УДК004

Ю.В. Литвин , студентка гр.101ТН
Т.М. Деркач, к.т.н., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ СУЧАСНОЇ ВІЙНИ

Інформаційні технології (ІТ) стали важливим елементом військових операцій в сучасному світі. Їх використання забезпечує збільшення ефективності та точності військових дій, а також допомагає забезпечити безпеку та захист військових та цивільних об'єктів.

Інформаційні технології мають різні напрямки використання. Наприклад, для забезпечення зв'язку між різними військовими підрозділами, що дозволяє оперативно координувати дії та передавати важливу інформацію. Зокрема, використання радіо та супутникового зв'язку дозволяє забезпечити швидкий та надійний зв'язок в будь-якій точці світу.

Також однією з ключових галузей військових ІТ є збір та обробка інформації. Це означає збирання та аналіз інформації з різних джерел, включаючи супутникові зображення, відео та аудіозаписи, даних з сенсорів та смартфонів, соціальних мереж та інших джерел. Ці дані можуть бути використані для визначення розташування ворожих військ, руху техніки, пошуку підрозділів та іншої інформації, необхідної для ведення операцій. Саме такі дані потрібні для ефективного використання дронів у воєнний час.

Військові дрони – це безпілотні літальні апарати, які використовуються для виконання різноманітних завдань у військових операціях. Військові дрони можуть бути різних типів та конфігурацій, включаючи малий індивідуальний дрон, середні та великі багатофункціональні апарати з довгим часом польоту. Використання військових дронів зазвичай дозволяє знизити ризик для життя військових, покращити точність ударів та збільшити ефективність виконання різних військових завдань.

Військові дрони мають ряд властивостей, які роблять їх популярними серед військових сил та розвідувальних агентств. До найважливіших властивостей дронів можна віднести дистанційне керування, що дозволяє військовим операторам контролювати дрон з безпечної відстані та уникнути небезпеки.

Військові дрони працюють за допомогою вбудованих комп'ютерів, датчиків, камер, радіо та інших електронних компонентів, які керують польотом апарата та збирають інформацію.

Під час польоту військовий дрон може бути керований оператором на землі або автономно працювати за програмою, яку заздалегідь завантажили в його пам'ять.

Військові дрони (безпілотні літальні апарати) складаються з різних компонентів, які забезпечують їх функціонування та контроль. Усі ці компоненти працюють разом, щоб дати можливість військовим дронам виконувати різноманітні завдання, допомагаючи військовим операціям вестися більш ефективно та безпечно.

Основні компоненти військового дрона:

- Корпус – зазвичай зроблений з легких матеріалів, таких як карбонові волокна або пластик, що дозволяє зберегти вагу і збільшити час польоту.
- Двигун – електричний або залізничний, в залежності від типу дрона. Він забезпечує підйом та рух апарата в повітрі.
- Камера та інші сенсори – ці компоненти використовуються для збору різноманітної інформації про навколишнє середовище, включаючи зображення з висоти, відео, аудіо та дані з GPS.
- Керування – віддалений пульт керування забезпечує можливість дистанційного управління дроном. Він може включати контролер та інші елементи управління.
- Зброя – деякі військові дрони можуть бути оснащені різними видами зброї, такими як ракети або кулемети, що дозволяє їм виконувати завдання у військовій операції.
- Безпека – системи безпеки забезпечують захист від перешкод та відмов компонентів, що можуть вплинути на безпеку польоту.
- Комп'ютерна програма – це програмне забезпечення, що керує рухом дрона, збирає інформацію та передає її до пульта керування або до інших систем. Саме розробка програмного забезпечення є ключовим моментом для забезпечення дієздатності дрона.

Програмне забезпечення, яке використовується в умовах війни може бути різного спрямування та призначення:

- системи управління бойовими машинами (Combat Vehicle Management Systems);
- системи управління вогневою підтримкою (Fire Support Management Systems)
- системи дронів (Drone Systems);
- системи управління комунікаційними мережами (Communication Network Management Systems);
- системи розвідування та аналізу інформації (Intelligence, Surveillance and Reconnaissance Systems).

Ще не менш важливим аспектом є тестування та валідація – перед використанням в реальних умовах дрони повинні бути протестовані та

валідовані, щоб переконатися в їх надійності та ефективності.

Слід зазначити, що використання дронів також може мати етичні та правові наслідки, зокрема щодо порушення приватності та безпеки громадян. Крім того, дрони можуть стати об'єктом кібератак, що може призвести до витоку конфіденційної інформації або перехоплення керування дроном. У цілому, військові дрони мають великий потенціал у військових діях, проте їх використання повинно бути обмеженим та контрольованим з метою забезпечення безпеки та дотримання міжнародного права.

УДК004

В.О. Данилко , студентка гр.103ТН
Т.М. Деркач, к.т.н., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

КІБЕРЗЛОЧИННІСТЬ У ВСІХ ЇЇ ПРОЯВАХ: ВИДИ, НАСЛІДКИ ТА СПОСОБИ БОРОТЬБИ

У наші дні використання інформаційних технологій не має меж. Віртуальний простір переймає від реального все підряд, у тому числі й злочинність у її нових формах і проявах. Поняття кіберпростору, введеного письменником Вільямом Гібсоном у п'єсі «Le Neuromancer», описує віртуальний простір як такий, в якому циркулюють електронні дані всіх комп'ютерів світу.

Практично кожен чув про кіберзлочинність і, можливо, навіть особисто з нею зіштовхувався. Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою комп’ютера і в мережі Інтернет. Об’єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні. Слід відмітити, що кіберзлочинці суттєво активізували діяльність у період воєнного стану в Україні.

Піратство та кіберзлочинність в Україні

Нормативне регулювання цієї сфери в Україні не встигає за розвитком технологій, що загострює проблему кіберзлочинності. На рівні фізичних осіб кіберзлочинність пов’язана з використанням піратського програмного забезпечення: зловмисники можуть отримати доступ до персональних даних користувача. Згідно з дослідженням Асоціації виробників програмного забезпечення (BSA) за останні роки напередодні війни рівень піратства в Україні становив більше 80%. За оцінками Міжнародного альянсу інтелектуальної власності (IIPA), Україну визнано «піратом №1» у світі.