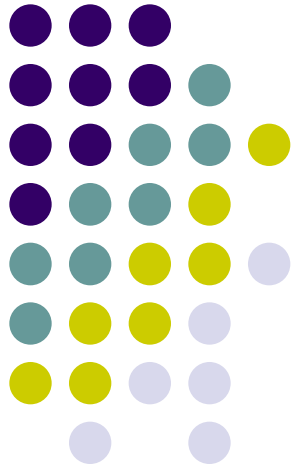
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
“ЛЬВІВСЬКА ПОЛІТЕХНІКА”

Кафедра

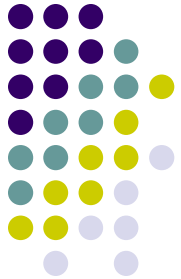
безпеки інформаційних технологій

“Дослідження способів захисту від вторгнень в мережу за допомогою підміни параметрів системи”

Дипломник: студент групи *БІ-41*
Сеніш Андрій Романович

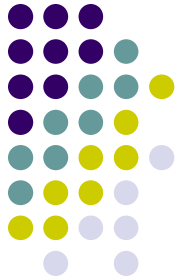


“Дослідження способів захисту від вторгнень в мережу за допомогою підміни параметрів системи”



- ***МЕТА РОБОТИ:***
- дослідження існуючих реалізацій високоінтерактивних систем для вбудованих пристроїв,
- аналіз вразливостей у вбудованих пристроях
- розробка моделі спеціальної інтерактивної системи, призначеної для дослідження поведінки злочинця у вбудованих пристроях.
- ***АКТУАЛЬНІСТЬ:*** Технологія Honeypots дозволяє відстежувати та вивчати нові способи злому, збору інформації та специфічного захисту від комп'ютерних злочинців.

Класифікація приманок



1) **Пасивні – аналізуючі** (research honeypots)

2) **Активні-виробничі** (production honeypots)

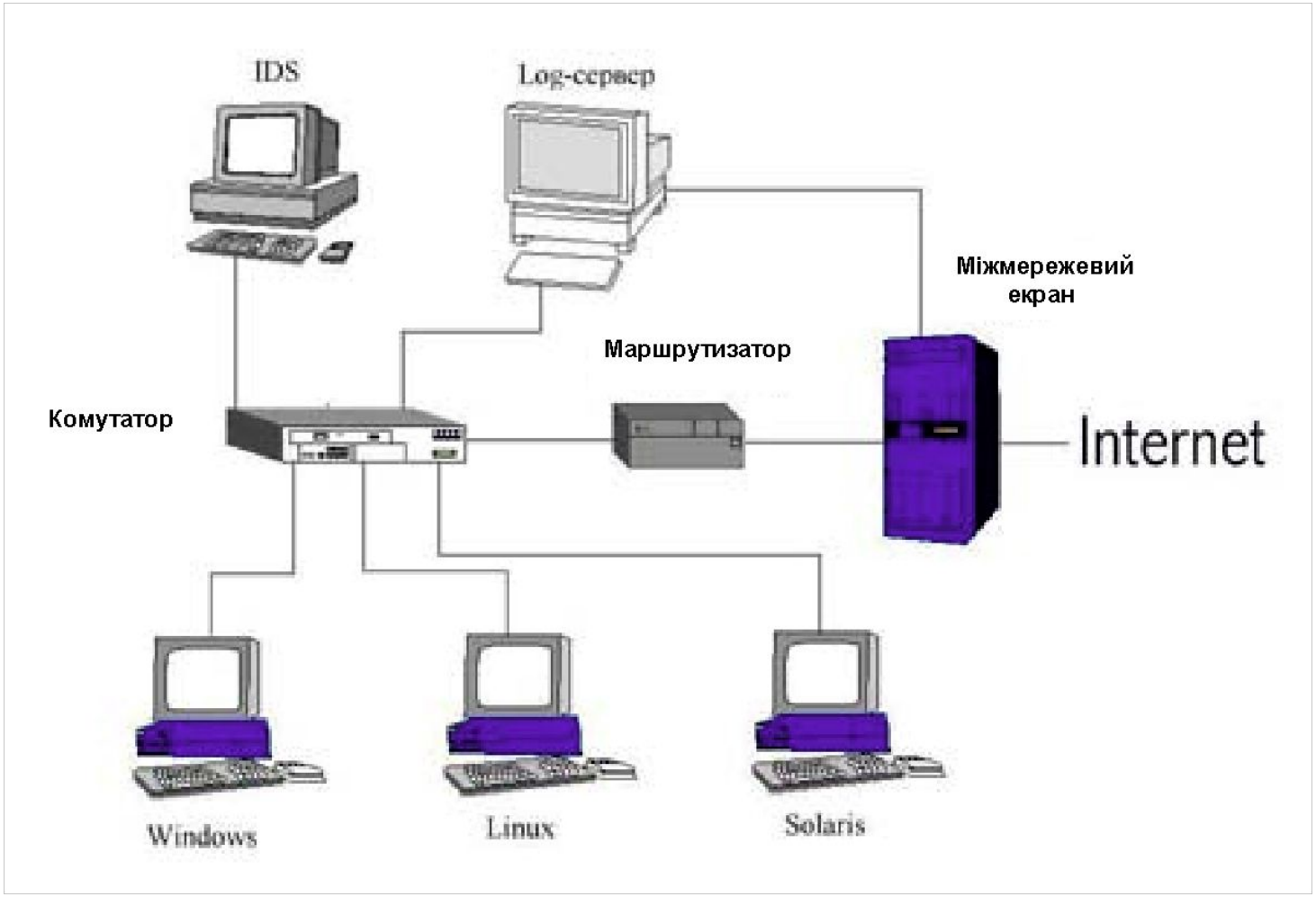
(помилкові цілі для викриття та ідентифікації нападника після того, як він раз побував у вашій організації)

Існує ще дві великі категорії :
взаємодія визначає рівень активності, який Honeypot дозволяє **атакуючому**.

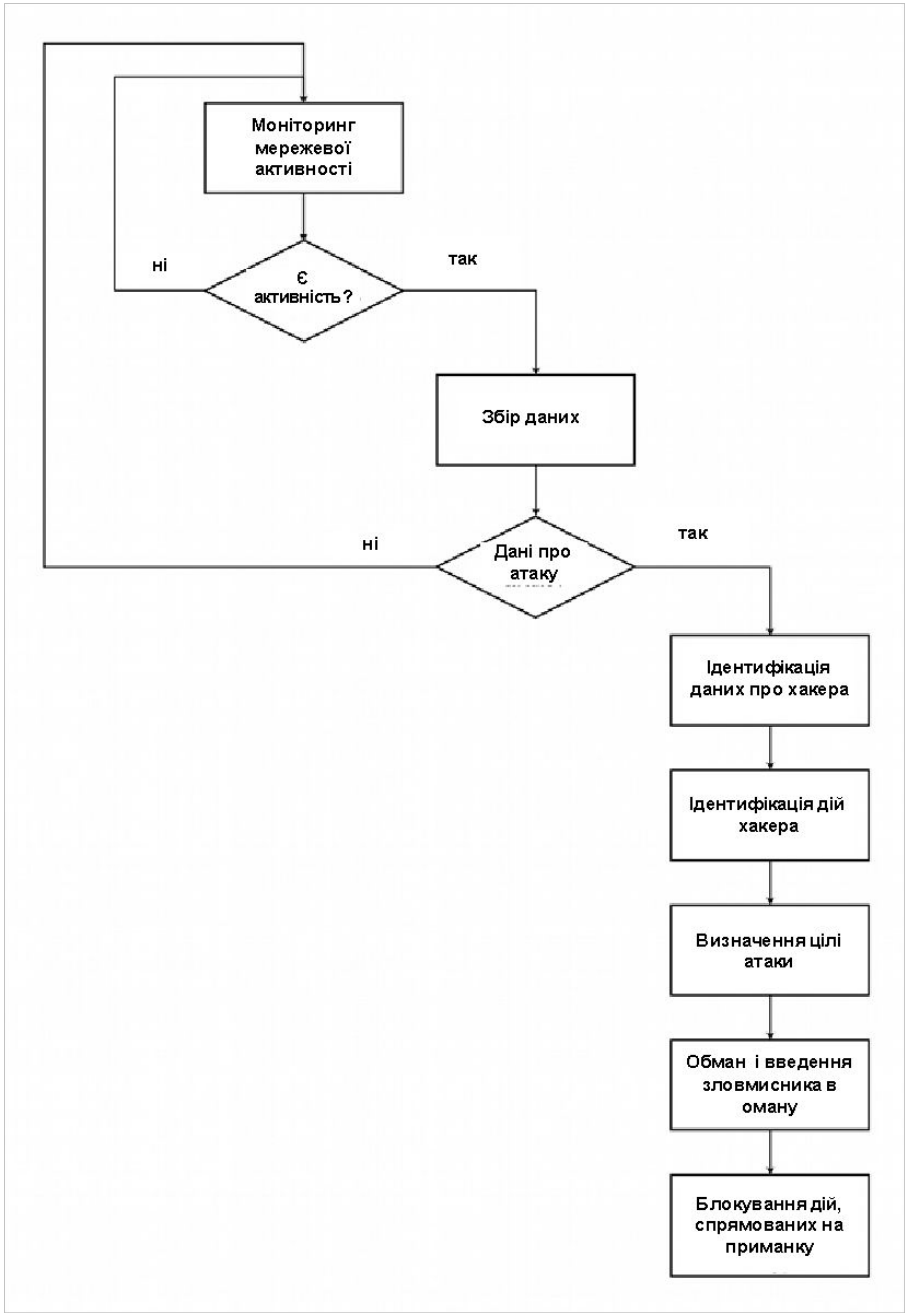
1)**низької взаємодії (low-interaction)** (емуляція сервісів і операційних систем)
Переваги: простота,
Недоліки: отримують обмежений обсяг інформації , виявляють відомі види активності злочинців, їх легко виявити.

2) високої взаємодії (highinteraction) (справжні операційні системи і програми)
Переваги: можна отримати вичерпну кількість інформації, вся активність фіксується,
Недоліки: можна використовувати реальну систему щоб атакувати інші системи, складніше розміщувати і підтримувати

Типова Honeynet, в якій honeypots представлені у вигляді різних операційних систем



Алгоритм роботи високоінтерактивної системи



Функції високоінтерактивних систем:

– збір і контроль даних (трафіку, журналів);

– виявлення атак;

– ідентифікація злочинця;

– визначення мети атаки;

- реагування на дії, блокування;

– введення в оману шляхом підміни інформації, а також шляхом зміни конфігурації;

- взаємодії адміністратора з інтерактивною системою

Схема вторгнення злочинця в високоінтерактивну систему

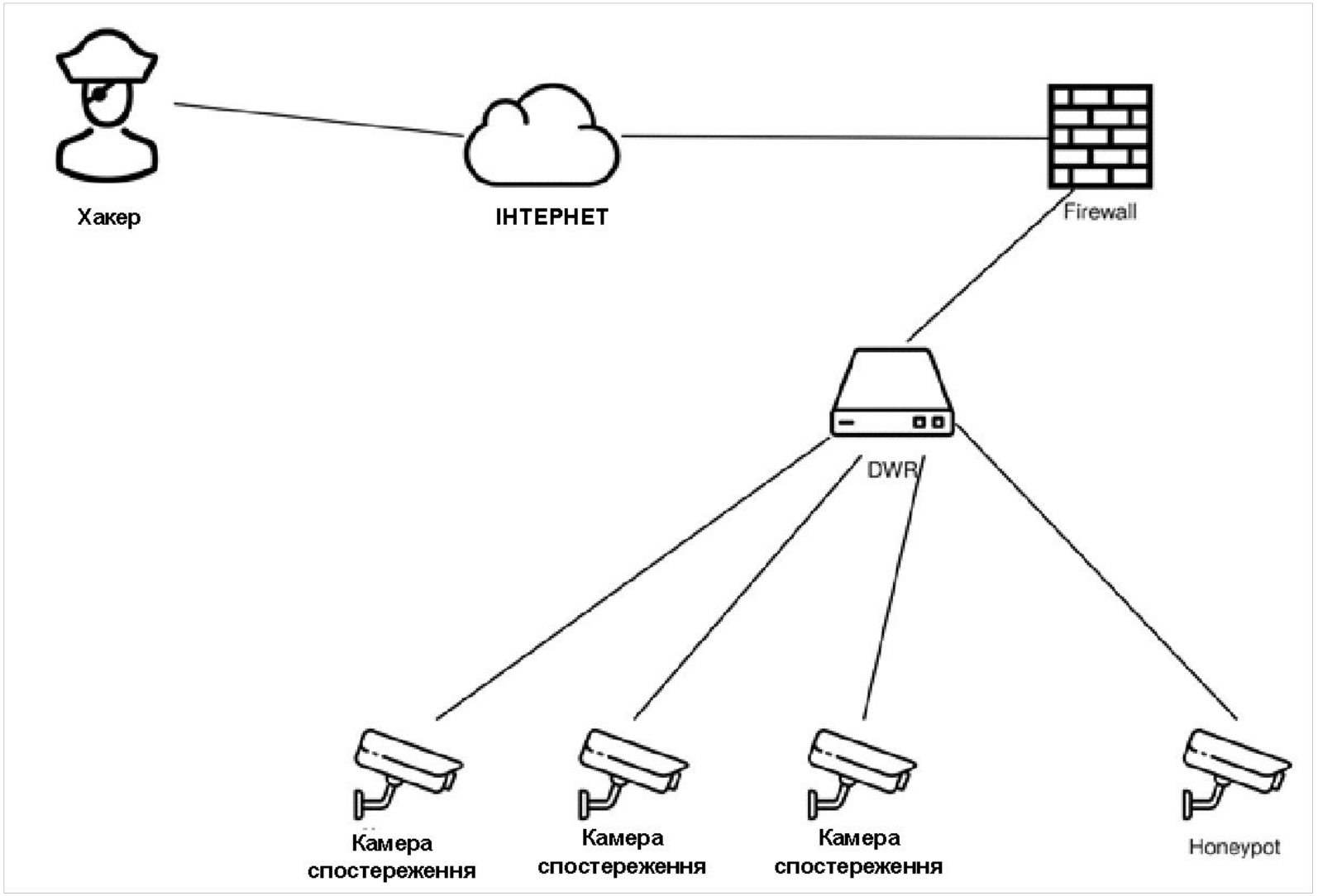
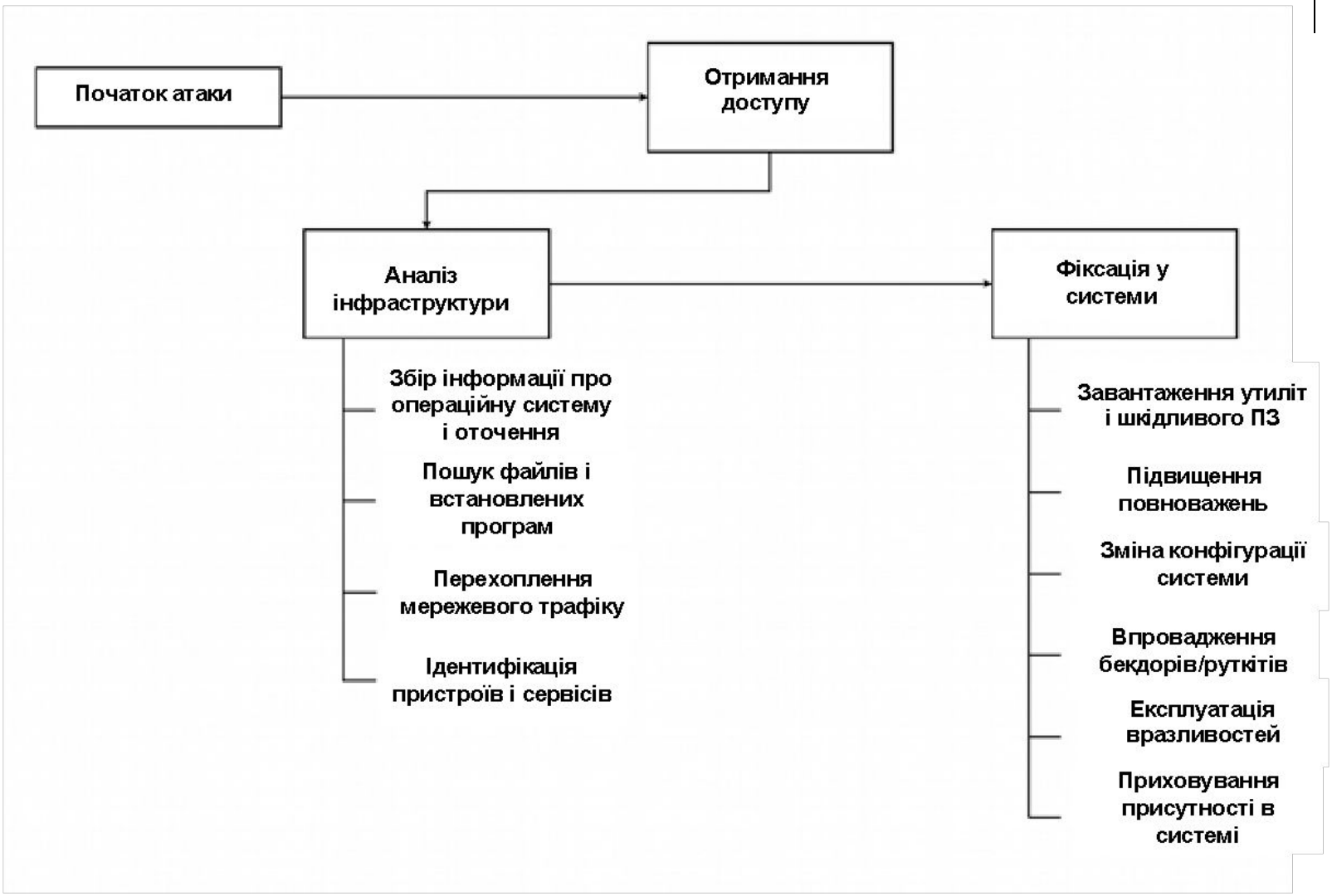
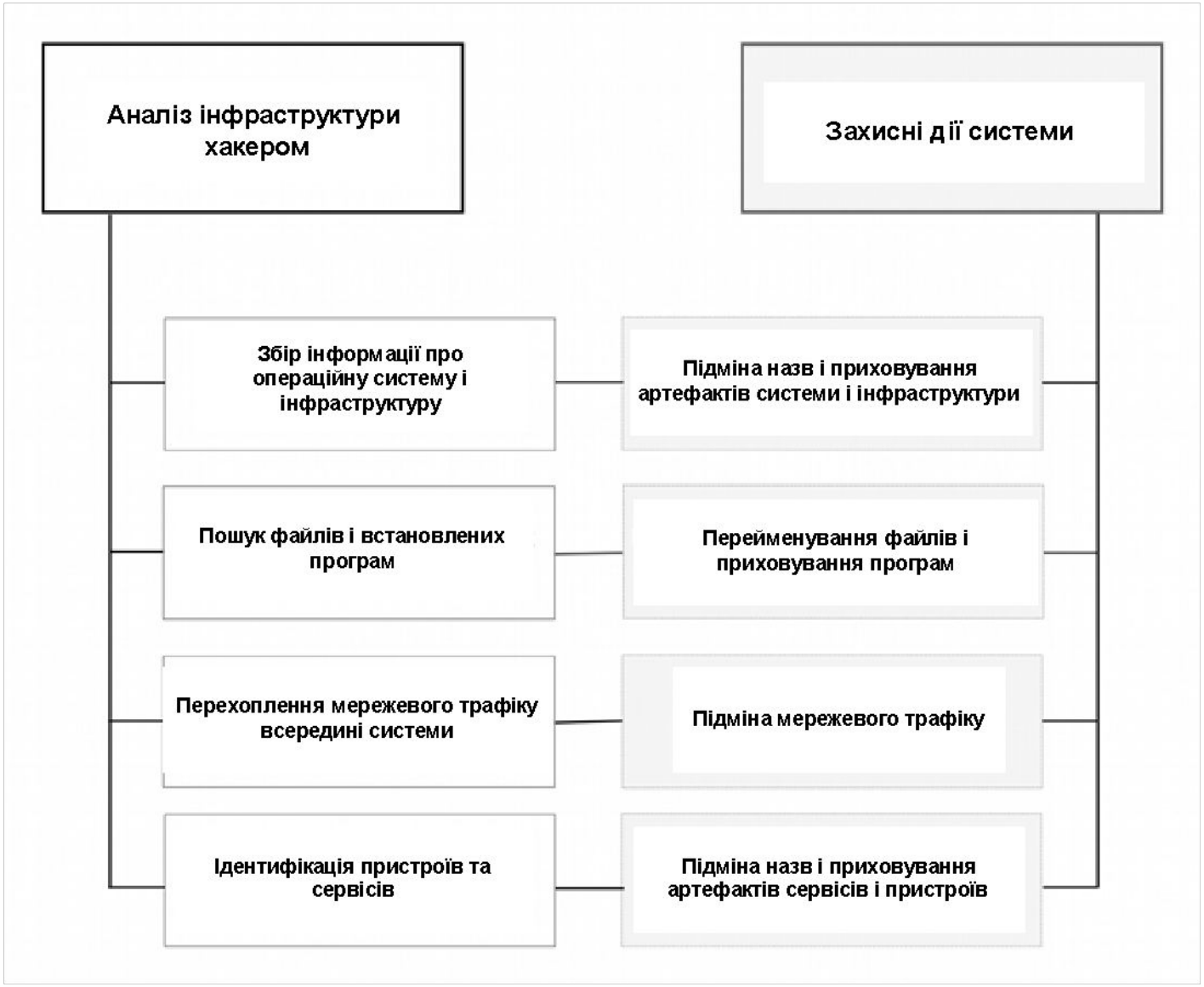


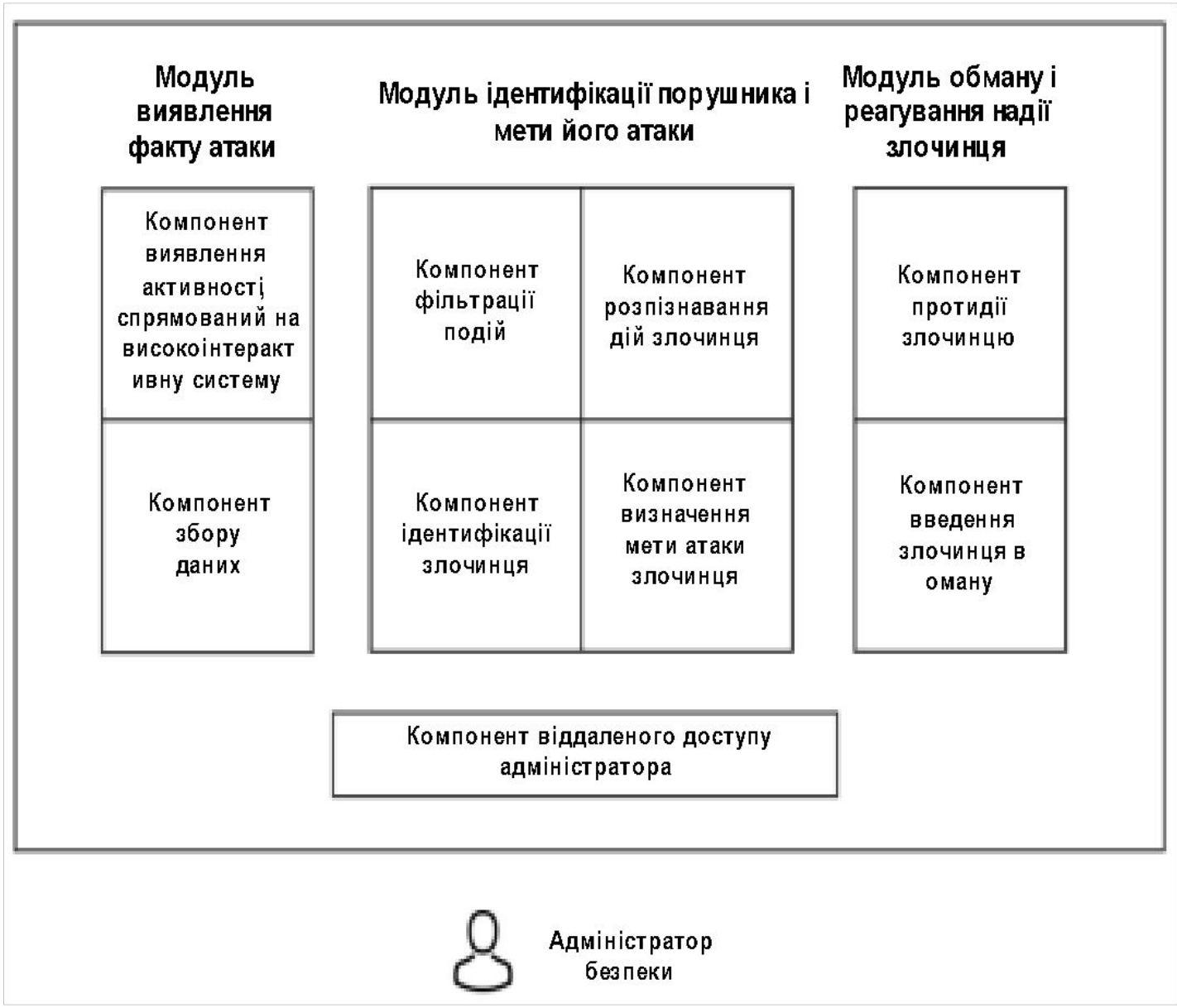
Схема поведінки злочинця у високоінтерактивній системі



Реагування високоінтерактивної системи на дії злочинця



Модель високоінтерактивної системи для вбудованих пристроїв



Дії атакуючого злочинця, які генеруються програмою event_generator

user@user:~$ docker start falcoeventgenerator

user@user:~$ docker attach falcoeventgenerator

```
***Action read_sensitive_file
Reading /etc/shadow...
***Action spawn_shell
Spawning a shell to run "ls > /dev/null" using system()...
***Action system_procs_network_activity
Becoming the program "shalsum" and then performing network activity
***Action network_activity
Opening a listening socket on port 8192...
***Action system_user_interactive
Forking a child that becomes user=daemon and then tries to run /bin/
ogin...
login: must be suid to work properly
***Action user_mgmt_binaries
Becoming the program "vipw" and then running the program /bin/ls
NOTE: does not result in a falco notification in containers
***Action exec_ls
bin       home      media     proc      sbin      sys       var
dev       httpd     mnt       root      shalsum   tmp       vipw
etc       lib       mysqld    run       srv       usr
***Action write_binary_dir
Writing to /bin/created-by-event-generator-sh...
***Action write_etc
Writing to /etc/created-by-event-generator-sh...
***Action write_rpm_database
Writing to /var/lib/rpm/created-by-event-generator-sh...
***Action change_thread_namespace
Calling setns() to change namespaces...
NOTE: does not result in a falco notification in containers, unless
ontainer run with --privileged or --security-opt seccomp=unconfined
***Action create_files_below_dev
Creating /dev/created-by-event-generator-sh...
***Action db_program_spawn_process
Becoming the program "mysql" and then spawning a shell
***Action spawn_shell
Spawning a shell to run "ls > /dev/null" using system()...
***Action exfiltration
Reading /etc/shadow and sending to 10.5.2.6:8197...
***Action mkdir_binary_dirs
Creating directory /bin/directory-created-by-event-generator-sh...
Could not create directory "/bin/directory-created-by-event-generato
-sh": File exists
```

Результати роботи прототипу високоінтерактивної системи

user@user:~$ docker start falco

user@user:~$ docker attach falco

```
12:17:35.781219878: Warning Sensitive file opened for reading by non-
trusted program (user=root name=httpd command=httpd --action read_sen
sitive_file --interval 6 --once file=/etc/shadow parent=event_generat
or gparent=<NA> ggparent=<NA> gggparent=<NA>)
12:17:42.782153835: Notice A shell was spawned in a container with an
 attached terminal (user=root falco-event-generator (id=08800c953963)
 shell=sh parent=event_generator cmdline=sh -c ls > /dev/null termina
l=34835)
12:17:43.786439406: Notice Known system binary sent/received network
traffic (user=root command=sha1sum --action network_activity --interv
al 0 --once connection=127.0.0.1:8192)
12:17:44.787677304: Informational System user ran an interactive comm
and (user=bin command=login )
12:17:46.793249399: Error File below a known binary directory opened
for writing (user=root command=event_generator  file=/bin/created-by-
event-generator-sh)
12:17:47.793455312: Error File below /etc opened for writing (user=ro
ot command=event_generator  parent=<NA> file=/etc/created-by-event-ge
nerator-sh name=event_generator gparent=<NA> ggparent=<NA> gggparent=
<NA>)
12:17:48.793816944: Error Rpm database opened for writing by a non-rp
m program (command=event_generator  file=/var/lib/rpm/created-by-even
t-generator-sh)
12:17:49.794127985: Notice Namespace change (setns) by unexpected pro
gram (user=root command=event_generator  parent=<NA> falco-event-gene
rator (id=08800c953963))
12:17:50.794327262: Error File created below /dev by untrusted progra
m (user=root command=event_generator  file=/dev/created-by-event-gene
rator-sh)
12:17:51.797383508: Notice Database-related program spawned process o
ther than itself (user=root program=sh -c ls > /dev/null parent=mysql
d)
12:17:52.801505189: Warning Sensitive file opened for reading by non-
trusted program (user=root name=event_generator command=event_generat
or  file=/etc/shadow parent=<NA> gparent=<NA> ggparent=<NA> gggparent
=<NA>)
12:17:54.802369413: Error File below known binary directory renamed/r
emoved (user=root command=event_generator  operation=rename file=<NA>
 res=0 oldpath=/bin/true newpath=/bin/true.event-generator-sh )
12:17:54.802406624: Error File below known binary directory renamed/r
emoved (user=root command=event_generator  operation=rename file=<NA>
 res=0 oldpath=/bin/true.event-generator-sh newpath=/bin/true )
```

ВИСНОВКИ

- Атаки на вбудовані пристрої, становлять велику небезпеку.

Тому, що безпека вбудованих пристроїв знаходиться на примітивному рівні. Захистом можуть бути високоінтерактивні системи, призначені для дослідження поведінки злочинців.

- Основним завданням бакалаврської роботи було створення моделі високоінтерактивної системи, яка може стати основою для створення реальної високоінтерактивної системи, що імітує будь-який вбудовуваний пристрій.
- Також сформовано вимоги, яким має відповідати модель спеціальної інтерактивної системи для вбудованих пристроїв і на підставі вимог побудована модель високоінтерактивної системи для вбудованих пристроїв.
- На підставі вищезазначеної моделі з використанням відкритого вихідного коду високоінтерактивної системи Sysdig Falco був створений прототип інтерактивної системи для вбудованих пристроїв.
- Дана модель відповідає вимогам і може використовуватися для розробки реальної високоінтерактивної системи для вбудованих пристроїв з підміною параметрів.