Я добре знаюся на всіх видах тайнопису
і навіть сам написав невеличку розвідку,
де розглянув сто шістдесят різноманітних шифрів,
але мушу визнати, що цей випадок — для мене цілковита новина.
Шерлок Холмс, оповідання А. К. Дойля "Чоловічки в танці"»

ВСТУП

Сьогодні найціннішим активом будь-якої організації є інформація і в основі всіх бізнес-процесів лежать інформаційно-комунікаційні технології. У цих умовах грамотно вибудуваний захист даних компанії – одна з ключових умов забезпечення її конкурентоспроможності та розвитку. Недостатня захищеність інформації може привести до значних негативних наслідків для бізнесу, аж до повної його зупинки. Надійна і захищена робота мереж передачі даних, комп'ютерних систем і мобільних пристроїв є найважливішою умовою для функціонування держави і підтримки економічної стабільності суспільства.

Велика частина інформації, що зберігається строго конфіденційна і не призначена для публічного перегляду. При захисті конфіденційної інформації високому рівню безпеки персональних даних окремих людей і груп сприяє криптографія. Вона виступає ефективним методом, що дозволяє передавати інформацію в захищеній формі, забезпечуючи безпеку, конфіденційність і цілісність даних є криптографія. Вона використовується з метою забезпечення безпеки зберігання даних, захисту інформації при передачі через відкриті канали зв'язку і по локальній мережі. Всі представлені завдання вирішуються різними засобами із застосуванням різних криптографічних технологій.

З огляду на розвиток сучасних інформаційних технологій і рівень використання різних мов програмування, однією з найбільш ефективних для вирішення завдань кібрбезпеки і криптографії є програмна мова Python.

Навчальний посібник містить навчальний матеріал з дисциплін, що пов’язані з методикою вивчення та застосування методів кібербезпеки, в ньому наведені основні відомості про криптографію, методи криптографії, а також особливості мови програмування Python. У посібнику наведено якісний огляд інструментів для моніторингу мережевої безпеки. Що важливо, опис інструментів для моніторингу доповнюється практичними прикладами їх застосування.

Автори починають з опису ключових елементів мови прогармування Python, знання яких необхідно для подальшого застосування. Потім приділена увага більш складним темам, поданим так, щоб читач міг поступово нарощувати свій досвід: розподіл обчислювального навантаження між декількома процесами і потоками, використання складних типів даних, керуючих структур і функцій, створення додатків для роботи з базами даних SQL і з файлами DBM.

Для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня усіх форм навчання.

Навчальний посібник сприяє формуванню наступної компетентності – КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах, яка дозволяє отримати наступні результати навчання: РН-9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН-14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН-15. Використовувати сучасне програмно-апаратне забезпечення

інформаційно-комунікаційних технологій; РН-16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН-17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та РН-18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН-20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН-29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН-35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
РН-47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН-50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).