Швейцарія, Німеччина, Норвегія, Данія, Ісландія, Японія, Люксембург та Сінгапур. Комфортна та безпечна атмосфера існує у Новій Зеландії, Сінгапурі та и Японії. В цих державах влада кілька десятиліть тому провела радикальні реформи в правозахисних сферах, реформувала суди, запровадила великі штрафи за порушення громадського порядку та законів.

Тому на державного і регіональному рівнях виникає необхідність постійного моніторингу рівня злочинності в країні, вживати заходи боротьби із злочинністю, забезпечувати високий рівня безпеки в Україні шляхом вдосконалення досвіду високорозвинених країн світу [2], використання їх досягнень, удосконалення прогалин у вітчизняній законодавчій та правовій базі, а також підвищувати рівень кваліфікації працівників та підрозділів правоохоронних органів для ефективної протидії економічній злочинності.

Використані джерела:

1. Рівень злочинності у світі. [Електронний ресурс]. – Режим доступу: - https://visasam.ru/emigration/vybor/prestupnost-v-mire.html

2. Rubalchenko L., Ryzhkov E. Ensuring enterprise economic security. SCIENTIFIC BULLETIN OF THE DNIPROPETROVSK STATE UNIVERSITY OF INTERNAL AFFAIRS. 2019. SPECIAL ISSUE №1.- P.268-271

Синиціна Ю.П. доцент кафедри економічної та інформаційної безпеки, к.т.н., доцент (Дніпропетровський державний університет внутрішніх справ, м. Дніпро)

СУЧАСНІ ПІДХОДИ ДО БЕЗПЕКИ ОПЕРАЦІЙНИХ СИСТЕМ

В області безпеки операційних систем в останні роки відбуваються помітні зміни. Все почалося з того, що в спільнотах розробників і в компаніях, що створюють операційні системи, поступово зміцнилося розуміння неможливості виправити все до однієї помилки в програмному коді. Розроблення питань захисту інформації, зокрема реалізації механізмів захисту сучасних операційних систем, займаються зарубіжні науковці В.Г. Проскурин, С.В. Крутов, І.В. Мацкевич [2], П.Б. Хорев [3], О.В. Казарін [4], проте стрімкий розвиток інформаційних технологій у сфері створення нових операційних систем безупинно дає матеріал для наукових досліджень. З урахуванням зазначеного більшість сучасних універсальних ОС не виконують у повному обсязі вимоги до захисту автоматизованих систем для оброблення конфіденційної інформації. Тому, вони не можуть без використання додаткових засобів захисту застосовуватися для захисту навіть конфіденційної

інформації. Утім, основні проблеми захисту тут викликані не тим, що не виконані окремі вимоги до механізмів захисту в ОС, а недосконалістю реалізованої в ОС концепції захисту, розроблення якої потребує подальшого наукового дослідження.

Операційна система є спеціально організованою сукупністю програм, яка управляє ресурсами системи (електронно-обчислювальної машини (ЕОМ), обчислювальної системи, інших компонентів інформаційно-обчислювальної мережі) з метою найбільш ефективного їх використання і забезпечує інтерфейс користувача з ресурсами.

Нажаль, проблеми з безпекою є майже у всіх операційних системах. Зробити щось ідеально — просто неможливо. Проте, іноді кількість «дірок» у безпеці виходить за всі допустимі рамки. Такі проблеми можуть як існувати з моменту створення ОС, так і з'являтися після деяких оновлень. За результатами аналізу, проведеної командою The Best VPN [4], сформовано своєрідний ТОП ОС, які мали найбільшу кількість таких «дірок» (рис. 1).

№№	Назва ОС	К-сть «дірок»
1	Android	414
2	Debian Linux	360
3	Windows Server 2016	357
4	Windows 10	357
5	Windows Server 2019	351
6	Adobe Acrobat Reader DC	342
7	Adobe Acrobat DC	342
8	cPanel	321
9	Windows 7	250
10	Windows Server 2008	248
11	Windows Server 2012	246
12	Windows 8.1	242
13	Windows RT 8.1	235
14	Ubuntu	190
15	Fedora	184

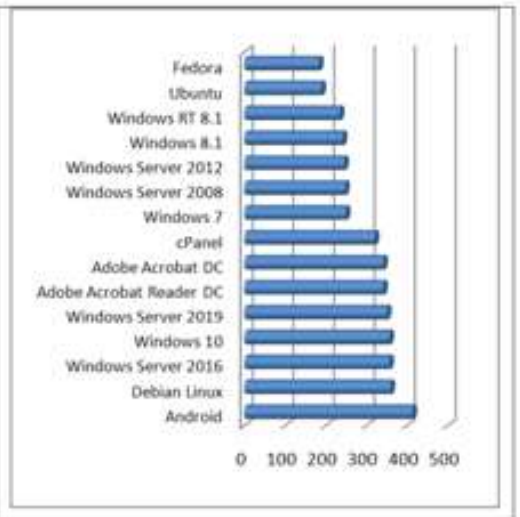

Рис. 1. Рейтинг ОС за кількістю виявлених «фейлів» за 2019 р.

У 2019-му безсумнівним лідером за кількістю фейлів стала Android. На другому місці розташувалася Debian Linux, а за нею — серверна Windows Server 2016 та Windows 10. Незважаючи на всі зусилля, у коді операційних систем, який стає все складніше, нові помилки додаються швидше, ніж виправляються старі. Частина з цих помилок призводить до вразливості інформаційної безпеки, що є серйозною проблемою. Щоб її вирішити, в галузі з'явилося два взаємодоповнюючих підходи, які почали покращувати ситуацію з безпекою операційних систем.

Перший підхід: ядро операційної системи має володіти засобами самозахисту. Іншими словами, в разі помилки або атаки система повинна безпечно обробити цю ситуацію. Існує популярна аналогія, де розробка операційних систем наших днів порівнюється з автомобільною індустрією 60-х років XX століття: тоді через величезну травматизму в ДТП автовиробники почали розробляти засоби безпеки для пасажирів, щоб автомобіль був не тільки надійний в звичайній ситуації, а й безпечний в разі аварії. Аналогічні технології розробляються в наші дні для

операційних систем. Зокрема, в цьому році фахівці Microsoft Security Response Center представили детальний огляд типів вразливостей і способів боротьби з ними в ядрі Windows. Також розроблена карта засобів захисту ядра Linux, яка відображає взаємозв'язки між типами вразливостей, методами їх експлуатації та наявними механізмами захисту.

Однак на практиці впровадження засобів самозахисту ядра операційної системи не буває безкоштовним. За підвищення безпеки зазвичай доводиться платити падінням продуктивності і додатковими складнощами для розробників системи. Наочним прикладом цього служать спроби усунення апаратних вразливостей Spectre, Meltdown, MDS на рівні операційних систем.

Другий підхід до вирішення проблеми помилок в операційних системах - це безперервне використання автоматичних засобів динамічного і статичного аналізу. Наші операційні системи написані на низькорівневих мовах програмування за цілою низкою причин. Такі мови дають розробнику більшу потужність і при цьому вимагають від нього великої уважності та професіоналізму. А людям властиво помилятися, тому на допомогу приходять автоматизовані засоби перевірки. Це і різноманітні методи статичного аналізу, включаючи пошук помилок по паттернам, і технології динамічного аналізу, однією з найпопулярніших серед яких став фаззинга (методика тестування ПО випадковими даними). Прикладом проекту, що вносить значний вклад в безпеку багатьох операційних систем, є фаззер syzkaller.

При цьому у розвитку автоматизованих засобів пошуку вразливостей є важливий побічний ефект: вони доступні не тільки захисникам, а й атакуючим.

Слід зазначити, що не існує одного стандарту захисту, а захист не є бінарним вибором. Те, наскільки захищена оперативна система, потрібно розглядати в контексті потреби організації. Саме тому найбільш результативним сьогодні вважається комплексний підхід. Виділивши окремо найбільш важливі елементи ОС можна добитися повноцінного захисту системи із повноцінним захистом, найбільш наближеним до ідеального.

Використані джерела:

1. Проскурин В.Г. Защита в операционных системах / В.Г. Проскурин, С.В. Крутов, И.В.Мацкевич. – М. : Радио и связь, 2000. – 168 с.

2. Хореев П.Б. Методы и средства защиты информации в компьютерных системах / П.Б. Хорев. – М. : Академия, 2005. – 256 с.

3. Казарин О.В. Безопасность программного обеспечения компьютерных систем / О.В. Казарин. – М. : МГУЛ, 2003. – 212 с.

4. ТОП ОС за визначенням команди The Best VPN. Електронний ресурс. URL: https://9to5google.com/2020/03/06/android-vulnerabilities-report-2019/