НАПРЯМ 10. ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА У ВОЄННИЙ І ПОВОЄННИЙ ПЕРІОД

DOI https://doi.org/10.36059/978-966-397-444-6-53

Бєляков Р. О.,
кандидат технічних наук, доцент,
заступник начальника кафедри автоматизованих систем управління
Військового інституту телекомунікацій та інформатизації
імені Героїв Крут
м. Київ, Україна

Балан Д. Д.,
викладач кафедри автоматизованих систем управління
Військового інституту телекомунікацій та інформатизації
імені Героїв Крут
м. Київ, Україна

ПРОБЛЕМНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЗАГРОЗ СПОЖИВАННЯ ІНФОРМАЦІЇ ІЗ ВІДКРИТИХ ДЖЕРЕЛ ПОСАДОВИМИ ОСОБАМИ В УМОВАХ ВОЄННОГО СТАНУ

Інформаційна безпека при використанні посадовими особами відкритих джерел інформації є важливою проблемою, яка впливає на безпеку організацій приватність і національну безпеку. Оскільки посадові особи, зокрема керівний склад всіх рівнів часто має доступ до конфіденційної інформації, необережне використання відкритих джерел (таких як соціальні мережі, новинні ресурси або інші публічні платформи) може призвести до безпекових загроз на кількох рівнях. Нижче узагальнено найбільш поширені проблемні питання, які не втрачають своєї актуальності:

1. Фішинг та соціальна інженерія. Фішингові атаки, спрямовані на посадових осіб, використовують відкриті джерела для збору інформації, яка допомагає злочинцям персоналізувати атаки. Наприклад, інформація з соціальних мереж може бути використана для створення правдоподібних листів або повідомлень, що містять особисті фото, відеоматеріали, вподобання посадових осіб, специфіку споживчих пріоритетів, вподобань та смаку, даних про родичів та близьке коло

спілкування, з метою поглиблення рівня знань конфіденційних даних об'єкта спостереження.

Модель атаки може виглядати таким чином:

– злочинець знаходить інформацію про посадову особу через відкриті джерела;

– використовує ці дані для створення контекстного листа (з фальшивим підписом або детальною інформацією, отриманою з соцмереж);

– спонукає посадовця до розкриття даних або встановлення шкідливого програмного забезпечення.

2. Дезінформація та маніпуляція. Проблема дезінформації є ключовою для осіб, які приймають рішення. Використання відкритих але не верифікованих джерел може призвести до поширення фальшивих новин або неправдивих фактів. Це створює ризики для управління в кризових ситуаціях або прийняття стратегічних рішень на підставі хибних даних, результатах аналізу, фальш-трендів. Алгоритм впливу дезінформації: поширення фальшивих новин у відкритих джерелах; вплив на інформаційне поле посадової особи; прийняття рішень на основі недостовірних джерел.

3. Витік конфіденційної інформації. Посадові особи можуть ненавмисно розкривати важливу інформацію через свої власні канали комунікації, такі як використання соціальних мереж або відкриті публікації конфіденційних даних у зв'язку із порушенням базових вимог забезпечення кібергігієни. Часто це – випадкові витоки, такі як фотографії документів, листування, файли, або просто відомості про місцезнаходження об'єкта або його дії, що не повинні бути публічними. Приклад витоку: посадова особа публікує фотографію на публічній платформі; на знімку видно конфіденційні документи або обладнання; витік цієї інформації може бути використаний сторонніми особами для компрометування об'єкту, шпигунства за ним, шантажу тощо.

4. Кібершпигунство та аналіз комунікаційної інфраструктури. Зловмисники можуть використовувати інформацію з відкритих джерел для ідентифікації уразливих посадових осіб або співробітників організації з метою здійснення кібершпигунства. Аналіз відкритої інформації дозволяє зловмисникам знаходити слабкі місця в комунікаційній структурі, яку використовує посадова особа. Сценарій шпигунства:

– моніторинг відкритих джерел, таких як соціальні профілі посадових осіб;

– ідентифікація інтересів, зв'язків і місцезнаходження для підготовки шпигунських дій (наприклад, для встановлення прослуховувальних пристроїв або зараження системи шкідливим ПЗ).

Використання відкритих джерел інформації повинно бути ретельно регламентовано Законами та нормативними актами. Посадові особи

можуть неусвідомлено порушити законодавство про приватність, захист даних або інтелектуальну власність, якщо будуть використовувати неавторизовану інформацію з відкритих джерел.

Для забезпечення інформаційної безпеки необхідно, в першу чергу уникати формалізму проходження освітніх програм та тренінгів для посадових осіб щодо інформаційної (кібер) гігієни та захисту персональних даних. Необхідно постійно здійснювати моніторинг та аналіз відкритих джерел на предмет наявності персональних даних або іншої чутливої інформації. Забезпечити запровадження чітких політик і процедур щодо використання відкритих джерел та взаємодії з медіа. Інформаційна безпека посадових осіб при взаємодії з відкритими джерелами є багатогранною проблемою, яка потребує постійного контролю, навчання і технологічної підтримки, щоб мінімізувати ризики для національної і організаційної безпеки.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 28 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 15.10.2024).

DOI https://doi.org/10.36059/978-966-397-444-6-54

Данькевич Ю. В.,
кандидат філологічних наук, доцент,
доцент кафедри комп'ютерних та інформаційних технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

БЕЗПЕКА ПЕРЕДАЧІ СЛУЖБОВОЇ ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ ДОКУМЕНТАХ ПІДПРИЄМСТВ ДЕРЖАВНОЇ ФОРМИ ВЛАСНОСТІ У ВОЄННИЙ ПЕРІОД

Одним із головних завдань безпечного функціонування систем електронного документообігу підприємств державної форми власності у воєнний час є дотримання нормативно-правових вимог, що регулюють передачу конфіденційної та службової інформації. Особливістю конфіденційної інформації є те, що вона має обмежений доступ як для фізичних, так і юридичних осіб. У статті 7 Закону України «Про доступ до публічної інформації» (далі – Закон) обґрунтовано, хто є «суб'єктами владних повноважень», та як саме конфіденційна інформація