УДК 004.056

М. Ф. Касьянчук
В. В. Лукічов
І. О. Волокітенко

ЗАХИЩЕНА СИСТЕМА АНАЛІЗУ ДАНИХ ДЛЯ СПЕЦІАЛЬНИХ ЗАДАЧ

Вінницький національний технічний університет
Головне управління Національної поліції у Вінницькій області

Анотація. *Розглянуто основні методи та засоби збору даних для веб-систем, визначено їх переваги, недоліки та вразливості захисту. Також розглянуто стандарт управління ризиками ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT), визначено його переваги та недоліки, запропоновано розробку методу оцінки ризиків.*

Ключові слова: *веб-система, збір даних, кібератака, стандарт оцінки ризиків, метод, критерій.*

Система збирання та аналізування даних передбачає використання веб-технологій, як бази для збору інформації. Щоб система була захищеною вона має відповідати переліку стандартів ISO/IEC визначених чинним законодавством України [1]. Оскільки система збирання та аналізування даних може бути атакованою як різним шкідливим програмним забезпеченням, так і кіберзлочинцями – потрібно передбачати ризики інформаційної безпеки. Для таких цілей у списку стандартів ISO/IEC є стандарт ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. Та якщо розглядати цей стандарт детально, ми можемо побачити, що він розрахований на велику кількість різних структур. Безумовно така варіативність є його перевагою адже надає можливість адаптувати рекомендації даного стандарту до власної структури для тої чи іншої компанії. Та недоліком стандарту ISO/IEC 27005:2019 є відсутність нормативного аспекту. А точніше коли справа доходить до визначення сфери управління ризиками, організація повинна робити все незалежно від того, чи це сфера застосування системи управління інформаційними ризиками, чи навіть критерії ризику. Тому такий підхід є доцільним лише для організацій які готові інвестувати значні внутрішні ресурси в розробку власної методології. Для того щоб компанії неготові витрачати значні ресурси на розробку власних методів управління ризиками могли ефективно використовувати даний стандарт захисту, **актуальною** є розробка простого та гнучкого методу управління ризиками, який зможе забезпечити задовільний чи навіть високий рівень безпеки для організацій з обмеженими ресурсами. Метод, який можна буде використовувати і для оцінки ризиків систем збирання та аналізування даних.

Постановка задачі. Відомий стандарт ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT). Потрібно розробити метод оцінки ризиків, що забезпечить високий або задовільний рівень захисту для систем збирання та аналізування даних.

Для **розв'язання задачі** необхідно розглянути методи збору інформації та їх засоби, а також види загроз, для систем даного типу. Потрібно сформувати основні критерії оцінки ризиків, визначити алгоритм на який буде опиратись метод при оцінці ризиків для систем збирання та аналізування даних.

Методи збору інформації мають такі види:

- Тематичне дослідження - це детальний опис процесу, структури чи досвіду в одній організації. Тематичні дослідження використовують опитування, статистичні дані про використання та якісні методи збору даних. Під час проведення досліджень спочатку збираються кількісні дані, а потім використовуються якісні стратегії.
- Контрольний список - це структура списку пунктів, яку потрібно спостерігати або оцінювати. Використовуючи цю техніку, ви можете відзначити наявність або відсутність критеріїв або записати короткі коментарі щодо теми.

- Інтерв'ю - для збору даних за допомогою цієї техніки інтерв'ю проводяться в групах або індивідуально. Під час співбесіди дані можна збирати за допомогою стенографії, відеозаписів, аудіозаписів або письмових нотаток.
- Опитування проводяться за допомогою анкет. Для проведення опитування з будь-якої конкретної теми використовується стандартний набір питань.
- Документи та записи включає перевірку наявних даних з баз даних, звітів, протоколів засідань, фінансових записів та інформаційних бюлетенів тощо. Це економічно ефективний метод збору даних. Однак іноді це може бути не повне джерело даних [2].

Поширеними засобами збору даних на веб-сайтах є:

- Форми – простий та ефективний засіб збору даних з полів відповідних форм, де користувач самостійно вводить дані в поля. Перевагою засобу є те, що для конкретної цілі збору даних від користувача можна визначити кількість необхідних полів, забезпечити їх коректність введення за допомогою валідації (перевірки коректності введених даних). Недоліком такого засобу є людський фактор, але зменшити цю вразливість допомагає валідація відповідних полів.
- Персери – програмне забезпечення що самостійно шукає необхідну інформацію в мережі, найчастіше шляхом, перебору текстового наповнення коду тих чи інших веб-ресурсів. Перевагою такогозасобу є його автономність, а недоліком може стати збір зайвої або некоректної інформації так, як при налаштуваннях парсера користувач може ввести не чіткі налаштування або такі налаштування, що не повністю відповідають цілям збору даних [3].

Системи збору та аналізу даних реалізовані через веб-застосунки та розміщені в мережі Інтернет часто можуть бути атаковані різними кіберзлочинцями (хакерами) або зловмисним програмним забезпеченням. Веб-системи найчастіше бувають вразливими до таких видів кібератак:

- Denial of Service – відмова в обслуговуванні. Це мережева атака, за допомогою якої зловмисники намагаються перенавантажити сайт таким чином, щоб він почав гальмувати, або став недоступний для звичайних користувачів. Тобто мета атаки, вичерпати ресурси сайту і досягти стану, коли він вже не в змозі відповідати на нові запити клієнтів – з цього моменту сайт вимушений «відмовляти в обслуговуванні» [4].
- DDoS – це випадки, коли сайт атакують не з одного пристрою, а відразу з великої кількості пристроїв. Чим більша кількість пристроїв, тим більше навантаження на сервер і вище ймовірність зробити сайт недоступним. Складність атаки вимірюється в часових рамках, чим довша атака, тим вона небезпечніша. Деякі іноземні компанії виділяють 5 типів DDoS-атак: TCP, HTTP, UDP, ICMP, інші.
- Троянські програми, або трояни (trojan) – це різновид шкідливих програм, які завдають шкоди системі, маскуючись під якісь корисні додатки. Троянські програми можуть застосовувати в якості прикриття знайомі користувачеві додатки, з якими він працював і раніше, до появи в комп'ютері «троянського коня». При іншому підході в повній відповідності з древньою легендою троянська програма приймає вид нового додатку, який намагається зацікавити користувача—жертву якимись своїми нібито корисними функціями.
- Мережеві черв'яки (worm) – це програми, здатні до самостійного поширення своїх копій серед вузлів в межах локальної мережі, а також з глобальних зв'язків, переміщаючись від одного комп'ютера до іншого без будь—якої участі в цьому процесі користувачів мережі. Оскільки більшість мережевих черв'яків передаються у вигляді файлів, основним механізмом їх поширення є мережні служби, засновані на файловому обміні. Так, черв'як може розсилати свої копії по мережі у вигляді вкладень в повідомлення електронної пошти або шляхом розміщення посилань на заражений файл на якому—небудь веб—сайті. Однак існують і інші різновиди черв'яків, які для своєї експансії використовують складніші прийоми, наприклад, пов'язані з помилками («дірками») у програмному забезпеченні.
- Шпигунські програми (spyware) – це такий тип шкідливих програм, які таємно (як правило, віддалено) встановлюються зловмисниками на комп'ютери нічого не підозрюють користувачів, щоб відстежувати і фіксувати всі їхні дії. У число таких дій може входити введення імені та пароля під час логічного входу в систему, відвідування тих чи інших веб—сайтів, обмін інформацією з зовнішніми і внутрішніми користувачами мережі та ін. Зібрана інформація пересилається зловмисникові, який застосовує її в злочинних цілях.
- Спам – це атака, виконана шляхом зловживання можливостями електронної пошти.Враховуючи ту важливу роль, яку відіграє електронна пошта в роботі сучасних підприємств і організацій, можна

зрозуміти, чому спам, дезорганізують роботу цієї служби, став розглядатися в останні роки як одна із суттєвих загроз безпеці [5].

Захист від даних видів атак досягається різними комплексними засобами. Деякі атаки можна зупинити на клієнтській частині, а інші можливо виявити і зупинити лише на серверній частині веб-системи.

Оскільки система збирання та аналізування даних буде реалізована через веб-додаток то при оцінці ризиків критеріями можуть бути такі фактори як вразливість сайту до DDoS-атак різних типів, також наявність конфіденційної передачі даних та їх шифрування. Наявність закритого доступу до даних які доступні лише авторизованим користувачам. Також для оцінки ризиків необхідно визначити порогові значення та критерії прийнятності, якщо їх буде перевищено – реагувати на ризик.

Висновок. В даній статті ми розглянули основні методи та засоби збору даних для веб-систем, визначили їх переваги, недоліки та вразливості захисту. Також розглянули стандарт управління ризиками ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) і визначили його переваги та недоліки, запропоновали розробку методу оцінки ризиків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Наказ про прийняття та скасування державних стандартів. URL: https://zakon.rada.gov.ua/rada/show/v0312774-19#Text
2. Data gathering strategies. URL: https://uk.myservername.com/10-best-data-collection-tools-with-data-gathering-strategies (дата звернення: 22.09.2022)
3. Збір інформації. Парсери. URL: https://avada-media.ua/ua/services/parser/(дата звернення: 27.09.2022)
4. Denial of Service. URL: https://www.trendmicro.com/vinfo/us/security/ definition/denial-of-service-dos (дата звернення: 02.10.2022)
5. Захист локальної мережі. URL: https://sites.google.com/site/zahistlokalnoiemerezi/tipi-atak

Касьянчук Максим Федорович – студент групи 1БС-21м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця. mfkasyanchuk@meta.ua

Лукічов Віталій Володимирович – к.т.н., старший викладач кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця.

Волокітенко Ігор Олександрович – доктор філософії, майор поліції, заступник начальника Головного управління Національної поліції у Вінницькій області, м. Вінниця.

Науковий керівник: ***Лукічов Віталій Володимирович***.

SECURE DATA ANALYSIS SYSTEM FOR SPECIAL TASKS

Abstract. *The main methods and means of data collection for web systems are considered, their advantages, disadvantages and security vulnerabilities are determined. The ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) risk management standard was also considered, its advantages and disadvantages were determined, and the development of a risk assessment method was proposed.*

Keywords: *web system, data collection, cyber attack, risk assessment standard, method, criterion.*

Maksym Fedorovych Kasianchuk - student of group 1BS-21m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia. mfkasyanchuk@meta.ua

Vitaliy Volodymyrovych Lukichov - Ph.D., senior lecturer of the Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Ihor Oleksandrovych Volokitenko - doctor of philosophy, police major, deputy chief of the Main Directorate of the National Police in the Vinnytsia region, Vinnytsia.