

Лабораторна робота № 1(1.3.6)

Завантаження та відкриття Kali Linux у Virtual Machine

Хід роботи:

Завдання 1: Задеплоїти пре-білд модифікованого Kali Linux у Virtual Machine. Для виконання цього завдання було встановлено Oracle Virtual Machine та .ova файл з модифікованим Kali Linux.

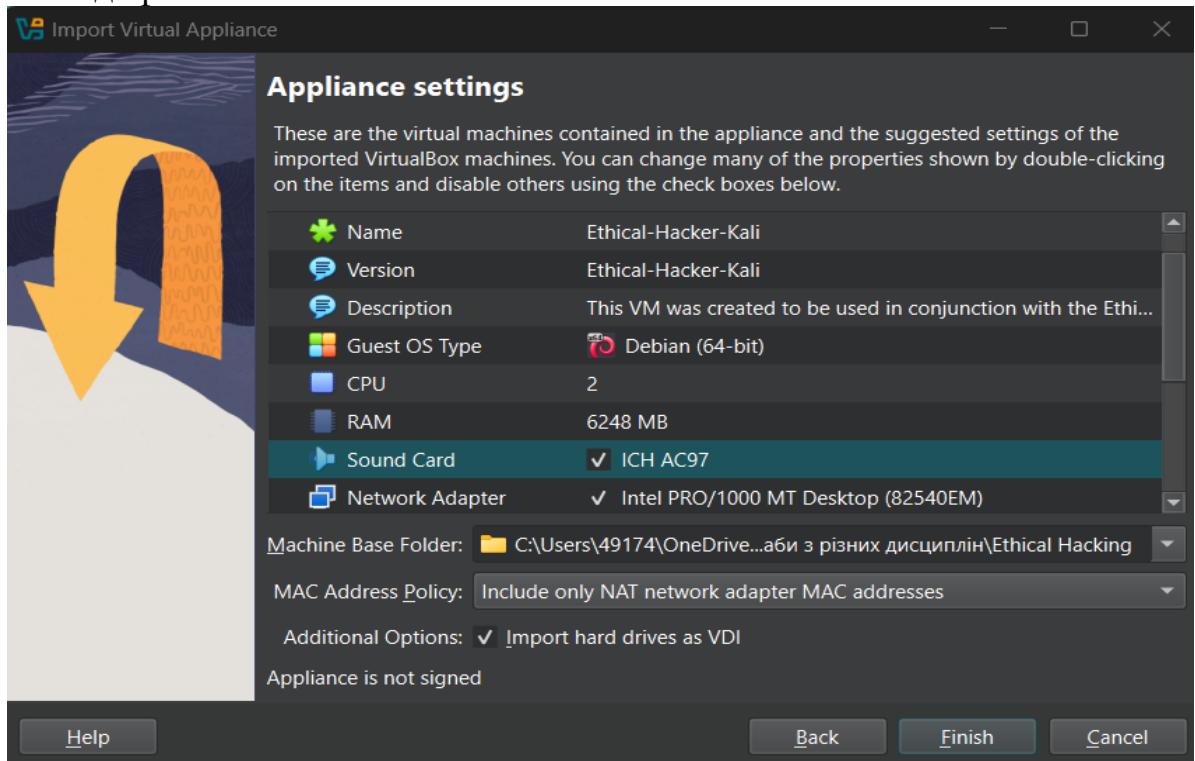


Рис. 1. Імпорт віртуальної машини за допомогою .ova файлу.

Результат виконання:

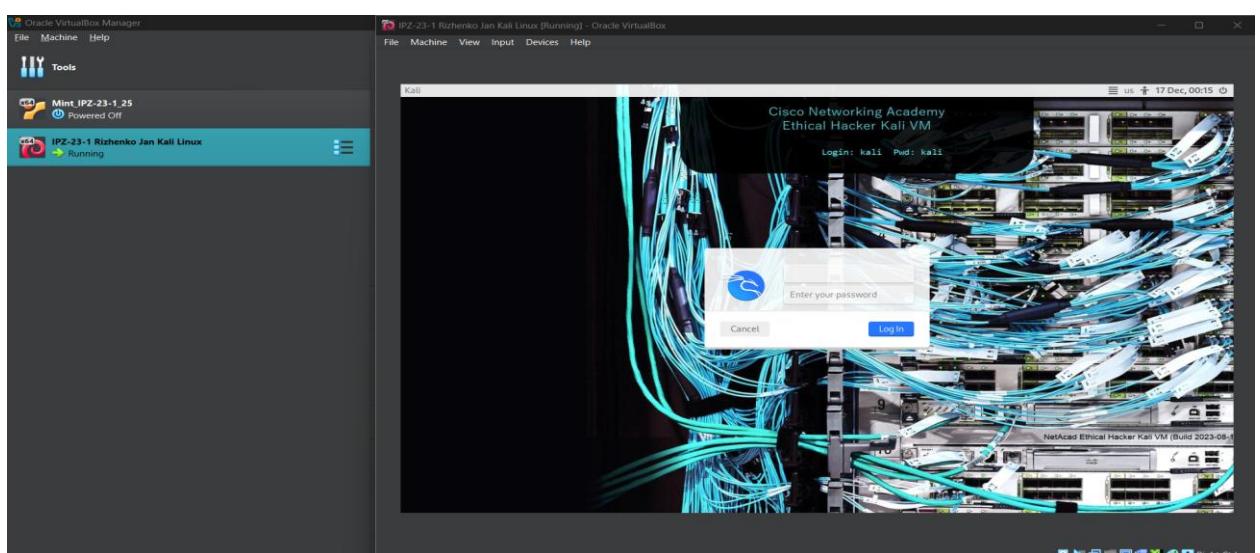


Рис. 2. Kali Linux було встановлено та налаштовано.

Змн.	Арк.	№ докум.	Підпис	Дата	ДУ «Житомирська політехніка».23.121.20.000 – Лр1(1.3.6)		
Розроб.	Рижсенко Я.В						
Перевір.	Покотило О.А.						
Керівник							
Н. контр.							
Зав. каф.							
Звіт з лабораторної роботи					Лім.	Арк.	Аркушів
						1	5
					ФІКТ Гр. ІПЗ-23-1[2]		

Завдання 2: Дослідіть можливості Kali Linux та дайте відповідь на запитання

Привілеї root

У Linux користувач **root** має повні адміністративні права, аналогічні користувачу Administrator у Windows. Команди **su** та **sudo** використовуються для отримання підвищених привілейв. Команда **su** переводить користувача в обліковий запис **root** після введення пароля **root**, а команда **sudo** дозволяє виконати одну команду з правами **root**, використовуючи пароль поточного користувача. У попередньо налаштованій системі Kali Linux користувач **kali** має право використовувати **sudo**.

Під час введення команди:

visudo

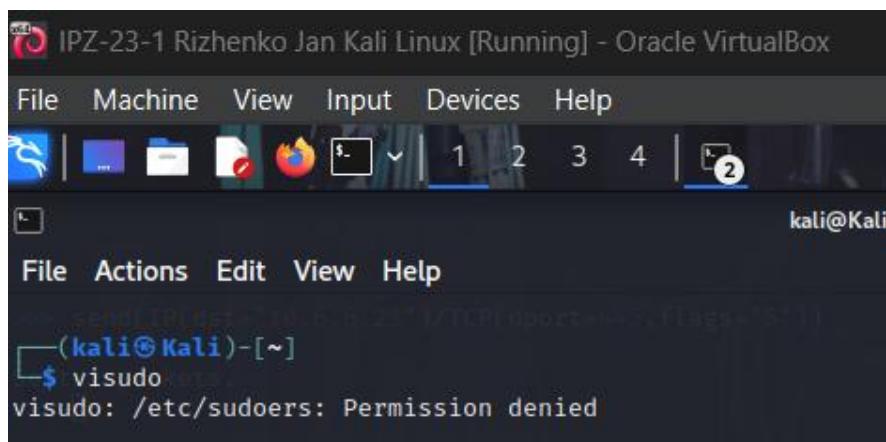


Рис. 3. Результат виконання команди visudo.

система повертає повідомлення **Permission denied**, що означає відсутність прав для перегляду та редагування файлу /etc/sudoers без підвищених привілеїв.

b.

Після введення команди:

sudo visudo

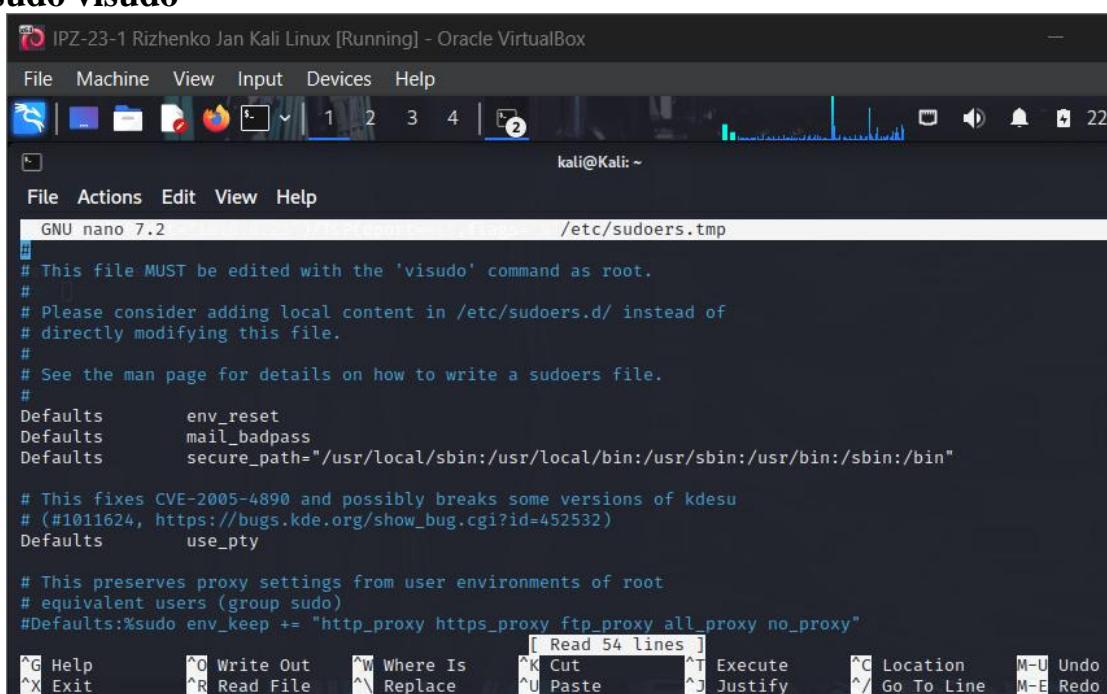


Рис. 4. Результат виконання команди sudo visudo.

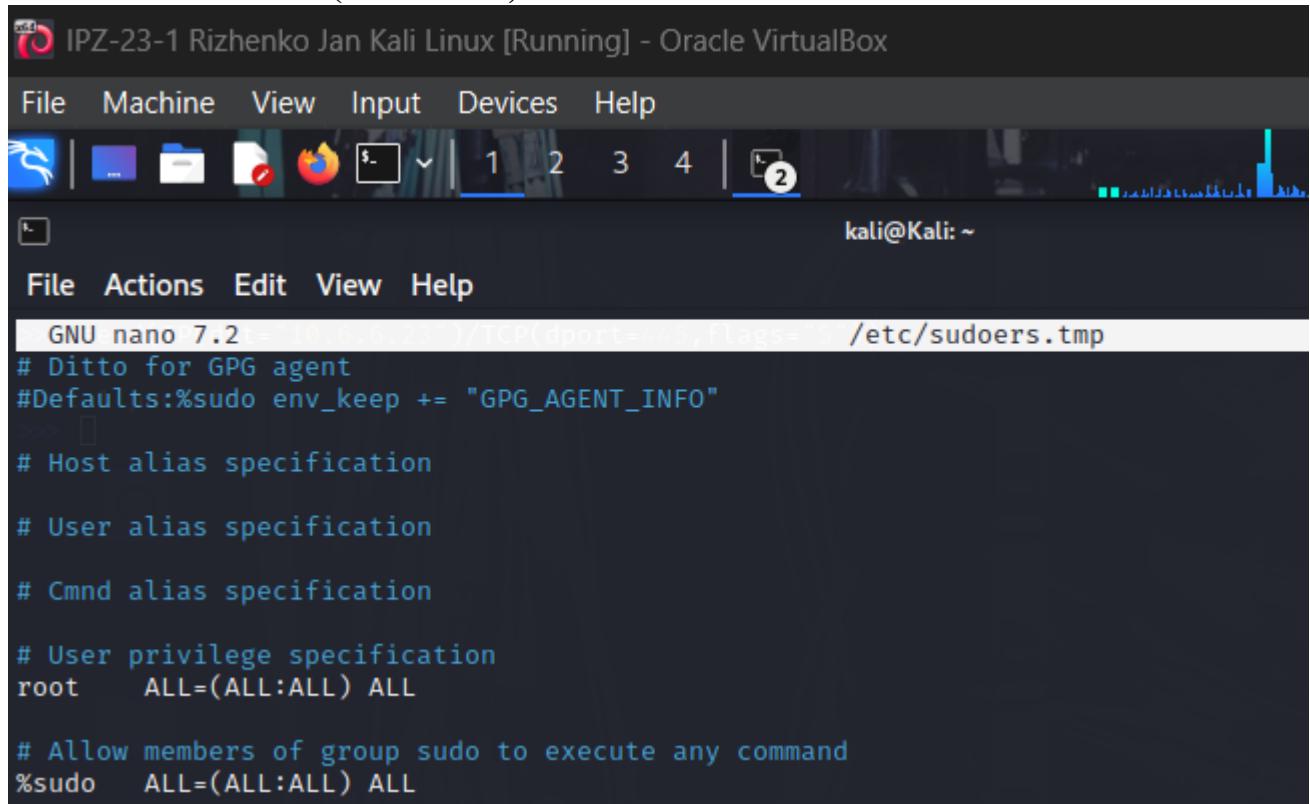
		<i>Риженко Я.В</i>				Арк.
		<i>Покотило О.А.</i>				ДУ «Житомирська політехніка».23.121.26.000 – Пр1(1.3.6)
Змн.	Арк.	№ докум.	Підпис	Дата		2

та введення пароля користувача **kali**, файл /etc/sudoers успішно відкривається, оскільки команда виконується з правами root.

c.

Наприкінці файлу /etc/sudoers присутній рядок:

%sudo ALL=(ALL:ALL) ALL



```
GNU nano 7.2                               /etc/sudoers.tmp
# Ditto for GPG agent
Defaults: %sudo env_keep += "GPG_AGENT_INFO"
>>>
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

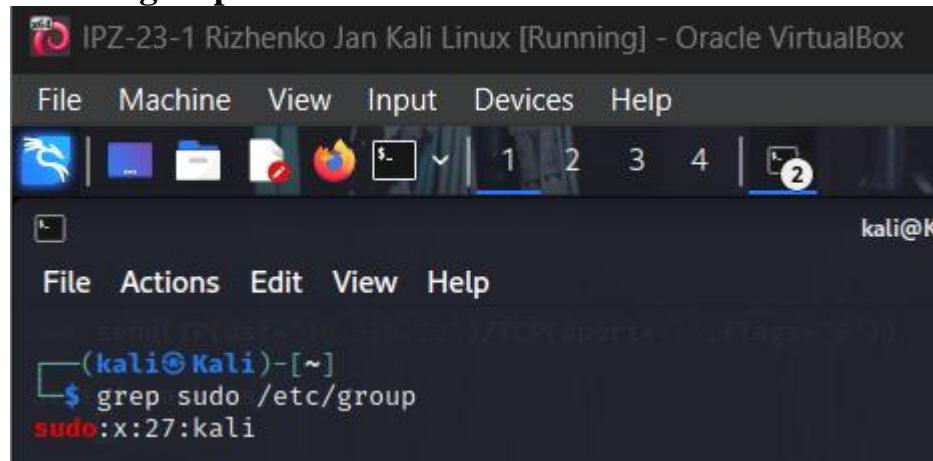
Рис. 5. Згаданий вище рядок.

Це означає, що всі користувачі, які входять до групи **sudo**, мають право виконувати будь-які команди з підвищеними привілеями. Файл було закрито без збереження змін за допомогою комбінації клавіш **Ctrl + X**.

d.

Команда:

grep sudo /etc/group



```
(kali㉿Kali)-[~]
$ grep sudo /etc/group
sudo:x:27:kali
```

Рис. 6. Результат виконання команди **grep sudo /etc/group**.

показує, що користувач **kali** входить до групи **sudo**, отже він має право використовувати команду sudo для отримання root-привілеїв.

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Пр1(1.3.6)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		3

Клавіатурні скорочення

a.

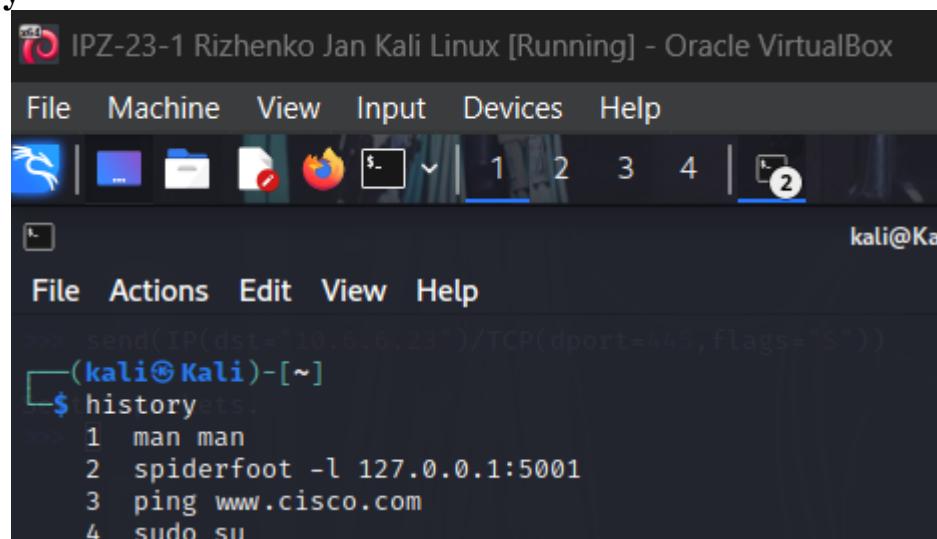
Для пошуку команди visudo за допомогою стрілки вгору потрібно було **натиснути клавішу (UP) 3 рази**.

Щоб знайти команду sudo visudo після цього, необхідно **натиснути стрілку (DOWN) 1 раз**.

b.

Команда:

`history`



The screenshot shows a terminal window titled "IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox". The terminal window has a menu bar with File, Machine, View, Input, Devices, Help. Below the menu is a toolbar with icons for file operations. The terminal itself shows the command history:

```
history
[~] $ history
 1 man man
 2 spiderfoot -l 127.0.0.1:5001
 3 ping www.cisco.com
 4 sudo su
```

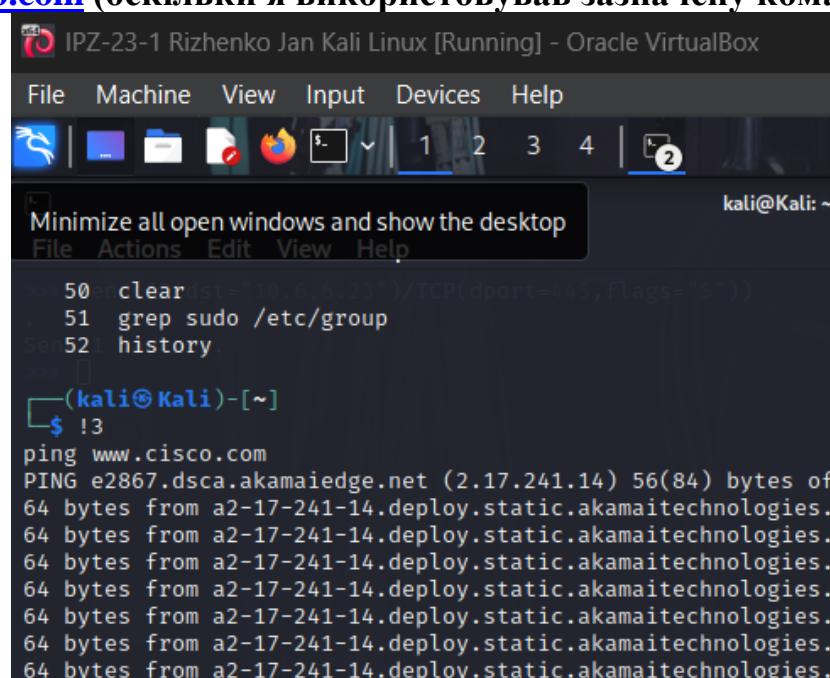
Рис. 7. Результат виконання команди `history`.

відображає список раніше введених команд у поточному терміналі разом із їхніми порядковими номерами.

c.

Після введення !3 відображається команда:

Ping www.cisco.com (оскільки я використовував зазначену команду 3 дії тому)



The screenshot shows a terminal window with a tooltip "Minimize all open windows and show the desktop" over the title bar. The terminal window has a menu bar with File, Actions, Edit, View, Help. Below the menu is a toolbar with icons for file operations. The terminal shows the command history and then the result of entering !3:

```
history
[~] $ !
 50 clear dst="10.6.6.23"/TCP(dport=445,flags="S")
 51 grep sudo /etc/group
 52 history
[~] $(kali㉿Kali)-[~]
[~] $ !3
ping www.cisco.com
PING e2867.dsca.akamaiedge.net (2.17.241.14) 56(84) bytes of
64 bytes from a2-17-241-14.deploy.static.akamaitechnologies.
```

Рис. 8. Результат введення !3.

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Пр1(1.3.6)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		4

Після введення !his відображається команда:

history

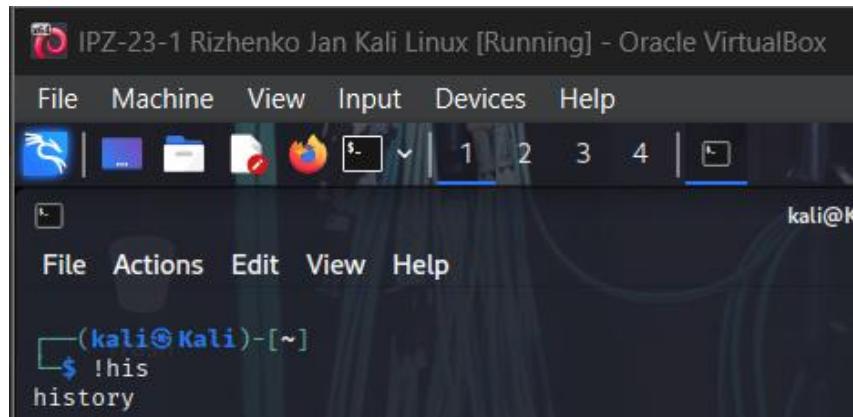


Рис. 8. Результат введення !his.

d.

Після введення hi та натискання клавіші **Tab** команда **не завершується автоматично**, оскільки існує кілька команд, що починаються з hi (наприклад, history, hping3 тощо).

e.

Після введення histo і натискання **Tab** команда автоматично доповнюється до:

history

оскільки вона є унікальною.

f.

Після введення:

ls /me

та натискання **Tab**, команда автоматично доповнюється до:

ls /media

Після натискання **Enter** відображається вміст каталогу /media.

Рефлексивне питання

Переваги використання інсталяційного образу або попередньо зібраниого образу для створення віртуальної машини Kali Linux полягають у швидкому розгортанні системи, відсутності необхідності ручного налаштування базових параметрів та гарантованій сумісності з навчальними завданнями. Попередньо зібраний образ дозволяє одразу розпочати роботу, тоді як інсталяційний образ надає більше гнучкості в налаштуванні системи відповідно до потреб користувача. Обидва варіанти спрощують процес навчання та зменшують кількість можливих помилок під час встановлення.

Висновки: Під час виконання лабораторної роботи я ознайомився з процесом завантаження та запуску Kali Linux у віртуальній машині, дослідив основні можливості операційної системи та принципи роботи з правами доступу користувачів. У ході роботи було отримано практичні навички використання команд 'su' і 'sudo', перевірки належності користувача до групи sudo, а також застосування клавіатурних скорочень і механізму історії команд для підвищення ефективності роботи в терміналі. Виконання завдання сприяло кращому розумінню основ адміністрування Linux та підготовці до подальшого вивчення систем інформаційної безпеки.

		Риженко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Пр1(1.3.6)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5