комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань.

Особливу увагу треба привертати підготовці особового складу НПУ до змін у загальній системі інформаційного забезпечення, а також навчання співробітників нових підрозділів грамотному використанню інформаційних систем для вирішення оперативно-службових завдань;

Також, система інформаційної безпеки має бути більш гнучкою. Треба розробляти нові методи, більш зручні у використанні, які охоплюють всі напрямки практичної діяльності НПУ. А саме збір, обробку та узагальнення оперативно-довідкової, аналітичної, статистичної та контрольної інформації для оцінки ситуації та прийняття обґрунтованих рішень на всіх рівнях управління НПУ.

Надзвичайно важливим є облік запитів поліцейських для запобігання корупції, продажу інформації з обмеженим доступом, тому він має відповідати певним критеріям захисту, таким як: двосторонній ключ або індивідуальний пароль, що має різні символи, цифри і букви, та закріплюється на певний строк.

Вирішення цих та інших завдань сприятиме створенню сучасної інформаційної системи НПУ, що сприятиме реалізації державної політики у сфері реформування системи правоохоронних органів, боротьби зі злочинністю та зменшенню кількості кібератак.

Одержано 19.04.2019

УДК 332.012+004.056

Ксенія Олександрівна КРАТАСЮК,
курсант групи Ф4-302 ХНУВС
Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

ВИКОРИСТАННЯ ДИСТРИБУТИВУ KALI LINUX У КІБЕРБЕЗПЕЦІ

На сьогоднішній день дистрибутив KaliLinux набирає велику популярність. Можливості KaliLinux зосереджені на тестуванні безпеки, це є великою перевагою над іншими операційними системами, але в той же час KaliLinux може бути використано хакерами з метою пошуку вразливостей у вашій системі – це являється недоліком дистрибутива.

Відмінності Linux від системи Windows полягає в тому, що Linux – відкритий та безкоштовний продукт, не потрібно платити за антивірусне програмне забезпечення, яке споживає багато системних ресурсів і робить ваш ПК повсякденним і потребує регулярного оновлення. Більшість LinuxDistribution має власний центр програмного забезпечення, з якого можна легко його встановити.

В Linux можна оновлювати всі системні програми з однією командою в терміналах.

Windows – дуже простий в установці та використанні, але його неможливо змінити. Необхідно встановлювати антивірусне програмне забезпечення, потрібно регулярно його оновлювати. Навіть хороший антивірус менш надійний, ніж Linux. Windows потребує великої кількості апаратних ресурсів, а також використовує пропускну здатність в антивірусному оновленні тощо.

Переваги KaliLinux. Наявні близько 600 інструментів: KaliLinux має велику колекцію інструментів тестування на проникнення; багатомовна підтримка; за допомогою KaliLinux кіберполіцейські можуть оцінити обчислювальну інфраструктуру хакерів, виявляти уразливості та цифрові сліди.

За допомогою KaliLinux можуть бути використані деякі кроки для тестування, проникнення та фіксації дії хакерів. Наприклад – розвідка, у цьому процесі кіберполіцейський збирає попередню інформацію про протиправні дії, це дає змогу краще планувати атаку. Потім – сканування, на цьому кроці використовуються технічні засоби для збору додаткової інформації про ціль, за допомогою сканера вразливостей для виявлення лазівки в безпеці цільової мережі. Деякі інструменти сканування та види атак у KaliLinux включають в себе ARP-сканування, ін'єкції jSQL, інструмент Cisco-аудит. Після чого – отримання доступу, на цьому етапі можливо проводити дії на цільовій мережі з метою вилучення деяких корисних даних для запуску додаткових атак. Деякі інструменти KaliLinux дозволяють здійснювати підтримку доступу. Крім того існують інструменти, що усувають будь-які ознаки минулої шкідливої активності в цільовій мережі. Наприклад, будь-які внесені зміни або збільшення доступу до прав, повертаються в їх вихідний статус.

Підбиваючи підсумки сказаному можна резюмувати KaliLinux є потужним інструментом для тестування на проникнення для спеціалістів з інформаційної безпеки. Користуючись KaliLinux, можна належним чином захистити критичну IT-інфраструктуру від зловмисників. KaliLinux дозволяє виконувати додаткові тестування на проникнення, щоб виявляти уразливості у вашій мережі.

Одержано 22.04.2019

УДК 343.98(477)

Данило Олександрович КУЛІКОВ,
курсант групи Ф4-302 ХНУВС
Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

ЗАСТОСУВАННЯ СПЕЦІАЛЬНОЇ ТЕХНІКИ ПІД ЧАС ПРОВЕДЕННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Згідно з главою 21 «Негласні слідчі (розшукові) дії» Кримінального процесуального кодексу України до негласних слідчих (розшукових) дій (далі – НСРД) належать, зокрема, НСРД, пов'язані із втручанням у приватне