2. Sokolov, V. Wireless and Mobile Security : Laboratory Workshop / V. Sokolov, M. Taj Dini, V. Buryachok. — K. : SUT, 2017. — 124 p.

3. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Лабораторний практикум / В. Ю. Соколов, М. Тадж-Діні / ред. перекл. О. П. Райтер. — К. : ДУТ, 2018. — 122 с. [Ukrainian].

4. Kali Linux Tools Listing. https://tools.kali.org/tools-listing

Євгеній Яковенко
Ситуаційний центр протидії кібербатакам СБУ
Київ, Україна

КІБЕРНЕТИЧНІ АТАКИ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Основним завданням Ситуаційного центру протидії кіберзагрозам є створення умов для безпечного функціонування кіберпростору, його використання в інтересах суспільства і держави - забезпечення кіберзахисту державних електронних інформаційних ресурсів, боротьба з кібертероризмом та кібершпигунством, а також реагування на комп'ютерні інциденти у сфері державної безпеки.

Протягом 2017 року Ситуаційним центром протидії кіберзагрозам виявлено та попереджено проведення спеціальними службами Російської Федерації низки цілеспрямованих кібернетичних атак направлених на отримання доступу до інформації, що обробляється в інформаційних системах органів державної влади України, а також проведення акцій технологічного (кібернетичного) тероризму, спрямованих на порушення штатного режиму функціонування комп'ютерних мереж та систем керування технологічними процесами на об'єктах критичної інфраструктури нашої держави.

Співробітники Ситуаційного центру протидії кіберзагрозам приймали безпосередню участь у розслідуванні більшості кібератак щодо державних електронних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури України.

Ключовими функціями Центру є запровадження системи виявлення та реагування на кібератаки та лабораторії з комп'ютерної криміналістики. За підтримки міжнародної спільноти в Україні буде створено мережу ситуаційних центрів кібербезпеки. Принциповим аспектом роботи Центру СБУ є його відкритість для співпраці з міжнародними установами, організаціями, підприємствами та профільними фахівцями.

Бойові дії у кіберпросторі становлять важливий елемент гібридної війни проти України. Кількість кібератак з ознаками участі спецслужб Росії невпинно зростає протягом 2014-2018 років. При чому, їх проведення направлено на викрадення інформації в органах державної влади України, блокування роботи підприємств соціальної сфери, нанесення фінансової та матеріальної шкоди державним інституція, розміщення недостовірної інформації з метою дискредитації уряду.

Так, у 2014 році кібершпигунські напади здійснено на комп'ютерні мережі Центральної виборчої комісії, Міністерства закордонних справ, Посольств України у Литві, Естонії, Бельгії, Місії України при НАТО. У 2015 року зловмисниками викрадалась інформація з комп'ютерів співробітників правоохоронних органів, Збройних Сил та учасників АТО.

Проте, на рубежі 2015 і 2016 років деструктивним програмним забезпеченням виведено з ладу комп'ютерні мережі енергетичних підприємств Київської, Хмельницької, Івано-Франківської, Чернівецької областей, внаслідок чого без електропостачання залишилось декілька десятків тисяч споживачів цих регіонів України. У грудні 2016 року відбулось декілька послідовних потужних кібератак на важливі об'єкти економіки, енергетики і транспорту України.

Так, 6 грудня атаковано Державне казначейство та Міністерство фінансів, 14 грудня – публічне товариство "Укрзалізниця". 17 грудня внаслідок кібератаки виведено з ладу електропідстанцію "Північна" Національної енергетичної компанії "Укренерго". 20 грудня

атаковано Державне підприємство "Адміністрація морських портів України". Перед тим шкідливе програмне забезпечення виявлено в інформаційних системах Одеської філії Державного підприємства "Дельта Лоцман".

Також у 2016 році було виявлено спроби проникнення до комп'ютерних мереж українських банків із застосуванням спеціалізованих програм, які потенційно мають ознаки шкідливого програмного коду. Ретельне вивчення обставин та технологічних даних про зазначені атаки дозволило зробити припущення, що вони спрямовані на отримання несанкціонованого доступу до операторських місць системи SWIFT, які знаходяться у банківських установах України.

У червні 2017 року зафіксовано факти несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем органів державної влади та управління, компаній енергетичного комплексу, державних та приватних фінансових установ, операторів зв'язку та провайдерів телекомунікаційних послуг, що викликали значний резонанс у суспільстві. Вказана атака стала відома у світі під умовною назвою "Petya.A".

Розповсюдження ШПЗ здійснювалось через оновлення системи електронного документообігу (SupplyChainAttack – атака через довірене джерело).

Зловмисники викрали аутентифікаційні дані адміністратора та з використанням його прав змінили конфігураційний файл оновлень прикладного програмного забезпечення.

Основними цілями зловмисників були великі державні та приватні компанії, порушення штатного функціонування інформаційних інфраструктур яких може дестабілізувати ситуацію в країні.

У січні та квітні 2018 року російськими спеціальними службами організовано кібернетично-інформаційну операцію з несанкціонованого втручання в роботу офіційного сайту Державного підприємства "Антонов" та поширення недостовірної інформації з метою дискредитації державного підприємства на міжнародній арені.

Також у 2018 році виявлено та попереджено акцію кібернетичної розвідки ФСБ РФ, яка реалізована хакерським угрупуванням "TURLA" та спрямована на отримання несанкціонованого доступу до інформаційних систем Міністерства закордонних справ України.

Sergiy Kuchma
Компанія «Автор»
Київ, Україна

RADIO COMMUNICATION AND IP NETWORKS PROTECTION

Radio communication with improved anti-jamming ability and udition protection

This is intended to provide high stealth, noise immunity and protection against eavesdropping.

Features:

- Digital methods of voice and data transmission.
- Stealth and noise immunity improvement: FHSS, DSSS – wideband signals for direct spread spectrum.
- Crypto protection of guaranteed sustainability.
- SDR implementation of radio station.
- Mass and dimensional characteristics of radio station units do not exceed the analogues parameters of the P-863 radios
- Use of the existing cable and antenna-feeder system installed at the aircraft will ensure the replacement of radio stations without making changes to the construction of the aircraft.