Міжнародна науково-практична конференція

“Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку”

14 березня 2024 року, м. Харків

дальності), радіальної швидкості і ширини допплерівського спектру. Тактико-технічні характеристики наведені в таблиці 3.

Таблиця 3 – Основні ТТХ РЛС Х1-М “Око”

Найменування характеристики	Значення
Інструментальна дальність, км	0,3 – 30
Імпульсна потужність передавача, Вт	30
Сектор огляду по куту місця, °	30
Азимутальний сектор огляду, °	360
Точність:	
– по дальності, м;	5
– по азимуту, °	1
Радіальна швидкість, м/с	0,1
Максимальна швидкість цілі, що супроводжується, м/с	60
Дальність виявлення при С/Ш, більше 15 дБ:	
– БЛА (0,01 м2), км;	7
– людина (0,5 м2), км;	18
– автомобіль, літак, (1 м2), км	25
Споживана потужність, Вт	300
Вага, кг	65

Таким чином, радіолокаційні засоби, які перебувають на озброєнні РТВ Повітряних Сил Збройних Сил України, потенційно здатні виявляти оперативно-тактичні БПЛА в межах своїх тактико-технічних характеристик. Використання оглядових РЛС РТВ для виявлення тактичних міні-БПЛА є недоцільним і невиправданим. Недоцільним – через надзвичайно низькі можливості з виявлення означеного типу цілей, а невиправданим – через невідповідність масштабів задач, для вирішення яких первісно проектувались і розроблялись РЛС РТВ. Новітня РЛС «СНОВ» та «Око» більш ефективні, для виявлення БПЛА, ніж радіолокаційні станції старого парку.

УДК 004.056

Здоренко Ю.М., Хакімов М.Е., Масловський А.В.

МЕТОДИ ЗАХИСТУ ВЕБ-РЕСУРСІВ ВІД ІН’ЄКЦІЙНИХ АТАК НА ОСНОВІ ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ

У сучасному світі використання власних веб-ресурсів є необхідною складовою забезпечення повсякденної діяльності установ та організацій. Цифрова трансформація комерційних та державних секторів відкриває безліч можливостей для швидкого та ефективного доступу до необхідних документів та послуг. Поряд з цим зростає рівень загроз від здійснення кібернетичних атак на веб-ресурси. Деякі атаки можуть відбуватися непомітно (без явних ознак) для користувачів, але мають значний негативний вплив на роботу інформаційних систем та можуть стати причиною витоку даних.

Одним з найпоширенішим способів проведення кібератак на веб-ресурс є ін’єкційні атаки [2]. До них відносять: XSS-ін’єкції (Cross-Site Scripting) та SQL-ін’єкції. Ін’єкційні атаки можуть реалізуватися, коли зловмисники використовують уразливості у веб-додатках, які можуть приймати ненадійні дані. Так, внаслідок додавання зловмисного коду у поля введення форм, можуть бути виконані неавторизовані команди, отриманий доступ до конфіденційних баз даних та отриманий повний контроль над веб-ресурсом. Також необхідно враховувати, що переважна більшість потенційних вразливостей в інформаційних системах виникає через людський фактор. Наприклад, випадкове надання доступу до баз даних особам, які не повинні мати доступу, може стати

причиною несанкціонованого втручання або витоку конфіденційної інформації. Також недбале тестування програмного забезпечення на етапах розробки та використання неперевіреного коду при оновленнях програмного забезпечення веб-ресурсу є передумовою вразливостей, які можуть бути використані зловмисниками для атаки на інформаційну систему. Тому важливо вдосконалювати процеси контролю доступу, навчання персоналу з питань кібербезпеки та ретельно перевіряти програмний код перед впровадженням на веб-ресурсі.

Для виявлення ін'єкційних атак можуть бути використані методи на основі використання інтелектуальних підходів. Так, в роботі [1] запропоновано визначати тип атаки JS(HTML)/ScrInject на основі використання нечіткої системи логічного виводу. Однак даний підхід ґрунтується на налаштуваннях вхідних параметрів на основі експертних знань (оцінок) та потребує періодичного перенавчання таких систем. Тому для визначення факту проведення ін'єкційної атаки та вчасного вжиття запобіжних заходів пропонується удосконалити зазначений підхід та використати нейро-нечітку систему. Такий тип інтелектуальних систем дозволяє поєднати можливості нечітких систем логічного виводу для визначення класу атаки та нейронних мереж - для налаштування значень параметрів систем логічного виводу та їхнього перенавчання. Використання такого підходу дозволить забезпечити надійний захист веб-ресурсів та забезпечити захист від нових атак в майбутньому.

Список використаних джерел

1. Здоренко Ю.М., Фесьоха О.В., Субач І.Ю. Методика виявлення кібератак типу JS(HTML)/ScrInject на основі застосування математичного апарату теорії нечітких множин / Збірник наукових праць ВІТІ № 4, – 2018, м. Київ.

2. OWASP top 10 vulnerabilities. Veracode. URL: https://www.veracode.com/security/owasp-top-10 (date of access: 23.02.2024).

УДК 37.09

Зеленюх О.М., Кузьменко Р.В., Канчуга М.К.

ТЕНДЕНЦІЇ У ПІДГОТОВЦІ ВОДІЇВ АВТОМОБІЛЬНОЇ ТЕХНІКИ

Традиційне навчання водіїв відбувається в один етап, до того, як водій отримує посвідчення водія. Дійсно, основною метою навчання водіїв є підготовка початківців до здачі іспитів на отримання посвідчення водія, а більшість видів навчання вважаються успішними, якщо навчаємі досягають навчальних цілей і успішно складають іспит. Проте очікується, що навчання водінню змінить їхню подальшу поведінку настільки, що це матиме вимірюваний вплив на аварійність. Ґрунтуючись на тривалій історії оціночних досліджень, більшість фахівців скептично ставляться до переваг водійської підготовки з точки зору безпеки руху. Саме навчання водінню стало дуже різноманітним, і створення стратегічного вдосконалення є досить складним завданням. Це важлива галузь у всьому світі, хоча вона залишається дуже фрагментованою.

Сучасне навчання водіїв має на меті зменшити фактори ризику для водіїв-початківців. Зростає розуміння того, що безпечне водіння передбачає зміну навичок і звичок, які визначають фактичну поведінку за кермом. Ненавмисні помилки і неправильні дії, ймовірно, сприяють підвищеному ризику для водіїв-початківців, хоча, можливо, і не в однакових пропорціях для всіх випадків.

Щоб досягти значного підвищення безпеки за допомогою навчання водіїв-початківців, стало досить загальновизнаним, що необхідно впроваджувати більш ком-