поодиноке явище, то під час пандемії воно прийняло масовий характер. Чому вірогідно були раді зловмисники. Більшість підприємств були вимушені відкрити доступ до своїх локальних мереж ззовні для роботи користувачів з дому. Це потенційно збільшує вірогідність зламу мережі підприємства через домашній пристрій користувача внаслідок не дотримання ним цифрової гігієни.

Висновки. Усе вищенаведене говорить про те, що злочинці ніколи не зупиняють свою діяльність, навіть під час пандемії. Тому відповідальним за кібербезпеку ні в якому разі не можна втрачати пильності і треба працювати над покращенням безпеки при роботі з дому, а користувачам обов'язково необхідно дотримуватися правил кібергігієни

Список використаної літератури

1. COVID-19: вплив на електронну комерцію. Юридична газета online. [Електронний ресурс] – Режим доступу : https://yur-gazeta.com/publications/practice/medichne-pravo-farmacevtika/covid19-vpliv-naelektronnu-komerciyu.html
2. Прямухіна О.-М. Д., Січко Т.В. Розвиток інтелектуальних технологій в умовах пандемій. Комп'ютерні технології обробки даних: матеріали всеукр. наук.-практ. конф., м. Вінниця, 2021. С. 47-49.
3. Стандарти ISO/IEC захистять від кіберзагроз. ДП «Укрметртестстандарт». [Електронний ресурс] – Режим доступу : http://csm.kiev.ua/index.php?option=com_content&view=article&id=3631%3A-isoiec---&catid=122%3A2015-09-15-07-01-23&lang=uk
4. Хакерська атака на Україну: подробиці. РБК-УКРАЇНА. [Електронний ресурс] – Режим доступу : https://www.rbc.ua/ ukr/news/hakerskaya-ataka-ukrainu-podrobnosti-1498566985.html

УДК 004.8

Комар Ю.О., студент 4 курсу спеціальності 122 «Комп'ютерні науки»
Потапова Н. А., к.е.н, доцент, доцент кафедри інформаційних технологій

ТЕСТУВАННЯ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ

Донецький Національний університет імені Василя Стуса, м. Вінниця

Занурюючись у діяльність оцифровування українських правил та переведення систем забезпечення життєдіяльності, ми стикаємось з новими проблемами безпеки інформаційних технологій.

Слід зазначити, що на сьогодні інформаційні технології є невід'ємною частиною майже всіх сфер сучасного суспільства. За всіма оцінками експертів, до теперішнього часу склалася ситуація, коли можливості і стійкість

інформаційних систем, в значній мірі визначаються показниками якості, надійності і безпеки програмних засобів (в більшій мірі в порівнянні з апаратними засобами).

Програмне забезпечення стає одним з найбільш вразливих компонент сучасних інформаційних технологій, а використання програмних засобів у складі систем забезпечення діяльності об'єктів критичної інфраструктури, а також інших критичних систем породжує нову проблему – не можливості достатнього забезпечення інформаційної безпеки програмних засобів.

З огляду на це, справедливо визначити основні загрози сучасного світу щодо забезпечення інформаційної та кібербезпеки на об'єктах критичної інфраструктури:

1. Відсутність достатньої кількості фахівців з інформаційної безпеки та кібербезпеки на ОКІ;
2. Наявність вразливостей в програмному забезпеченні, що використовується на ОКІ;
3. Збільшення висококваліфікованих кібератак на ОКІ;
4. Застарілі підходи щодо забезпечення захисту інформації/інформаційної безпеки в державних установах та ОКІ;
5. Відсутність єдиних протоколів протидії кібератакам на ОКІ. В історії нашої держави визначено ряд гучних кібератак [6, 7] наведених у таблиці 1.

Пропонуємо розглянути поетапну реалізацію Кібератаки «BlackEnergy 3» на системи електропостачання «Прикарпаттяобленерго». На рисунку 1 відображено етапність реалізації кібератаки [5], а саме:

1) Було проведено фішшінг-атаку шляхом направлення електронного листа зі шкідливими кодом оператору «Прикарпаттяобленерго» для отримання доступу до мережі Обленерго. Шкідливий код був внесений у вигляді макросу до файлу Microsoft Office;

2) Ідентифікація та встановлення у фоновому режимі шкідливого програмного забезпечення «BlackEnergy 3» на робочій станції оператора;

3) Викрадення критичних даних для адміністрування з мережі «Прикарпаттяобленерго»;

4) Використання віртуальних приватних мереж (VPN) для входу до ICS мереж «Прикарпаттяобленерго»;

5) Використання існуючих інструментів для віддаленого доступу та управління в мережі «Прикарпаттяобленерго»;

6) Використання модифікованого KillDisk для видалення основних записів завантаження уражених елементів системи, а також цільове видалення деяких журналів подій;

7) Управління системи енергопостачання для впливу на підключене навантаження із запланованим відключенням обслуговування;

8) Телефона атака на відмову в обслуговуванні call-центру.

Таблиця 1

Перелік реалізованих кібератак на ОКІ у період з 2015-2017 років

№	Найменування атаки	Вражені ОКІ	Дата реалізації
1	Кібератака	«Прикарпаттяобленерго»	23 грудня 2015

	«BlackEnergy 3»		року
		«Київобленерго»	23 грудня 2015 року
		«Чернівціобленерго»	23 грудня 2015 року
2	Кібератака з використання вірусу Petya	Аеропорт «Бориспіль», «Харків», «Київ» 27 червня 2017 року Укренерго	27 червня 2017 року
		Чорнобильська АЕС	27 червня 2017 року
		Київський метрополітен	27 червня 2017 року
		ЗМІ	27 червня 2017 року
		Укрзалізниця	27 червня 2017 року
		Київводоконал	27 червня 2017 року
		ДП «Антонов»	27 червня 2017 року

Джерело: [1, 2, 3]

Результатами цієї атаки було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин.

Протидія або профілактика запобіганню таким або подібним кібератакам, які були наведені в таблиці 1, є проведення на ОКІ аудитів інформаційної безпеки з тестуванням на проникнення.

Тестування на проникнення [1, 2] (Pentest) – це процедура (спроба) оцінки реальної захищеності інформаційної системи з використанням контрольованих і максимально безпечних для інфраструктури та бізнес-процесів атак, а також виявлення та спроби експлуатації вразливостей.

Проведення пентесту дозволяє надати детальну інформацію про існуючі прогалини в безпеці інформаційних систем та запланувати найбільш важливі напрямки щодо поліпшення стану їх захищеності.

Головна мета пентесту – знайти в інфраструктурі і додатках клієнта уразливості, які потенційно можуть бути використані зловмисниками. Крім того, тестування на проникнення допомагає зрозуміти, наскільки ефективні розроблені політики в області IT-безпеки і чи варто їх удосконалювати. Іноді пентести проводяться, щоб перевірити готовність фахівців інформаційної безпеки до відбиття кібератак на інформаційні системи організації.

Рис. 1. Етапи реалізації кібератаки «BlackEnergy 3» в «Прикарпаттяобленерго»

Опираючись на міжнародні практики можемо розглянути етапи [3, 4] проведення тестування на проникнення:

1. Розвідка, збір інформації щодо об’єкта тестування;
2. Вибір методів та інструментів для здійснення атаки;
3. Доставка до систем об’єкта тестування вибраного інструмента атаки;
4. Експлуатація вразливостей виявлених в системі об’єкта тестування;
5. Встановлення шкідливого програмного забезпечення;
6. Отримання доступу та контролю над системою об’єкта тестування;
7. Здійснення узгоджених дій для підтвердження успішного тестування на проникнення.

Використовуючи зазначену методику тестування на проникнення фахівці максимально наближено відображають ситуації кібератаки на системи ОКІ. При цьому, працівники відповідальні за захист інформації можуть навіть і знати про тестування та відпрацьовувати заходи щодо запобігання кібератакам.

Виходячи з цього, з метою підвищення рівня кібербезпеки на державному рівні слід визначити такі основні питання:

- необхідності проведення аудитів інформаційної безпеки на ОКІ з обов’язковим проведенням тестування на проникнення;
- необхідності розробки та затвердження відповідних методик з проведення тестування на проникнення;
- розширення державно-приватного партнерства в рамках впровадження системи незалежного аудиту інформаційної безпеки та проведення тестувань на проникнення;
- можливості проведення загальнодержавних навчань з запобігання кіберзагрозам на ОКІ та державних органів в рамках державно-приватного партнерства;
- використання в системах ОКІ програмних та технічних засобів, що

пройшли державну експертизу у сфері захисту інформації;

- проведення навчань співробітників ОКІ з питань інформаційної та кібербезпеки.

Список літературних джерел.

1. The Open Source Security Testing Methodology Manual. URL: https://www.isecom.org/OSSTMM.3.pdf.
2. Penetration testing execution standard. URL: http://www.pentest-standard.org .
3. Technical Guide to Information Security Testing and Assessment. URL:: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800- 115.pdf .
4. OWASP Testing Guide v4. URL: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_ Testing _Guide_v4.pdf .
5. Кібератака на енергетичні компанії України. URL: https://cutt.ly/GhmtxVf .
6. TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf .
7. Хакерські атаки в Україні (2017). URL: https://cutt.ly/ohmtvta.

УДК 004.056

Курдупов О. Л., студент 3 курсу спеціальності 122 «Комп'ютерні науки»
Потапова Н. А., доцент, доцент кафедри інформаційних технологій

ВИКОРИСТАННЯ МЕТОДУ МОНТЕ-КАРЛО ДЛЯ АНАЛІЗУ ПРОЕКТНИХ РИЗИКІВ

Донецький національний університет імені В. Стуса, м. Вінниця

Вперше опис методу Монте-Карло з'явився в 1949 р. у статті американських математиків Дж. Неймана та С. Улама "The Monte Carlo Method". Назва методу походить від міста Монте-Карло, відомого своїми казино, адже саме рулетка є найпростішим "генератором випадкових чисел", на роботі якого засновано сам метод. Область застосування методу Монте-Карло досить широка: від розрахунку систем масового обслуговування до обчислення інтегралів від складних функцій.

Схема використання методу Монте-Карло для кількісного аналізу проектних ризиків включає певну кількість етапів, реалізація яких дозволяє використати комп'ютерний експеримент в оцінці непередбачуваних результатів. На першому етапі будується модель залежності, що характеризує проект результуючого показника від різних змінних та параметрів проекту. Ті фактори, значення яких можуть змінюватися, є змінними та моделюються випадковими величинами. А ті фактори, значення яких є постійними впродовж життєвого циклу проекту, є параметрами та моделюються константами. Як висновок,