерів, способи програмного та апаратного видалення інформації за допомогою плагінів, usb-адаптерів тощо

Розглянуто основні правові положення в галузі інформаційної безпеки, описуються поняття інформації та її безпека, комп’ютери, автоматизовані та комп'ютерні системи, інтегрована система безпеки, захист від несанкціонованого доступу, цілісності, доступності, конфіденційності та безпеки

Виявлено, що заходи захисту інформації, описані в нормативних документах, передбачають усі можливі типи інформаційних загроз, створені з розрахуванням можливої ​​шкоди від їх створення та ціни заходів та обмежень безпеки

Розглянуто найпоширеніші типи кейлогерів, як вони розподіляються та створюються, приховуються, їх поточний стан; описується, як вони видаляють інформацію з комп'ютера користувача, та визначає основні причини її створення

Розглянуто принципи роботи, встановлення, приховування кейлогерів

Визначено, що для захисту кейлогерів використовується різноманітне програмне забезпечення

Зроблено висновки, що досить важко повністю виявити наявність кейлогерів у системі. Неможливо також бути впевненим, повністю вилучено його з системи чи ні. В даний час видно, що антивірусне ПЗ розвивається в тому ж темпі що і шкідливе ПЗ, так з часом користувачі можуть знайти спосіб повного захисту від кейлогерів

# СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності [Електронний ресурс]. - Режим доступу: http://www.viche.info/journal/598/.
2. Закон України «Про національну безпеку України» [Електронний ресурс]: № 2469-VIII від 21.06.2018; // Сайт Верховної Ради України. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19>.
3. Основні положення інформаційної безпеки в нормативно-правових актах [Електронний ресурс]. - Режим доступу: http://cryptohistory.ru/pages/npzib-01/.
4. Закон України «Про інформацію» [Електронний ресурс]: № 2657-XII [Редакція від 02.10.1992 р.]; // Сайт Верховної Ради України. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12/ed19921002?head=1>.
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс]: № 1170-VII [Редакція від 19.04.2014 р.]; // Сайт Верховної Ради України. – Режим доступу: https://zakon2.rada.gov.ua/laws/show/80/94-вр.
6. Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 08.10.97 р. № 1126. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1126-97-п.
7. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – [Чинний від 1997–01–01] . – Київ : Держспоживстандарт України, 2006. – ІV, 192 с. – (Національний стандарт України). [Електронний ресурс] <http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id=38836>
8. Положення «Про технічний захист інформації в Україні» затверджено постановою Кабінету Міністрів України від 27.09.1999 № 1229/99. [Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1229/99.
9. НД ТЗІ 3.6-001-00 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 20.12.2000 р. №60.
10. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.
11. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.
12. НД ТЗІ 2.5-004-99 Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.
13. Keylogger [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Keylogger.
14. Зайцев О. В. Rootkits, spyware, adware, keyloggers, backdoors. Обнаружение и защита. / О.В. Зайцев. – СПб.: БХВ-Петербург, 2006. – с. 248.
15. Кейлогеры: теория и практика [Електронний ресурс]. – Режим доступу: https://tov-nachoperot.livejournal.com/9503.html.
16. Зайцев О. В. Rootkits, spyware, adware, keyloggers, backdoors. Обнаружение и защита. / О.В. Зайцев. – СПб.: БХВ-Петербург, 2006. – с. 219.
17. Клавиатурные шпионы [Електронний ресурс]. – Режим доступу: http://z-oleg.com/secur/articles/keylogger.php.
18. Современные программные и аппаратные клавиатурные шпионы [Електронний ресурс]. - Режим доступу: https://www.z-oleg.com/secur/articles/keylogger2.php.
19. Современные клавиатурные шпионы [Електронний ресурс]. - Режим доступу: http://compress.ru/article.aspx?id=15847.
20. Keylogger: найти и обезвредить [Електронний ресурс]. - Режим доступу: http://pro-spo.ru/antivir/4030-keylogger-najti-i-obezvredit.
21. GetKeyboardState function [Електронний ресурс]. - Режим доступу: https://msdn.microsoft.com/enus/library/windows/desktop/ms646299(v=vs.85).aspx.
22. Компьютерная контрразведка или кто следит за нами [Електронний ресурс]. - Режим доступу: https://it.wikireading.ru/53029.
23. Что такое одноразовый пароль? [Електронний ресурс]. - Режим доступу: https://www.protectimus.com/ru/how-it-works.
24. Что такое Keylogger (кейлогер): шпионаж чистой воды на ПК [Електронний ресурс]. - Режим доступу: https://sonikelf.ru/keylogger-chto-eto-ili-shpionazh-chistoj-vody-na-pk/.
25. Основні заходи інформаційної безпеки [Електронний ресурс]. - Режим доступу: https://stud.com.ua/84352/ekonomika/osnovni-zahodi-informatsiynoyi-bezpeki.
26. Проактивные методи антивирусной защиты [Електронний ресурс]. - Режим доступу: https://www.anti-malware.ru/analytics/Technology\_Analysis/antivirus-protection-proactive-methods.
27. Двухфакторная аутентификация: что это и зачем оно нужно? [Електронний ресурс]. - Режим доступу: https://blog.kaspersky.ru/what\_is\_two\_factor\_authenticatio/4272/.
28. Зайцев О. В. Rootkits, spyware, adware, keyloggers, backdoors. Обнаружение и защита. / О.В. Зайцев. – СПб.: БХВ-Петербург, 2006. – с. 238.
29. 4 шляхи протидії кейлогерам. [Електронний ресурс]. - Режим доступу: http://www.makeuseof.com/tag/4-ways-protect-keyloggers/
30. COVERT — программа антишпион для Windows [Електронний ресурс]. - Режим доступу: https://covert.ru/about-covert/description/.
31. Взлом беспроводной клавиатуры [Електронний ресурс]. - Режим доступу: https://xakep.ru/2017/06/22/wireless-keyboard-hack-keylogger/.
32. Кейлоггер [Електронний ресурс]. - Режим доступу: <https://www.keylogger.org/ru/keylogger.html>.
33. Keylogger [Електронний ресурс]. - Режим доступу: <https://uk.wikipedia.org/wiki/Keylogger>.
34. Клавиатурные шпионы [Електронний ресурс]. - Режим доступу: <https://compress.ru/article.aspx?id=11114>.