захисту для конкретної мережі необхідно враховувати особливості структури мережі, спеціалізації роботи підприємства, вірогідність проведення конкретних атак. Налаштування відповідного функціоналу на мережевому обладнанні дозволяє здійснювати контроль відповідності політиці мережевої безпеки та реалізовувати захист максимально близько до можливого джерела порушень, що, у свою чергу, мінімізує можливі негативні наслідки для корпоративної мережі моделі OSI.

Список бібліографічних посилань

1. Кучернюк В. П. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні). *Мікросистеми, електроніка та акустика*. 2017. № 6. Том 22. С. 64-70. URL: http://elc.kpi.ua/article/view/113191 (дата звернення: 24.10.2018).

2. Заборовский В. С., Лукашин А. А., Купреенко С. В., Мулюха В.А. Архитектура системы разграничения доступа к ресурсам гетерогенной вычислительной среды на основе контроля виртуальных соединений. *Вестник Уфимского государственного авиационного технического университета*. 2011. 5 (45). Том. 15. С. 170-174. URL: https://elibrary.ru/item.asp?id=18863047 (дата звернення: 24.10.2018).

3. Козлова М. 7 лучших сервисов защиты от DDoS-атак для повышения безопасности // HOSTING.cafe. 28 марта 2017 14:47. URL: https://habrahabr.ru/company/hosting-cafe/blog/324848/ (дата звернення: 24.10.2018).

4. Cisco Network Admission Control (NAC) Solution Data Sheet // Cisco. January 23, 2017. URL: https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html (дата звернення: 24.10.2018).

Одержано 24.10.2018

УДК 004.94

Сергій Геннадійович СЕМЕНОВ,
доктор технічних наук, старший науковий співробітник,
завідувач кафедри обчислювальної техніки та програмування
Національного технічного університету «ХПІ»;
ORCID: https://orcid.org/0000-0003-4472-9234;
Вячеслав Вадимович ДАВИДОВ,
докторант Національного технічного університету «ХПІ»;
Денис Геннадійович ВОЛОШИН,
аспірант Національного технічного університету «ХПІ»

ПРО ЗАВДАННЯ ПОЗИЦІОНУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УМОВАХ КІБЕРАТАК

Останнім часом в силових структурах держави для вирішення різного роду завдань (розвідка, транспортування, моніторинг та ін.) Все частіше використовують безпілотні літальні апарати (БПЛА). Пов'язано це багато в чому з їх все більш зростаючими технічними

можливостями, ефективністю і низькою вартістю їх використання. Сучасні БПЛА можна класифікувати по широкому спектру робочих характеристик. Це вага, вантажопідйомність, дальність, швидкість і навантаження на крило та ін.

Спрощена класифікація БПЛА представлена в табл. 1.

Таблиця 1

Класифікація БПЛА (Клас БПЛА)

Клас БПЛА	Маса, кг	Висота польоту, км	Час польоту, годин
ТЯЖКИ	над 1.000	до 20	24 та більш
СЕРЕДНІ	до 1.000	до 9 – 10	10 – 12
ЛЕГКІ	до 50	до 3 – 5	3 – 8
НАДЛЕГКІ	до 10	до 1	около 1

Проведені дослідження [1-6] показали, що для вирішення широкого кола завдань найбільш ефективно використовувати «Легкі» і «Надлегкі» БПЛА. У той же час основною проблемою таких БПЛА є їх мала захищеність від засобів РЕБ. Як правило, військові моделі БПЛА мають захищені канали зв'язку, дискредитації яких представляється порівняно складним завданням. Тому дуже часто під удар таких БПЛА потрапляють їхні засоби навігації (GPS, ГЛОНАСС і т.і.). Наприклад, така кібератака як підміна справжніх координат апарату на помилкові, дозволяє збити БПЛА з призначеного курсу, а іноді і посадити в заздалегідь заданому місці.

Існує кілька варіантів розв'язання проблеми. Наприклад, у БПЛА які літають вище 9-10 км перехоплення сигналу з супутників навігації ставати досить важким завданням, тому що крім того, що треба мати дрон здатний літати вище, потрібно зуміти направити його точно над апаратом жертви і супроводжувати його протягом всього перехоплення, до того ж військові канали GPS мають засоби захисту, для подолання якого так само необхідні тимчасові і обчислювальні ресурси, всі ці фактори роблять перехоплення такого роду неприйнятним по ефективності і ресурсовитратності. Однак БПЛА здатні літати вище 10 км мають велику вартість, їм необхідна злітно-посадкова смуга і отримання інформації з великої висоти буде негативно позначатися на якості одержуваних даних.

Другий спосіб – це відмова від систем супутникової навігації. Більшість БПЛА мають штатні засоби об'єктивного контролю – відео- та фотофіксація, а також бортові інерціальні системи навігації (гіроскоп, акселерометр, барометр і т.п.) на основі даних з фотоапаратури орієнтується на місцевості.

В основі третього підходу лежить інерціальна система позиціонування дрона, яка з певною точність виводить апарату на заданий курс і після виконання поставленого завдання, повертає його в задану область розміром кілька десятків кілометрів, де вже локальна система позиціонування у вигляді спеціальних радіомаяків направить

БПЛА на відповідне місце посадки. Недоліком цього методу в умовах сучасних умовах обмеженого простору ведення бойових дій є можливість перехоплення або глушіння сигналу локальної системи позиціонування, враховуючи її малу потужність в польових умовах і близько прихильність до умовному противнику (а саме на малих відстанях і використовуються БПЛА останніх двох типів).

Для створення методу позбавленого більшості перерахованих вище недоліків пропонується використовувати інерційну систему позиціонування з використанням додаткових датчиків і спеціального математичного блоку, який за рахунок використання елементів штучного інтелекту буде знижувати похибка позиціонування.

Висновок. Єдиним на сьогодні надійним рішенням для збереження БПЛА в умовах протидії сучасних засобів РЕБ є установка на його борт безплатформеної інерціальної навігаційної системи (БІНС) в комплексі зі спеціальними пристроями, які розпізнають втручання в управління апаратом і переводять його повністю в автономному режимі. В цьому випадку навігація здійснюється за рахунок координат, які видаються БІНС, і апарат продовжує виконувати заздалегідь запрограмоване завдання, наприклад, політ по певних точках для ведення розвідки місцевості.

Список бібліографічних посилань

1. Arjomandi M. Classification of unmanned aerial vehicles // Techn. overview. The Univ. of Adelaide, Australia. 2011.

2. Теодорович Н. Н., Строганова С. М., Абрамов П. С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами. *Интернет-журнал «НАУКОВЕДЕНИЕ»*. 2017. № 1. Том 9. URL: http://naukovedenie.ru/PDF/13TVN117.pdf (дата звернення: 02.11.2018).

3. Радиоэлектронная борьба. От экспериментов прошлого до решающего фронта будущего. / Под ред. Н. А. Колесова, И. Г. Насенкова. М. : Центр анализа стратегий и технологий, 2015. 248 с.

4. Дмитрий Ю. Радиоэлектронный нож для беспилотника: как взломать и перехватить БПЛА // Интернет журнал «Звезда». URL: https://tvzvezda.ru/news/vstrane_i_mire/content/201609120753-8de1.htm (дата звернення: 02.11.2018).

5. Веремеенко К. К., Желтов С. Ю., Ким Н. В., Себряков Г. Г., Красильщиков М. Н. Современные информационные технологии в задачах навигации и наведения беспилотных маневренных летательных аппаратах. М. : ФИЗМАТЛИТ, 2009. 266 с.

6. Инерциальная навигационная система для БПЛА // Авиация… 17.01.2017. URL: https://aviation21.ru/inercialnaya-navigacionnaya-sistema-dlya-bpla/ (дата звернення: 02.11.2018).

Одержано 02.11.2018