УДК 004.056

І. С. Смолявський
В. В. Лукічов
І. О. Волокітенко

СИСТЕМА ЗАХИСТУ ДАНИХ ДЛЯ СПЕЦІАЛЬНИХ ЗАДАЧ

Вінницький національний технічний університет
Головне управління Національної поліції у Вінницькій області

Анотація. *В роботі розглядається міжнародний стандарт безпеки інформаційних технологій ISO/IEC 27001. Розглядається його впровадження в інформаційні системи, структура цього стандарту а також все сімейство стандартів ISO/IEC 27x. Рівень на якому даний стандарт впроваджений на території України проблематика його впровадження та вдосконалення в національній системі інформаційної безпеки.*

Ключові слова: *безпека інформації, захист інформації, запобігання ризиків, органи оцінки відповідності, інформаційна безпека, інформаційні технології.*

В процесі розвитку інформаційних технологій, паралельно розвивається сфера інформаційної безпеки. За останні декілька десятиліть було вироблено десятки різних методів та практик захисту інформації, які зібрані до купи в системах управління інформаційною безпеки. Користуючись цими практиками, спеціалісти з інформаційної безпеки можуть ефективно реагувати та протидіяти сучасні загрозам, що виникають в інформаційній сфері. Одним з таких методів є міжнародний стандарт інформаційної безпеки ISO/IEC 27001. Він увібрав у себе найкращі практики з організації управління інформаційною безпекою та найкращі методи протидії ризикам. Впровадження даного стандарту в національну систему інформаційної безпеки допоможе державі в максимально швидких строках реагувати на різного роду загрози в інформаційному середовищі. Дотримання саме цього стандарту – великий крок до визнання перед світовим товариством а також покращує економічні показники країни. Виходячи з цього, тема роботи є актуальною на сьогодні. Метою роботи являється ознайомлення з стандартом ISO/IEC 27001. Визначення його ролі у світовій системі інформаційної безпеки та системі ІБ України. Дослідження проблематики впровадження ISO/IEC 27001 в Україні в систему.

Постановка задачі. Відомий стандарт ДСТУ ISO/IEC 27001 Потрібно розробити методику захисту, що забезпечить високий або задовільний рівень захисту для систем збирання та аналізування даних.

Відповідно до ISO / IEC 27001: 2013 та ISO / IEC 27002: 2013, основні вимоги безпеки до даних є конфіденційність, цілісність, доступність, справжність, підзвітність та конфіденційність.

Для **вирішення задачі** було розглянуті основні методи виявлення та знешкодження загроз а також методики запобіганню атакам.

Системи IPS можна розглядати як розширення систем виявлення вторгнень (IDS), так як завдання відстеження атак залишається однаковою. Однак, вони відрізняються в тому, що IPS повинна відслідковувати активність в реальному часі і швидко реалізовувати дії щодо запобігання атак.

Методика захисту від DoS-атак.

Ідентифікація за допомогою цифрового відбитку браузера. Суть техніки Browser Fingerprinting в тому, що код опитує браузер користувача на предмет всіх специфічних та унікальних налаштувань і даних для цього браузера і для цієї системи, для комп'ютера. Для ідентифікації можна використати, наприклад, такі дані [2]: мова браузера; часовий пояс; розмір екрану, масив, глибина кольору екрану; системний шрифт; SessionStorage, LocalStorage, IndexedDB, OpenDatabase і інші технології стандарту HTML5; налаштування процесорів doNotTrack, cpuClass, тип платформи та інші дані, що стосуються користувача та платформи; інформація про плагіни. Всі ці отримані дані об'єднуємо у рядок і передаємо на вхід хеш-функції, яка використовує їх і перетворює на 32-розрядний номер у вихідному файлі. Це і буде ідентифікатор користувача. В цілому, можна збирати більше або менше даних для ідентифікації, тим самим збільшуючи або зменшуючи точність вгадування клієнта, але що більша точність – то більше ресурсів сервера треба виділити на цю операцію.

Формування «рейтингу лояльності» користувача. Для формування «рейтингу лояльності» кожному користувачу з ідентифікатором обчислюється значення параметру (наприклад, час, проведений на сайті або веб-сервісі), а потім цей параметр порівнюється з параметрами часу інших користувачів сайту або веб-застосунку. Також отриманий параметр можна порівнювати з середнім значенням всіх користувачів. Отримане порівняння може мати декілька станів – наприклад: «невідомий користувач», «відомий користувач», «лояльний користувач». Його ми записуємо на сервер та асоціюємо з ідентифікатором. В залежності від специфіки кожного окремо розглянутого сайту або сервісу параметр часу може бути замінений на будь-який інший, який відображає лояльність користувачів. Наприклад – кількість відвіданих сторінок сайту або кількість придбаного товару. Однозначно лояльними можна вважати користувачів, які пройшли процес реєстрації на сайті та навели дані про себе.

Запис ідентифікатора на бік клієнта. Для аутентифікації користувача під час перевищення ліміту запитів на сервер він повинен довести свою неналежність до ботів, які атакують сервер. Для зменшення навантаження на фільтр можна використовувати cookie з раніше записаним ідентифікатором (цифровим відбитком браузера). Ефективним елементом збереження інформації в файлі cookie є елемент, який не можна видалити. Для цієї мети можна використати evercookie, що не тільки зберігає дані в сховищі, наприклад, файли cookie-файлів, але і використовує всі доступні репозиторії сучасних веб-браузерів. Для звичайного користувача, знання якого поверхові, видалення цих файлів cookie неможливе, оскільки потрібно отримати доступ до 6-8 місць на жорсткому диску для виконання ряду дій, щоб їх очистити [3].

Реалізація роботи сайту під час ймовірної DoS-атаки. Для реалізації фільтрації користувачів можна використовувати проксі-сервери, наприклад nginx або lighttpd. Режим фільтрації включається під час перевищення кількості запитів до сервера. Максимальний ліміт звернень до сервера визначається в кожному випадку окремо і залежить від технічних потужностей сервера. У випадку, коли ліміт звернень перевищений, запускається режим роботи «ймовірність DoS-атаки». Алгоритм роботи фільтру під час цього режиму:

1) Відбувається звернення до сервера, і клієнт передає cookie разом з HTTP запитом; фільтр зчитує ідентифікатор, знаходить відповідний параметр «рейтингу лояльності» і, якщо параметр відповідає певним критеріям, переадресовує клієнта на сервер.

2) Якщо cookie відсутня, то фільтр ідентифікує браузер за допомогою цифрового відбитку і шукає збіги в базі даних відомих користувачів. Якщо збіг знайдено і параметр «рейтингу яльності» відповідний – переадресовує клієнта на сервер. 3) В усіх інших випадках проксі-сервер відсіює запити на доступ до серверу, доки кількість звернень на сервер не повернеться до норми (нижче максимального ліміту звернень). Як саме буде відбуватися відхилення або пропуск користувача на сайт, залежить від окремо вибраної технології фільтру – міжмережевого екрану. Завдяки такому алгоритму лояльні і постійні користувачі сайту або веб-застосунку можуть без перешкод користуватись веб-сервером, тоді як боти та ненадійні користувачі не матимуть доступу до сайту, тим самим знижуючи навантаження на сервер. Це зробить DoS-атаку недоцільною у зв'язку з тим, що сайт або сервіс не втрачає своїх постійних і лояльних користувачів, а отже не втрачає свої прибутки у таких великих кількостях, як було би за умови загальної відмови у обслуговуванні для всіх користувачів.

Висновок. В даній статті розглянуто основний стандарт ДСТУ ISO/IEC 27001 та метод протидії DoSатакам з урахуванням інтересів власника сайту та його постійних користувачів. Запропоновано простий алгоритм дій для підготовки протидії DoS-атакам, а також алгоритм дій під час ймовірної DoS-атаки. Запропонована методологія є досить гнучкою і масштабованою, тому може бути використана для захисту сайтів та сервісів дуже широкого профілю, незалежно від їх специфіки та об'ємів відвідування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Наказ про прийняття та скасування державних стандартів. URL: https://zakon.rada.gov.ua/rada/show/v0312774-19#Text
2. Browser Fingerprint – анонимная идентификация браузеров [Електронний ресурс]. — 2017. — Режим доступу: https://habr.com/company/oleg-buni n/blog/321294/. (дата звернення: 22.09.2022)
3. March 2017 Web Server Survey [Електронний ресурс]. — 2017. — Режим доступу: http://news.n etcraft.com/archives/2017/03/24/march-2017 -web-server-survey.html. (дата звернення: 27.09.2022)

4. Evercookie – самые устойчивые куки [Електронний ресурс]. — 2014. — Режим доступу: https: //habr.com/post/104725/02.10.2022)
5. Захист локальної мережі. URL: https://sites.google.com/site/zahistlokalnoiemerezi/tipi-atak

Смолявський Ілля Сергійович – студент групи 1БС-21м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця. Illya.acrobat38@gmail.com

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

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

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

DATA PROTECTION SYSTEM FOR SPECIAL TASKS

Abstract. *The work examines the international information technology security standard ISO/IEC 27001. Its implementation in information systems, the structure of this standard, and the entire family of ISO/IEC 27x standards are considered. The level at which this standard is implemented on the territory of Ukraine, the issues of its implementation and improvement in the national system of information security.*

Keywords: *information security, information protection, risk prevention, conformity assessment bodies, information security, information technologies.*

Smoliavskyi Illia Sergiovich- student of group 1BS-21m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia. Illya.acrobat38@gmail.com

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. lukichov.vitalyi@vntu.edu.ua

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