АНАЛІЗ ЗАГРОЗ БАЗАМ ДАНИХ В ЕЛЕКТРОЕНЕРГЕТИЧНІЙ ГАЛУЗІ ДЛЯ ПІДФИЩЕННЯ ЗАХИСТУ СИСТЕМ КЕРУВАННЯ

Воскобойник П.О., магістрант, Лавренова Д.Л., к.т.н., ст. викл.
КПІ ім. Ігоря Сікорського, кафедра автоматизації енергосистем

Вступ. Безпека, захист і надійність завжди були важливим питанням проектування та експлуатації енергосистем. А з розвитком інформаційної інфраструктури електроенергетичної галузі інформаційна безпека стає все більш важливою. На сьогодні розроблений ряд стандартів для забезпечення кіберзахисту саме енегооб'єктів [1]. Одна із задач убезпечення роботи енергосистеми (та об'єктів електроенергетики) є безпека баз даних. Бази даних стали невід'ємною та важливою частиною всього комплексу програмного забезпечення. Системи баз даних дозволяють систематично зберігати дані про стан енергосистеми для подальшого оброблювання та аналізу, зокрема в режимі реального часу.

Мета роботи. Проаналізувати типи кіберзагроз базам даних в електроенергетичній галузі.

Матеріали і результати досліджень. Роботу систем баз даних розділяють на дві узагальнені категорії: управління даними (отримання, передавання та зберігання інформації) та аналіз даних.

На сьогоднішній день робота з даними в інформаційно-комунікаційних системах проводиться або в системах керування базами даних, або, інколи, в простих файлових системах. В обох випадках основними функціями системи керування базами даних є:

– визначення формату даних та встановлення зв'язків між елементами бази даних;
– збір даних та занесення їх до бази;
– оновлення або видалення вже існуючих елементів бази даних;
– видача необхідних збережених даних за запитом;
– оптимізація процесу видачі інформації;
– обмеження прав деяких користувачів щодо операції над певними елементами бази даних;
– резервне зберігання та відновлення даних, що були втрачені.

Загальним стандартом систем керування базами даних є реляційна база даних, тобто зберігання інформації у вигляді таблиць. Зазвичай, для цього використовують Microsoft SQL Server, SAP Sybase, MySQL та PostgreSQL. Також існують системи, що використовують нереляційні бази даних (NoSQL). Такі типи зустрічаються все частіше. Це, наприклад, Apache Cassandra, InfiniteGraph, MongoDB, OpenQM.

Дані можуть зберігатися централізовано на жорстких дисках. Але більш сучасні варіанти – резидентні бази даних, що зберігають інформацію в оперативній пам'яті (voltDB) та зберігання на SSD. Також набуває поширення

зберігання в «хмарі». Хмарні бази даних можна використовувати або шляхом підключення віртуальної машини до стандартної хмари або шляхом використання сервісу баз даних. Прикладами сервісів хмарних баз даних є Amazon's DynamoDB та SimpleDB.

База даних може мати різні внутрішні формати даних. Наприклад, службами режимів використовуються бази даних, що містять інформацію про навантаження, перетоки потужностей, втратах потужності, параметрах нормального режиму, комутаціях тощо, для служб релейного захисту та автоматики необхідні дані по струмах короткого замикання та інформація для визначення місць пошкодження. Службам підстанцій необхідно забезпечити зберігання та обробку даних за результатами ремонту та діагностики силового обладнання. Вся ця інформація є різноплановою і має свої окремі формати. Тобто отримання найбільш повної та достовірної інформації про систему в цілому вимагає значних витрат часу для зведення до єдиного формату різноманітних типів даних.

Оскільки електричні станції мають різні типи – теплові електростанції, гідроелектростанції, вітроелектростанції, сонячні електростанції, то системи керування даними можуть відрізнятися за структурою. Наприклад, для звичайної теплової станції, що працює на вугіллі, система бази даних має містити такі параметри, як тиск пари, коефіцієнт надлишку повітря, температура димових газів та котлової води.

Бази даних систем диспетчерського керування та збору даних (SCADA) та розподілених систем керування (DCS) особливо уразливі. Так несанкціонований доступ до бази даних може дозволити спотворити дані через надання доступу до редагування. А спотворення даних, на яких базується процес керування енергосистемою може призвести до масштабної аварії. Це відноситься до світових загроз – тероризму.

На сьогоднішній день більшість незахищених місць інформаційних мереж швидко становляться публічно відомими та доступними для використання будь-ким. Відповідно, можна навести наступний перелік слабких місць SCADA:

– системи керування для більш ефективного та практичного використання з'єднуються із корпоративними мережами та інтернетом. Але навіть закриті мережі не є ідеально ізольованими, оскільки можливе під'єднання на неконтрольованих зв'язках.

– фізичні компоненти замінюються мікропроцесорними, що мають багато можливостей, зокрема можливість зміни конфігурації через веб-сервер та віддаленого доступу та контролю. Такі можливості збільшують також і кількість потенційних уразливостей.

– широке використання 802.11 WLAN надало широких можливостей для крадіжки інформації. Бездротові мережі дозволяють одному клієнту керувати великою кількістю подій та операцій.

Також слід зазначити, що можливість проникнення в систему керування може виникати через помилки та неуважності персоналу (соціальна інженерія).

Згідно з дослідженнями [2], найбільш частими типами атак є навмисне ушкодження пам’яті, крадіжка даних від облікових записів, перехват даних та ін’єкції коду (рис. 1).

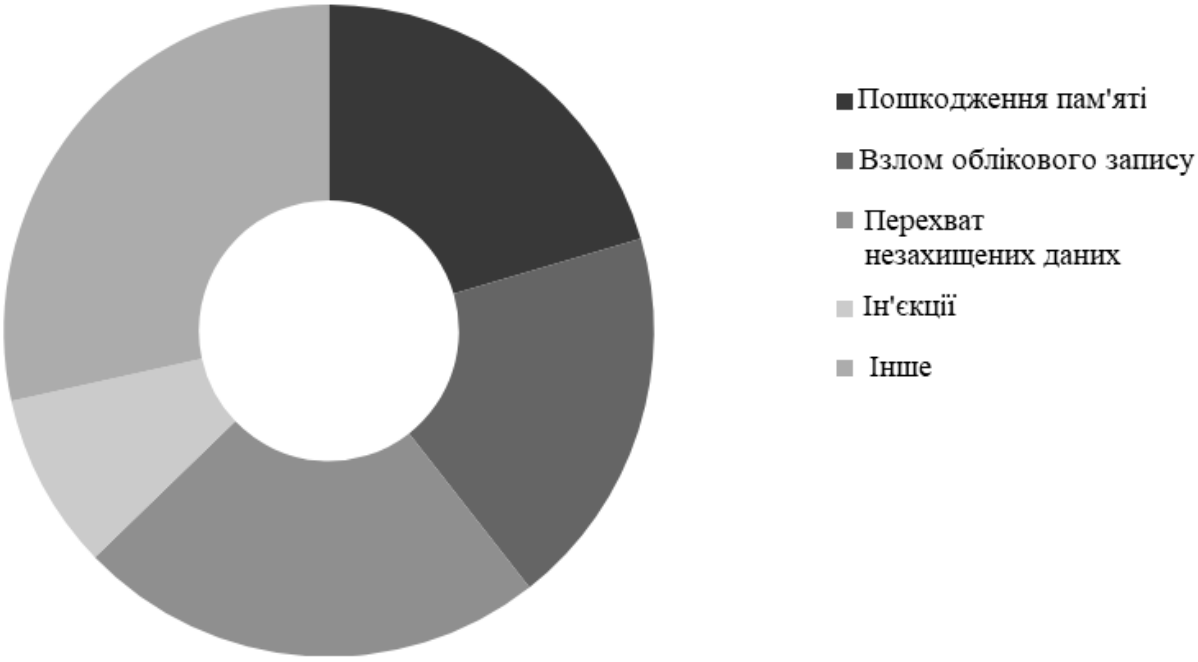

Рисунок 1 – Категорії уразливостей

Як видно з діаграми, найбільшу частку з визначених уразливостей (23%) займає категорія перехоплення незашифрованих даних.

20% від загальної кількості уразливостей займають атаки на пам’ять коли програма під час запису даних перезаписує їх за межами буфера. Це викликає помилки, отримання хибної інформації, відмови програми або проблеми в системі безпеки.

У 19% випадків використовують недоліки системи керування обліковими записами через використання користувачами «слабких» паролів, недбалого їх зберігання та відсутності грамотного обмеження прав категорій користувачів.

Лише 9% загроз – це ін’єкції (занурення) спеціального коду в програму для зміни її роботи. Цей тип найбільш розповсюджений у вигляді SQL-ін’єкцій для спотворення даних з баз даних.

Окрім цього існує загроза проведення атаки на системи керування енергооб’єктами використовуючи концепцію розвідки відкритих джерел (Open source intelligence – OSINT). Одним з методів є пошук серед всіх підключених до інтернету пристроїв та систем з метою отримання доступу через них до інтерфейсів керуванням сонячних, вітрових та гідроелектростанцій [3].

На останок слід зазначити, що починаючи з 2020 року в конкурсі етичних хакерів Pwn2Own з’явиться окрема номінація для зламу промислових систем

керування. Віднині в конкурсі п’ять категорій автоматизованих систем категорій для зламу: сервери керування, сервер уніфікованої архітектури OPC, DNP3-шлюз, інтерфейс користувача (робоча станція оператора) та програмне забезпечення Engineering Workstation (EWS). Зокрема, в результаті цієї акції будуть випробувані на надійність системи безпеки компаній Schneider Electric та Rockwell Automation [4].

Висновки. Ринкові відносини зумовили появу нових загроз, таких як знання конкурента про активи та роботи системи, а також загрозу втручання в роботу енергосистеми ззовні. Задля підсилення кібербезпеки енергосистем впроваджено ряд стандартів. Однак, залишається ряд задач ще не охоплених повною мірою цими стандартами. Наприклад, надійний захист баз даних. А з урахуванням швидкості розвитку інформаційних технологій і, відповідно, технологій зламу та втручання в роботу питання кіберзахисту стають першочерговими особливо в сфері електроенергетики де найменше втручання може призвести до фатальних наслідків.

На сьогоднішній день, як стверджують розробники, єдиним інструментом захисту від шкідливих програм та зламу для пристроїв ICS/SCADA є MalCrawler [5].

Перелік посилань

1. Керування енергосистемами та відповідний інформаційний обмін. Безпека даних та зв’язку. Частина 1. Безпека зв’язку мережі та системи. Загальні положення (IEC/TS 62351-1, IDT), ДСТУ IEC/TS 62351-1:2014. – [Чинний від 02.12.2014]

2. The State of SCADA HMI Vulnerabilities. Vulnerabilities & Exploits, May 23, 2017: [Електроний ресурс] – Режим доступу: https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities

3. Stephen Hilt, Numaan Huq, Vladimir Kropotov, Robert McArdle, Cedric Pernet, Roel Reyes. “Critical Infrastructures Exposed and at Risk: Energy and Water Industries”

4. The Zero Day Initiative [Електроний ресурс] – Режим доступу: https://www.zerodayinitiative.com/blog/2019/10/28/pwn2own-miami-bringing-ics-into-the-pwn2own-world

5. Power Utility Equipment & Technology MalCrawler analyzes. [Електроний ресурс] – Режим доступу: https://www.malcrawler.com/industry/power/