КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2(22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.22.6883
УДК 004.415.538

Кіпчук Феодосій Валентинович
аспірант кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0003-4816-9246
f.kipchuk.asp@kubg.edu.ua

Соколов Володимир Юрійович
кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

МОДЕЛЬ РОЗРАХУНКУ ВИТРАТ НА БАГ-БАУНТІ ПРОГРАМИ ТЕСТУВАННЯ ВРАЗЛИВОСТЕЙ БЕЗПЕКИ

Анотація. У статті описані способи дослідження баг-баунті програм та запропоновано новий підхід для розрахунку оцінки знайдених вразливостей. Робота починається з вводу у розуміння процесів управлінням вразливостями, поняття поверхні вразливості атаки. У роботі наведено аналіз статистики всіх знайдених вразливостей в інформаційних системах за останні десять років, які розділені за стандартною оцінкою CVSS. Проаналізовано види і вектори атак на прикладі фінансового сектору. Додатково проведено розподілення зламів і інцидентів по векторам атак на фінансовий сектор. Далі наведено співвідношення найпопулярніших видів і векторів атак до критичності інформаційних систем. Представлено рейтинг критичних і високих вразливостей однієї з платформ баг-баунті з детальним описом видів атак і технік експлуатації. Невід'ємною частиною процесу управління вразливостями є категоризація важливості і впливу на організацію. Також представлено можливі сценарії життєвого циклу для знайденої вразливості в інформаційній системі очима власника інформації про вразливість та власника такої інформаційної системи. Проведено порівняльний кількісний і якісний аналізи зрілості програм баг-баунті від моменту запуску і протягом років, а також чинники впливу на зрілість програми. Проаналізовано статистику знайдених вразливостей в публічних баг-баунті програмах за останні шість років. Запропоновано власний підхід до розрахунку ефективної вартості програми баг-баунті та проведено експериментальну перевірку на трьох програмах. Висвітлено фактори впливу на розрахунок ефективної вартості вразливостей. Розглянуто підходи до оцінок і валідації вразливостей платформами баг-баунті та етапи арбітражу між власником інформаційної системи та дослідником вразливостей. Наприкінці дослідження наведено рекомендації для набуття вищого рівню зрілості процесів управління вразливостями. Виковки висвітлюють безперервність виникнення і зникнення додаткових факторів у процесах управління вразливостями, в яких програми баг-баунті є невід'ємною частиною. Взаємозалежність зрілості процесів компанії та її програми баг-баунті, що потребує залучення достатніх ресурсів, задля ефективності її роботи.

Ключові слова: вразливість; атака; баг-баунті; етичний хакінг; пентестинг; винагорода; Common Vulnerability Scoring System; CVSS.

ВСТУП

Робота презентує новий метод оцінки вартості вразливостей, що надходять у формі звітів по програмі баг-баунті. Ця робота покликана висвітлити додаткові фактори, які не завжди беруться до уваги під час планування правил запуску програм баг-баунті, що неопосередковано впливає на адекватність виплат і як результат налагодження позитивною репутації для заохочення дослідників з вразливостей.

Головна мета дослідження — аналіз існуючих методів заохочення зовнішніх ресурсів для тестування складних інформаційних систем (аналог бета-тестуванню функціональності) для підвищення ефективності моделей баг-баунті. Та розробка моделі адекватного розрахунку вартості, яка призведе до адекватного планування ресурсів власниками інформаційних систем, дозволить розрахуватись з дослідниками вразливостей, уникаючи продажу таких вразливостей особам з непристойними намірами.

Постановка проблеми. Наразі одним з популярних трендів є Видимість Поверхні Атаки «attack surface visibility» (ВПА). ВПА відноситься до можливостей ідентифікувати та прив'язати усі потенційні точки входу та вразливості у цифрових активах компаній. ВПА є важливою складовою з точки огляду процесу управління вразливостям для будь-яких організацій. Відсутність або недостатня ВПА може призвести до неефективності процесу управління вразливостями, витрачаючи багато ресурсів на ручні процеси, неправильний розподіл ресурсів інформаційної безпеки та тестування. Управління Видимістю Поверхні Атаки «attack surface management» (УВПА) є сукупністю постійної розвідки, аналізу, ремедіації, моніторингу вразливостей та потенційних векторів атак інформаційної безпеки організації. Недостатнє УВПА створює наступні виклики для інформаційної безпеки: неповне врахування ризиків інформаційної безпеки та неефективність центру операційної безпеки [1]. 70% організацій були зламані за останній рік через невідомі, неконтрольовані або погано контрольовані публічно доступні інтернет-ресурси [2].

Всесвітньо відома платформа баг-баунті HackerOne пропонує власне бачення і підхід до ВПА та УВПА. УВПА забезпечує інвентаризацію активів, що динамічно оновлюється завдяки декільком ресурсам: постійне сканування ВПА сервісами HackerOne, імпортованими результатами інших сканерів або іншого програмного забезпечення з відкритим початковим кодом та існуючим списком активів компанії. Одним з успішних прикладів реалізації УВПА від HackerOne є один з банків США, що у процесі багаторічної хмарної міграції, протягом кількох тижнів після впровадження HackerOne Assets ВПА зросла з приблизно 150 цифрових активів до понад 800, що означає збільшення видимості у 5,3 рази. У поєднанні з додатковою інформацією про ризики, наданою експертами з безпеки персоналу, це одразу дало банку більш точне розуміння профілю ризиків і допомогло групі безпеки визначити пріоритетність активів із найвищим ризиком для негайних дій [1].

Один з яскравих прикладів є запуск компанією Мета розширеної програми баг-баунті. Враховуючи різкий стрибок інтересу і розвитку технологій доповненої реальності та метавсесвіту Meta розширила програму, на $300 тис. у цьому напрямку. Враховуючи новизну фізичних пристроїв для цього специфічного сектора, та запуск першої програми баг-баунті для пристроїв віртуальної реальності, як доповнення було впроваджено щорічну конференцію BountyCon [3]. Також загальний фонд виплат Meta по програмам баг-баунті у 2022 році склав $2 млн [4]. Відповідно до звіту Bugcrowd 2022 [5], завдяки дослідникам вразливостей та білим хакерам на платформі Bugcrowd було попереджено кіберзлочинів на суму $27 млрд, але 91% хакерів погодились, що тестування безпеки за певну одиницю часу не захищає компанію цілий рік.

Аналіз останніх досліджень і публікацій. Попередня робота [6] полягала у вивченні підходів оцінки аудиту інфраструктури провідними міжнародними стандартами, що є невід'ємною частиною для визначення вимог щодо процесів формування інформаційної та кібернетичної безпеки. У [7]–[10] було проведено дослідження, які відображали стан розвитку і тенденцій програм баг-баунті за попереднє десятиліття. До предмету досліджень увійшли вразливості та загрози для класичних систем та інтернету речей, включаючи вразливості нульового дня. Принципи ринкового

та не ринкового розкриття вразливостей. Дослідження [7] було проведено з різних точок огляду та включало у себе: розрахунок операційної вартості програми баг-баунті на день, середня оцінка вартості відповідно до складності вразливостей, кумулятивний аналіз трендів у порівнянні вартості вразливостей та кількості звітів у розрізі днів запуску та існування програм. Також [10] покривала специфічну тематику відповідального розкриття вразливостей, аукціони вразливостей та чорні продавці. Проте дані, наведені в [7]–[10] потребують актуалізації через стрімкий розвиток інформаційної безпеки та кількість інструментів для захисту інформаційних, людських і кібернетичних ресурсів. Також зростаючою популярності набули вразливості нульового дня, які стали широко розповсюджені за останні два роки. Робота [11] вивчає новий підхід до розуміння вразливостей нульового дня, виступаючи посередником у відносинах між власником інформаційної системи та власником раніше невідомих вразливостей у цій системі для максимізації вигоди. Запропонований підхід є ризикованим і потребує задоволення таких критеріїв: специфічного правового регулювання, ідентифікації всіх сторін учасників, позитивної репутації арбітражу, при якій власник і хакер довірятимуть арбітру.

В [12] описують вивчення зрілості програм баг-баунті, яка неопосередковано впливає на її ефективність. Так, на початку відкриття програми з великою вірогідністю її ефективність буде доволі низька, що характеризується низькою швидкістю обробки звітів, необхідним часом на валідацію вразливості, її виправлення та присудження винагороди. Однак з часом існування програми налагоджується взаємодія різних відділів компанії, що покращує загальну продуктивність, відповідно з накопиченням досвіду та оптимізацією взаємодії. В основі [12] закладено розрахунок сталих (об’єктивних) та залежних (суб’єктивних) факторів. Результати представлено у вигляді лінійної регресії з фіксованими ефектами вимірювання взаємозв’язку досвіду і продуктивністю усунення вразливостей та того самого взаємозв’язку через пом’якшуючий ефект звітів.

МЕТОДИКА ДОСЛІДЖЕННЯ

В роботі використано наступні методи: огляду процесу винагороди за знаходження помилок та слабких місць як невід’ємна частина процесу управління вразливостями; розрахунку впливу факторів на етапи процесу винагороди за знайдені помилки та уразливості; порівняння різних типів вразливостей для широко використовуваних типів програм баг-баунті; категоризації та пріоритезації знайдених та відзвітованих вразливостей та їх вплив на продуктові системи. Об’єкт дослідження — програми баг-баунті для програмних продуктів та інформаціних систем. Предмет дослідження — способи побудови ефективної програми баг-баунті.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналіз статистики існуючих баг-баунті програм

Враховуючи той факт, що кількість різновидів інформаційних систем кратно зросла, все ж основні загальновживані розробки припадають на Microsoft, Apple, Meta, Google тощо. Найбільш вживані системи цікавлять білих і чорних хакерів, дослідників вразливостей. Для об’єктивного розуміння важливості захисту інформаційних і кібернетичних систем необхідно було взяти базовий показник як вказівник потенційної загрози. Таким показником було обрано та представлено на рис. 1 усереднену статистику усіх виявлених типів вразливостей відповідно до оцінки Common Vulnerability Scoring System (CVSS) за останні десять років [13].

ISSN 2663 - 4023

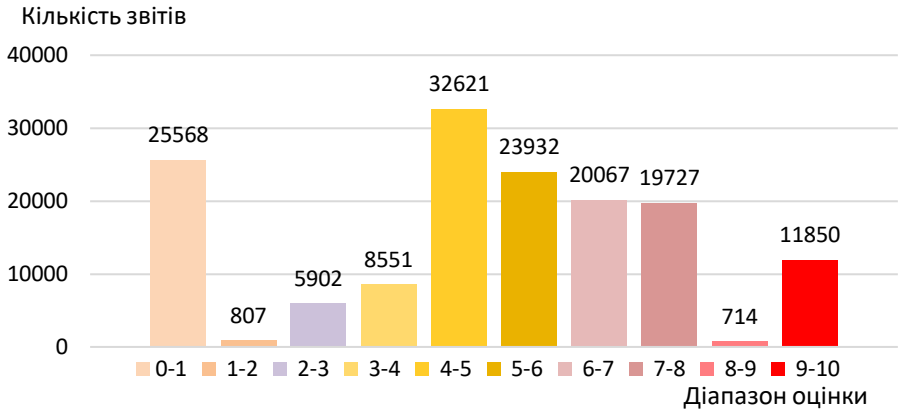

Рис. 1. Розподілення вразливостей за оцінкою CVSS за 2013–2023

Основоположні принципи визначення вразливостей і видів загроз описані Міжнародною спілкою електрозв'язку. Нижче наведено типи загроз:

– вразливості закладені в *дизайні* та *специфікації систем*, які в результаті експлуатації призводять до помилок і вразливостей;
– вразливості *впровадження*, які виникають через помилки або недогляди під час роботи системи або виконання протоколу;
– вразливості *конфігурації* та *налаштувань* [14].

Було проаналізовано програми баг-баунті за останні шість років, які були зареєстровані на платформі баг-баунті HackerOne [15] і мали 470 і більше закритих звітів. Враховуючи те, що першу програму на платформі було зареєстровано у листопаді 2013, то ця дата була застосована як початкова для всіх компаній, що приєднались до платформи. Було виключено програми, в яких не вказано середній розмір винагород, дата приєднання або кількість закритих звітів. Усього було проаналізовано 15 компаній, які взяли участь у програмі баг-баунті. Результати кількісного аналізу приведено на рис. 2.

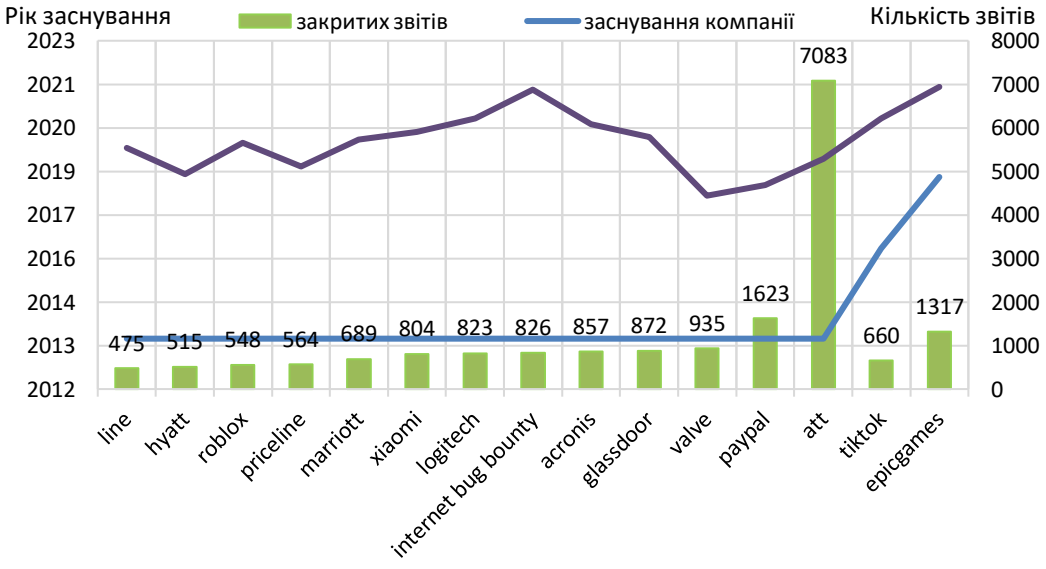

Рис. 2. Співставлення заснування програми баг-баунті та запуск компанії

Також було проведено аналіз 133 програм, але з меншим порогом за кількістю звітів — від дев'яти та більше. Це дає можливість показати, за який період програми баг-баунті набувають найкращої продуктивності за кількістю звітів закритих протягом року. З табл. 1 видно, що закритих звітів найбільше для компаній, які запустили програму баг-баунті більше п'яти років тому.

Таблиця 1

Співвідношення зрілості програми баг-баунті відповідно до дати початку програми і середньої кількості закритих звітів

Дата запуску програми	Кількість компаній	Середня кількість закритих звітів	Середня кількість закритих звітів на одну компанію
січ.–черв. 2023	19	72	3,8
2022	28	112	4,0
2021	23	197	8,6
2020	34	267	7,9
2019	18	558	31,0
2018	11	372	33,9

Відповідно до Vulnerability Rating Taxonomy версії 1.10 [16], було визначено наступні найбільш критичні вразливості, які були виявлені та провалідовані компаніями-учасницями баг-баунті програм на платформі BugCrowd (див. табл. 2).

Таблиця 2

Таксономія рейтингу вразливостей першого та другого пріоритетів

Пріоритет	Категорія	Вразливість	Опис	Вид атаки
1	Неправильна конфігурація безпеки сервера	Використання даних авторизації за замовчуванням	—	Троянська атака, соціальний інжиніринг
1	Ін'єкція на стороні сервера	Включення файлу	Локальна	Троянська атака, соціальний інжиніринг
1	Ін'єкція на стороні сервера	Дистанційне виконання коду	—	Ін'єкції, троянська атака
1	Ін'єкція на стороні сервера	SQL-ін'єкція	—	Ін'єкції, базові атаки застосунків
1	Ін'єкція на стороні сервера	Зовнішня ін'єкція XML	—	Ін'єкції, базові атаки застосунків
1	Порушення автентифікації та керування сеансами	Обхід автентифікації	—	Ін'єкції, базові атаки застосунків, атаки на дані авторизації
1	Витік чутливих даних	Розкриття паролів	Для публічно доступних систем	Ін'єкції, базові атаки застосунків, соціальний інжиніринг, людина в середині, атаки на дані авторизації
1	Незахищена операційна система або прошивка	Ін'єкція команд	—	Ін'єкції
1	Незахищена операційна система або прошивка	Статично закодовані паролі	Для привілейованих користувачів	Атаки на дані авторизації, базові атаки застосунків
1	Злам криптографії	Криптографічний недолік	Неправильне використання	Базові атаки застосунків

1	Неправильне налаштування безпеки автомобіля	Інформаційно-розважальна система, головний пристрій радіо	Витік персональних ідентифікаційних даних	Базові атаки застосунків
1	Неправильне налаштування безпеки автомобіля	Радіочастотний концентратор	Клонування брелка	Мережеві атаки і розвідка
2	Неправильна конфігурація безпеки сервера	Неправильно налаштований DNS	Викрадення піддомену	Мережеві атаки і розвідка
2	Неправильна конфігурація безпеки сервера	Неправильно налаштований OAuth	Викрадення акаунту	Атаки на дані авторизації, людина в середині
2	Витік чутливих даних	Слабка реалізація скидання пароля	Витік токену через отруєння заголовка хосту	Атаки на дані авторизації, людина в середині
2	Міжсайтовий сценарій (англ. XSS)	Збережений	Непривілейований користувач для всіх	Атаки на дані авторизації, базові атаки застосунків
2	Порушення контролю доступу	Підробка запитів на стороні сервера (англ. SSRF)	Внутрішній високий вплив	Атаки на дані авторизації, базові атаки застосунків
2	Підробка міжсайтового запиту (англ. CSRF)	Для всього додатку	—	Атаки на дані авторизації, базові атаки застосунків
2	Відмова в обслуговуванні на рівні програми (англ. DoS)	Критичний вплив і/або легка складність	—	Відмова в обслуговувані
2	Незахищена операційна система або прошивка	Статично закодовані паролі	Для непривілейованих користувачів	Базові атаки застосунків
2	Неправильне налаштування безпеки автомобіля	Інформаційно-розважальна система, головний пристрій радіо	Маніпуляція прошивкою (англ. OTA)	Базові атаки застосунків, мережеві атаки і розвідка
2	Неправильне налаштування безпеки автомобіля	Інформаційно-розважальна система, головний пристрій радіо	Виконання коду (англ. CAN)	Базові атаки застосунків, ін’єкції
2	Неправильне налаштування безпеки автомобіля	Радіочастотний концентратор	CAN ін’єкція/взаємодія	Мережеві атаки і розвідка, ін’єкції

Інцидент — подія безпеки, яка порушує цілісність, конфіденційність або доступність інформаційних активів. Злам — інцидент як результат підтвердженого розкриття даних неавторизованій стороні. Наприклад, розподілена атака відмови на обслуговування (DDoS), найчастіше є інцидентом, а не зламом, оскільки дані не викрадаються. Проте, це не робить цей вид атаки менш серйозним [17]. На рис. 3 представлено розбивку різноманітних активів, які постраждали від зломів. У фокусі є вторгнення в систему, базові атаки веб-додатків і соціальний інжиніринг.

ISSN 2663 - 4023

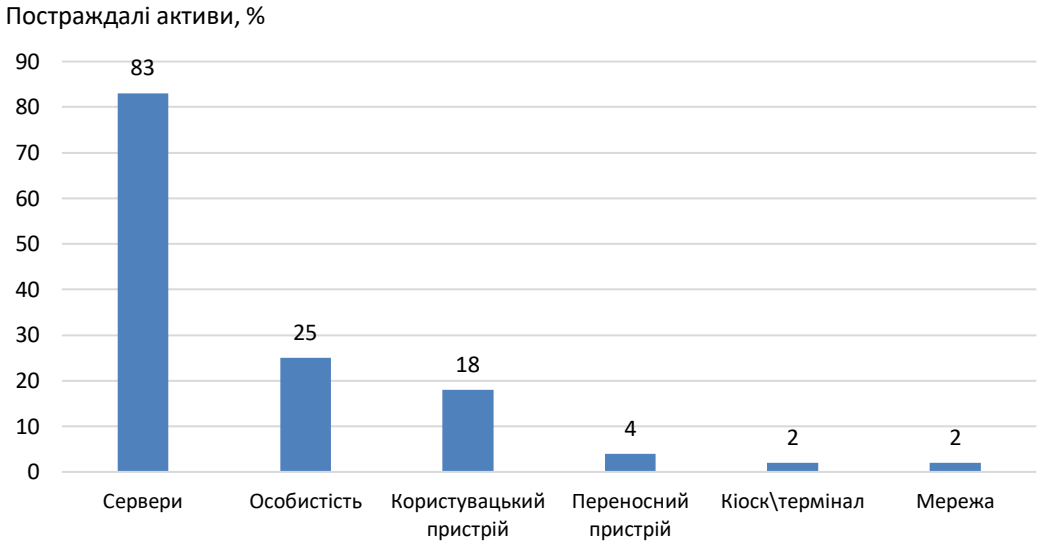

Рис. 3. Слабкі місця інформаційної інфраструктури

На рис. 4 і 5 показано найпопулярніші різновиди атак і вектори атак зломів, пов'язаних із віртуальною валютою, і це жорстка конкуренція між експлуатацією вразливостей, використанням викрадених даних авторизації та фішингом. Внутрішні дані та системні дані зазвичай є побічними продуктами значного порушення з кількома етапами, такими як: викрадення зловмисниками конфіденційної інформації з електронними листами та документами. Облікові дані набули популярності за останні п'ять років, оскільки використання викрадених облікових даних стало найпопулярнішою точкою входу для зломів [17].

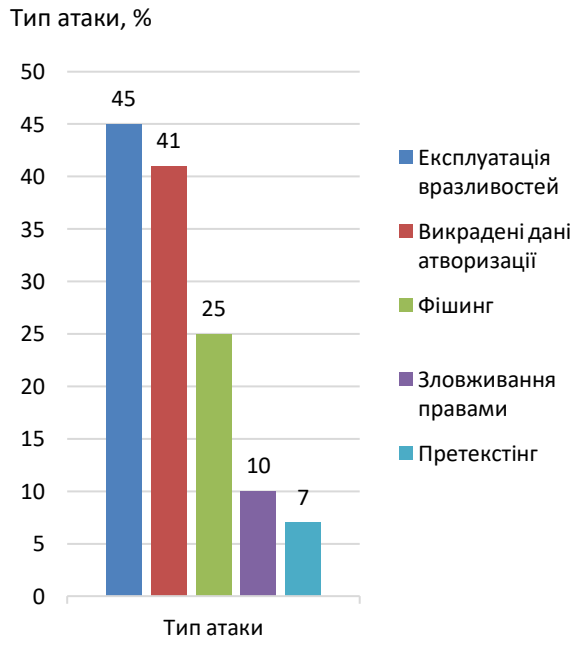

Рис. 4. Типи атак при зламах

Рис. 5. Вектори атак при зламах

Вивчаючи вектори атак на фінансовий сектор у відсотковому співвідношенні для зламів і інцидентів у табл. 3 визначено три основні категорії. Різні помилки як от

неправильна доставка (misdelivery), втручання у системи та базові веб-атаки застосунків є найпопулярнішою комбінацією векторів атак. У випадку успішності застосування одного з цих векторів атак, інші два стають легшими до експлуатації та подальшій атаці.

Таблиця 3

Розподілення зламів і інцидентів по векторам атак на фінансовий сектор

Вектори атак	Зламів, %	Інцидентів, %
Все інше	—	0,4
Відмова в обслуговувані	0,1	67,5
Викрадені дані авторизації	1,1	0,3
Зловживання правами доступу	3,7	2,0
Соціальний інжиніринг	16,1	5,1
Різні помилки	22,9	7,6
Втручання у системи	25,9	7,8
Базові атаки веб застосунків	30,3	9,3

Категоризація важливості та впливу на організацію

Вразливості можна розподілити за рівнем ризику:

- *низький*: не впливає на критичні функції системи. Це може бути помилка інтерфейсу, неправильна конфігурація. Не впливає на цілісність, конфіденційність або доступність;
- *середній*: така вразливість може вплинути на некритичну роботу деяких систем, призвести до витоку технічних даних або вплинути на користувачів. Але ця вразливість може бути використана одночасно з іншими середніми вразливими місцями, яку загалом можна оцінити як високу;
- *високий*: вразливість прямо чи опосередковано впливає на цілісність, конфіденційність або доступність системи. Функції реєстрації, авторизації та захисту даних можуть бути використані для часткового вилучення конфіденційних даних або захоплення контролю над модулями системи;
- *критичний*: прямий вплив на всю систему, що призводить до повної маніпуляції даними, захоплення контролю над системою, відключення або блокування будь-яких функцій аж до знищення даних або фізичного обладнання.

Враховуючи велику кількість різновидів і векторів атак, необхідно зауважити, що їх ризик відрізняється від сектору економіки, в якій існують інформаційні системи. В цій роботі було взято за приклад фінансовий сектор. У табл. 4 наведено різні види атак та ризик їх застосування, які притаманні фінансовому сектору. Базові атаки на застосунки включають атаки на звичайні та веб-застосунки.

Таблиця 4

Фактори втрат на базі бізнес ризиків і ранжування типів атак

Види атак	Рівень ризику, %			
	Критичний	Високий	Середній	Низький
Відмова в обслуговувані	70	20	10	0
Вірусна атака	15	70	15	0
Атаки на дані авторизації	15	70	15	0
Мережеві атаки і розвідка	15	70	15	0
Людина в середині	0	15	70	15
Соціальний інжиніринг	0	15	70	15
Базові атаки застосунків	0	10	20	70
Ін’єкції	0	10	20	70

Наведена вище інформація вкладається у наступні висновки:

- вектори атак суттєво не змінились за останні 5 років;
- найуразливішими до атак є веб застосунки та людський фактор, використовуючи вразливості серверів, викрадені дані авторизації та соціального інжинірингу;
- атаки на відмову в обслуговуванні є найпопулярнішими для створення інцидентів інформаційної безпеки;
- створення великої кількості інцидентів і неефективність систем управління інформаційною безпекою послаблюють обороноздатність і відвертають увагу від потенційних місць зламу.

Апробація методу

Процес розробки і підтримки будь яких застосунків є доволі динамічним процесом, над яким зосереджується більша частина ресурсів продуктових компаній. Імплементація нових функцій і інтерфейсів, тестування багів, покращення інтерфейсів та зручності використання є постійними та циклічними процесами. Саме тому, більшість компаній виставляючи пріоритет на швидкість розробки жертвують безпекою такого продукту. Процес управління вразливостями є доволі специфічним і творчим одночасно. За правильної організації процесу, користувачі, розробники та етичні хакери можуть як допомагати у цьому процесі, так і ускладнювати його. Випадково чи навмисно знайдена вразливість може бути виявлена так само неочікувано швидко, або через великий час, після перебору і використання дуже складних технік тестування. Наступний важливий фактор є період життя знайденої вразливості, який за одиницю часу може бути виявлено, або вона буде виправлена без інформації про її існування у власника. Нині описані фактори було враховано для створення вірогідності використання найденої вразливості за наступною градацією:

1. Навмисний пошук на замовлення організації (зовнішній пентестинг);
2. Навмисний пошук хакерами (APT атака);
3. Навмисний пошук на замовлення організації (баг-баунті);
4. Навмисний пошук внутрішніми ресурсами (пентестинг);
5. Навмисний пошук внутрішніми ресурсами (сканування інструментами);
6. Ненавмисний пошук користувачами.

Було проаналізовано можливий характер дій для виявленої вразливості. Виявлена вразливість може бути знайдена користувачем випадково, оскільки користувачі, у більшості випадків не мають навичок етичних хакерів, і не можуть оцінити вплив виявленої вразливості на систему. По іншу сторону етичні хакери, які можуть бути як чорними так і білими хакерами, які навмисно обрали ціль для виявлення вразливості. На рис. 6 зображено діаграму можливого розвитку подій при виявленні вразливості користувачем або етичним хакером.

ISSN 2663 - 4023

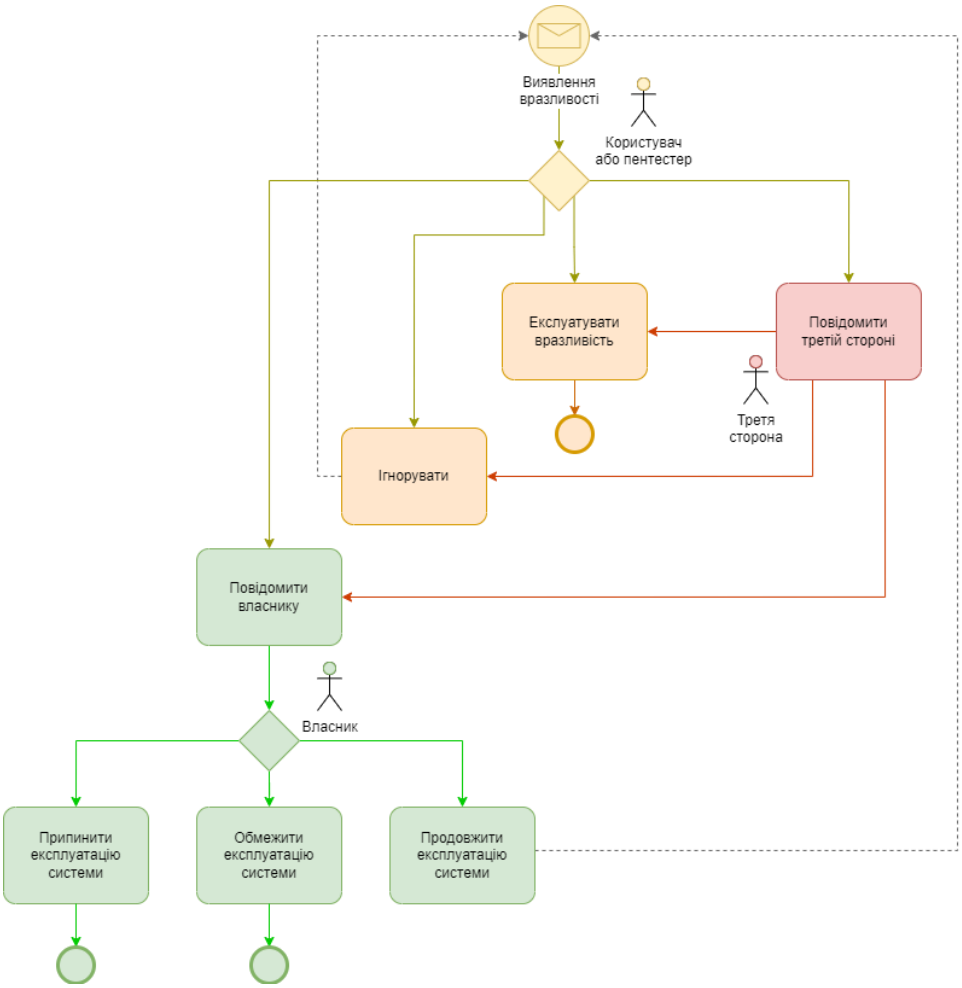

Рис. 6. Розвиток подій при виявлені вразливості в інформаційній системі

Розрахунок базової вартості відбувається простим множенням:

$$y = 500a, \tag{1}$$

де a — базова оцінка CVSS в інтервалі [4..10].

Розрахунок ефективної вартості програми\вразливості відбувається за формулою:

$$x = \frac{d\big(y * (b * c)\big) * e}{f}, \tag{2}$$

де a — рівень ризику (0,10 — низький, 0,25 — середній, 0,75 — високий, 1,00 — критичний); c — критичність системи (0,10 — низький, 0,25 — середній, 0,75 — високий, 1,00 — критичний); e — нокаут фактор (0 — присутній, 1 — відсутній); час існування вразливості (1,50 — до 7 днів, 1,00 — від 8 до 30 днів, 0,75 — від 31 до 90 днів, 0,40 — від 91 дня); f — кількість звітів по вразливості (1 — за 1-е повідомлення, 2 — за 2-е, 100 — за 3-е та наступні).

Окрім фактично підрахованої вартості провалідованої вразливості, також існують наступні фактори, які мають бути врахованими перед виплатою нагороди:

1. Існує вірогідність, що інформацію про вразливість отримає той, хто більше заплатить. Інформація про вразливість може бути ціннішою або для власника системи, або для інших зацікавлених сторін. На момент оцінки вартості вразливості, фактична ціна за вразливість може бути більшою для:

– власника системи, що заявив про присудження або збільшення нагороди за знайдену вразливість;

– іншої зацікавленої сторони, що заявила про нагороду за знайдену вразливість у такій системі.

2. Наявність нокаут фактору:
   – вразливість валідна, проте не входить в скоп програми (наприклад, домен не в скопі, приймаються тільки високі і критичні вразливості);
   – вразливість валідна, проте вона знаходиться поза зоною контролю замовника (наприклад, плагін для Atlassian);
   – вразливість валідна, але про неї було сповіщено постачальником або розробником про виявлення або закриття такої вразливості (до повідомлення про виявлення вразливості етичним хакером/користувачем);
   – вразливість існує, але не може бути застосована — невалідна;
   – знайдена вразливість відноситься до інформаційної системи або модуля системи, яку розробляє інша сторона і є відповідальною за забезпечення безпеки ресурсу (наприклад, інтеграція зі сторонньою системою «supply chain attack»).

Експериментальна перевірка методу

Для перевірки роботоздатності запропонованої формули необхідно провести калькуляцію на існуючих випадках. Платформа HackerOne надає можливість зробити звіти публічними, тому було вибрано три програми випадковим чином з різним рівнем складності [18]–[20]. Результати валідації представлено в табл. 5.

Таблиця 5

Валідація формули на прикладні існуючих звітів

Назва фактору	Коефіцієнт фактору		
	GitHub	**kOps**	**HackerOne**
Базова оцінка CVSS	6	8	8
Рівень ризику	0,25	0,75	1,00
Критичність системи	0,75	0,75	1,00
Нокаут фактор	1	1	1
Час існування вразливості	1,5	1,0	1,5
Кількість звітів по вразливості	1	1	1
Ефективна вартість програми\вразливості, $	844	2250	6000
Базова вартість, $	3000	4000	4000
Різниця між запропонованою та розрахованою сумами, $	–156	–250	–1500
Відносне відхилення, %	–15	–10	–20

Кожна програма була оцінена відповідно до запропонованої формули, з урахуванням орієнтовних факторів, таких як: рівень ризику, критичність системи та час існування вразливості. Кожна програма має свій бюджет, розмір якого є невідомим. Також неможливо врахувати усі додаткові фактори, які були описані у цьому розділі вище. Результати валідації представлені у вигляді різниці між оригінальною сумою винагороди, призначеною власником системи і результатом калькуляції формули. Також різниця представлена у відсотковому співвідношенні. Такий розрив свідчить про наявність додаткових факторів, які не враховані. Проте, в цілому сума виплат за новим підходом близька до оригінальної. У порівнянні між програмами kOps і HackerOne видно, що остання надає фінансування більше ніж в два рази, що значно заохочує дослідників шукати вразливості. За даними програмами, найвірогідніше, що дубльовані звіти про вразливість від інших хакерів будуть виступати нокаут фактором, що також слід врахувати.

Пріоритезація та арбітраж

Знайдені вразливості потребують валідації. На прикладі двох найпопулярніших платформ баг-баунті HackerOne використовує обов'язково базову калькуляцію CVSS вер. 3.1 за п'ятьма факторами, та опціонально розширену калькуляцію CVSS за восьма факторами. Також специфіка калькуляції вразливостей HackerOne полягає у поєднанні оцінок базової та середовища [21]. В той же час Bugcrowd використовує власну методологію Bugcrowd's Vulnerability Rating Taxonomy [16]. Така методологія побудована за принципом власного поділу критичності, який є результатом багаторічних валідацій та досвіду, отриманого за весь час введення такої таксономії.

Наведені вище методології оцінювання вразливостей є базовими, про потребують валідації зі сторони власника інформаційної системи. Під час валідації важливо забезпечити незалежну та якісну оцінку знайденої вразливості та присудити справедливу винагороду. Як правило така валідація відбувається за наступною схемою (див. рис. 7). У таких випадках платформи баг-баунті виступають арбітрами та назначають своїх представників для покращення процесу управління вразливостями між власником інформаційної системи та дослідником вразливості [22].

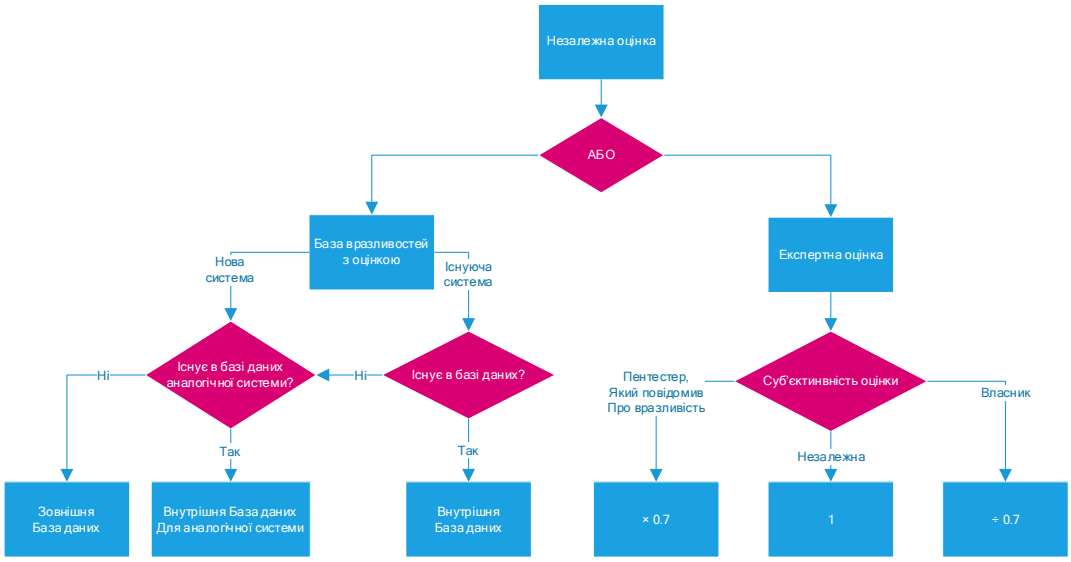

Рис. 7. Процес арбітражу оцінки вразливості

Такий процес називають сортуванням (від фр. triage), представники платформи, що входять у склад команди з сортування покращують процес наступним чином:

– перевірка адекватності і цінності інформації у початковому звіті;
– перевірка відповідності скопу програми;
– пошук дублів.

Рекомендації для запровадження програми баг-баунті

Результати дослідження вказують на наявність додаткових факторів, які складно попередньо прорахувати, оскільки вони є індивідуальними у кожному випадку. Однак, наявність таких факторів можна передбачити. Беручи до уваги незрілі програми, які були запущені власниками систем до трьох років, пропонується на організаційному рівні закласти у бюджет додаткових 10–20%, що допоможе покрити потенційні витрати та забезпечити стабільні витрати і набуття хорошої репутації і оптимізації програми.

Щоб забезпечити успіх та ефективність програми винагороди за виправлення помилок, слід враховувати наступні рекомендації:

1. Чітко визначте сферу застосування програми винагороди за виправлення помилок, включно з програмним забезпеченням, системами та платформами, які підлягають тестуванню.
2. Запропонуйте конкурентоспроможні та привабливі винагороди, щоб мотивувати етичних хакерів до участі в програмі. Формальні принципи при побудові розрахункових формул приведені в даній статті.
3. Впровадьте політику «безпечної гавані», яка захищає етичних хакерів від судових позовів за добросовісне повідомлення про вразливості.
4. Виділіть спеціальну контактну особу для спілкування з етичними хакерами, яка оперативно реагує на повідомлення про вразливості, підтверджує їхнє надходження та інформує хакерів про статус їхніх знахідок.
5. Створіть безпечне та контрольоване тестове середовище, де етичні хакери можуть проводити оцінку вразливостей, не впливаючи на виробниче середовище та дані користувачів.
6. Надайте чіткі інструкції щодо того, як повідомляти про вразливості, в тому числі про те, яку інформацію слід включати до звіту та як безпечно його надсилати.
7. Визначте чіткий процес оцінки та визначення пріоритетності вразливостей, про які повідомляється.
8. Пропонуйте освітні ресурси та документацію, які допоможуть етичним хакерам зрозуміти технологічний стек організації, засоби контролю безпеки та типові вразливості.
9. Постійно переглядайте та оновлюйте програму винагороди за виправлення помилок на основі відгуків, отриманих уроків та змін у загрозах безпеці.
10. Будьте прозорими щодо результатів програми винагород за виправлення помилок та її внеску в покращення загального стану безпеки організації.
11. Активно просувайте програму баг-баунті в спільноті кібербезпеки, щоб залучити різноманітну групу етичних хакерів і збільшити шанси на виявлення критичних вразливостей.
12. Розгляньте можливість партнерства з авторитетними платформами, які можуть допомогти в управлінні програмою, залучити кваліфікованих хакерів, а також надати додаткову підтримку і перевірку знахідок.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Процес управління вразливостей є комплексним, але кількість інструментів і підходів націлені на прискорення і подолання багатьох факторів, що ускладнюють ідентифікацію, валідацію та закриття вразливостей зростає пропорційно кожен рік-два. Баг-баунті як невід'ємна складова процесу управління вразливостями потребує значного рівня зрілості більшості процесів, який компанії набувають зазвичай протягом двох-трьох років від моменту запуску. Запропонована формула розрахунку вартості знайдених вразливостей може стати чудовим стартом для компаній без досвіду запуску програм баг-баунті. У свою чергу адекватно закладений бюджет дозволить оцінити орієнтовну кількість вразливостей, які компанія готова покрити протягом певного періоду часу. Варто зазначити, що наведені рекомендації є результатом тривалого досвіду і напрацювань, та допоможуть зробити процеси управління вразливостями більш зрілими.

Наразі в Україні спостерігаються спроби запровадити легалізацію баг-баунті в українському законодавстві. Наразі застаріле українське законодавство трактує таку діяльність як незаконне втручання в роботу інформаційних систем та карається згідно

кримінального кодексу. В Україні є гостра потреба у забезпеченні інформаційної і кібернетичної безпеки для державних і комунальних установ, що відіграють критичну роль для країни у багатьох секторах. Впровадження державного регулювання і легалізація баг-баунті дозволить покращити інформаційну і кібернетичну безпеку України завдяки запуску програм по пошуку вразливостей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Outsmart Cybercriminals with Proactive Attack Surface Management*. (2023). HackerOne. https://content.cdntwrk.com/files/aT0xNDkwMDE4JnY9MSZpc3N1ZU5hbWU9b3V0c21hcnQtY3liZXJjcmltaW5hbHMtd2l0aC1wcm9hY3RpdmUtYXR0YWNrLXN1cmZhY2UtbWFuYWdlbWVudCZjbWQ9ZCZzaWc9NjZjMTFkOWEyMTc0Y2U0MTA0NGEyYzlmMTk4MzMxMDU%253D
2. *The State of Attack Surface Management*. (2022). Randori. https://www.randori.com/reports/the-state-of-attack-surface-management-2022/
3. *Meta Bug Bounty*. (2023). Meta. https://www.facebook.com/BugBounty
4. Oren, N. (2022). *Looking Back at Our Bug Bounty Program in 2022*. https://about.fb.com/news/2022/12/metas-bug-bounty-program-2022/
5. *Priority One Report*. (2022). Bugcrowd. https://www.bugcrowd.com/resources/reports/priority-one-report/
6. Kipchuk, F., et al. (2021). Assessing Approaches of IT Infrastructure Audit. In *IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*. https://doi.org/10.1109/picst54195.2021.9772181
7. Walshe, T., Simpson, A. (2020). An Empirical Study of Bug Bounty Programs. *In IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF)*. https://doi.org/10.1109/ibf50092.2020.9034828
8. Ahmed, A., Deokar, A., Lee, H. C. B. (2021). Vulnerability Disclosure Mechanisms: A Synthesis and Framework for Market-based and Non-Market-based Disclosures. *Decision Support Systems, 148*. https://doi.org/10.1016/j.dss.2021.113586
9. Ding, A., De Jesus, G., & Janssen, M. (2019). Ethical Hacking for Boosting IoT Vulnerability Management. In *8th International Conference on Telecommunications and Remote Sensing (ICTRS)*. https://doi.org/10.1145/3357767.3357774
10. Parra, C., & Subramanian, H. (2019). A Bargaining Games Approach to Information Security Interactions. In 2019 First International Conference on Digital Data Processing (DDP). *IEEE*. https://doi.org/10.1109/ddp.2019.00025
11. Guo, M., et al. (2021). Revenue Maximizing Markets for Zero-Day Exploits. In *Autonomous Agents and Multi-Agent Systems, 35(2)*. https://doi.org/10.1007/s10458-021-09522-w
12. Ahmed, A., & Lee, H. (2020). Organizational Learning on Bug Bounty Platforms. In *26th Americas Conference on Information Systems (AMCI)*. 1–10.
13. *SecurityScorecard*. (2023). CVSS Scores. https://www.cvedetails.com/cvss-score-charts.php?fromform=1&vendor_id=&product_id=&startdate=2013-06-01&enddate=2023-06-19
14. International Telecommunication Union. (2020). ITU-T Rec. Technical Report. Security in Telecommunications and Information Technology. 7th ed. https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTSS-2020-4-PDF-E.pdf
15. *Directory*. (2023). HackerOne. https://hackerone.com/directory/programs
16. *Vulnerability Rating Taxonomy*. (2021). Bugcrowd https://bugcrowd.com/vulnerability-rating-taxonomy
17. *Data Breach Investigations Report*. (2023). Verizon. https://www.verizon.com/business/resources/Tb4e/reports/2023-data-breach-investigations-report-dbir.pdf
18. *Takeover of hackerone.engineering via Github*. (2023). HackerOne. https://hackerone.com/reports/2085260
19. *Privilege Escalation in kOps using GCE/GCP Provider*. (2023). HackerOne. https://hackerone.com/reports/1842829
20. *An Attacker Can View Any Hacker Email via /SaveCollaboratorsMutation Operation Name*. (2023). HackerOne. https://hackerone.com/reports/2032716
21. *Severity*. (2023). HackerOne. https://docs.hackerone.com/hackers/severity.html#gatsby-focus-wrapper
22. Buriachok, V., Sokolov, V., & Skladannyi, P. (2019). Security Rating Metrics for Distributed Wireless Systems. In *8th International Conference on "Mathematics. Information Technologies. Education" (MoMLeT&DS), vol. 2386*, 222–233.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Feodosiy Kipchuk
Student of Volodymyr Buriachok Department of Information and Cybersecurity
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0003-4816-9246
f.kipchuk.asp@kubg.edu.ua

Volodymyr Sokolov
PhD, associate professor of Volodymyr Buriachok Department of Information and Cybersecurity
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

MODEL FOR CALCULATING THE COSTS OF A BUG BOUNTY PROGRAM FOR TESTING SECURITY VULNERABILITIES

Abstract. The article describes the ways of researching bug bounties of programs and proposes a new approach for calculating the score of the found vulnerabilities. The paper begins with an introduction to the understanding of vulnerability management processes and the concept of an attack surface. The paper analyzes the statistics of all vulnerabilities found in information systems over the past ten years, which are divided according to the standard CVSS score. The types and vectors of attacks are analyzed in the example of the financial sector. Additionally, hacking and incidents are categorized by attack vectors in the financial sector. The following is the ratio of the most popular types and vectors of attacks to the criticality of information systems. A rating of critical and high vulnerabilities of one of the bug bounty platforms is presented with a detailed description of the types of attacks and exploitation techniques. An integral part of the vulnerability management process is the categorization of importance and impact on the organization. Possible life cycle scenarios for the identified vulnerability in an information system are also presented through the eyes of the owner of the vulnerability information and the owner of such an information system. A comparative quantitative and qualitative analysis of the maturity of bug bounty programs from the moment of launch and over the years, as well as the factors influencing the maturity of the program, are carried out. The statistics of vulnerabilities found in public bug bounty programs over the past six years are analyzed. The author proposes her approach to calculating the effective cost of a bug bounty program and conducts an experimental test on three programs. The factors influencing the calculation of the effective cost of vulnerabilities are highlighted. Approaches to vulnerability assessment and validation by bug bounty platforms and the stages of arbitration between the owner of the information system and the vulnerability researcher are considered. The study concludes with recommendations for achieving a higher level of maturity in vulnerability management processes. The forging highlights the continuity of the emergence and disappearance of additional factors in vulnerability management processes, in which bug bounty programs are an integral part. The interdependence of the maturity of the company's processes and its bug bounty program requires the attraction of sufficient resources for its effectiveness.

Keywords: vulnerability; attack; bug bounty; ethical hacking; pen-testing; reward; Common Vulnerability Scoring System; CVSS.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Outsmart Cybercriminals with Proactive Attack Surface Management*. (2023). HackerOne. https://content.cdntwrk.com/files/aT0xNDkwMDE4JnY9MSZpc3N1ZU5hbWU9b3V0c21hcnQtY3liZXJjcmltaW5hbHMtd2l0aC1wcm9hY3RpdmUtYXR0YWNrLXN1cmZhY2UtbWFuYWdlbWVudCZjbWQ9ZCZzaWc9NjZjMTFkOWEyMTc0Y2U0MTA0NGEyYzlmMTk4MzMxMDU%253D
2. *The State of Attack Surface Management*. (2022). Randori. https://www.randori.com/reports/the-state-of-attack-surface-management-2022/
3. *Meta Bug Bounty*. (2023). Meta. https://www.facebook.com/BugBounty
4. Oren, N. (2022). *Looking Back at Our Bug Bounty Program in 2022*. https://about.fb.com/news/2022/12/metas-bug-bounty-program-2022/

5. *Priority One Report*. (2022). Bugcrowd. https://www.bugcrowd.com/resources/reports/priority-one-report/
6. Kipchuk, F., et al. (2021). Assessing Approaches of IT Infrastructure Audit. In *IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*. https://doi.org/10.1109/picst54195.2021.9772181
7. Walshe, T., Simpson, A. (2020). An Empirical Study of Bug Bounty Programs. *In IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF)*. https://doi.org/10.1109/ibf50092.2020.9034828
8. Ahmed, A., Deokar, A., Lee, H. C. B. (2021). Vulnerability Disclosure Mechanisms: A Synthesis and Framework for Market-based and Non-Market-based Disclosures. *Decision Support Systems, 148.* https://doi.org/10.1016/j.dss.2021.113586
9. Ding, A., De Jesus, G., & Janssen, M. (2019). Ethical Hacking for Boosting IoT Vulnerability Management. In *8th International Conference on Telecommunications and Remote Sensing (ICTRS)*. https://doi.org/10.1145/3357767.3357774
10. Parra, C., & Subramanian, H. (2019). A Bargaining Games Approach to Information Security Interactions. In 2019 First International Conference on Digital Data Processing (DDP). *IEEE*. https://doi.org/10.1109/ddp.2019.00025
11. Guo, M., et al. (2021). Revenue Maximizing Markets for Zero-Day Exploits. In *Autonomous Agents and Multi-Agent Systems, 35(2)*. https://doi.org/10.1007/s10458-021-09522-w
12. Ahmed, A., & Lee, H. (2020). Organizational Learning on Bug Bounty Platforms. In *26th Americas Conference on Information Systems (AMCI)*. 1–10.
13. *SecurityScorecard*. (2023). CVSS Scores. https://www.cvedetails.com/cvss-score-charts.php?fromform=1&vendor_id=&product_id=&startdate=2013-06-01&enddate=2023-06-19
14. International Telecommunication Union. (2020). ITU-T Rec. Technical Report. Security in Telecommunications and Information Technology. 7th ed. https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTSS-2020-4-PDF-E.pdf
15. *Directory.* (2023). HackerOne. https://hackerone.com/directory/programs
16. *Vulnerability Rating Taxonomy*. (2021). Bugcrowd https://bugcrowd.com/vulnerability-rating-taxonomy
17. *Data Breach Investigations Report*. (2023). Verizon. https://www.verizon.com/business/resources/Tb4e/reports/2023-data-breach-investigations-report-dbir.pdf
18. *Takeover of hackerone.engineering via Github*. (2023). HackerOne. https://hackerone.com/reports/2085260
19. *Privilege Escalation in kOps using GCE/GCP Provider*. (2023). HackerOne. https://hackerone.com/reports/1842829
20. *An Attacker Can View Any Hacker Email via /SaveCollaboratorsMutation Operation Name.* (2023). HackerOne. https://hackerone.com/reports/2032716
21. *Severity*. (2023). HackerOne. https://docs.hackerone.com/hackers/severity.html#gatsby-focus-wrapper
22. Buriachok, V., Sokolov, V., & Skladannyi, P. (2019). Security Rating Metrics for Distributed Wireless Systems. In *8th International Conference on "Mathematics. Information Technologies. Education" (MoMLeT&DS), vol. 2386*, 222–233.