Юхновський Д.С., магістрант,
Співак В.М., к.т.н., доцент,
Національний Технічний Університет України
«Київський Політехнічний Інститут»

ДОСЛІДЖЕННЯ БЕЗПЕКИ КАНАЛУ ЗВ'ЯЗКУ З НЕВІЙСЬКОВИМ БЕЗПІЛОТНИМ АПАРАТОМ

Під системою інформаційної безпеки будемо розуміти організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист каналу зв'язку [1].

Розуміючи інформаційну безпеку безпілотного апарату як стан, за якого контроль над апаратом може бути здійснений у повній мірі лише з пульту керування, правомірно визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації та мети, а також інші умови і дії, що порушують безпеку. При цьому, природно, слід розглядати і заходи захисту інформації від неправомірних дій, що призводять до нанесення збитку [2].

Види загроз інформаційної безпеки:

- За характером порушення: порушення конфіденційних даних, порушення працездатності системи, незаконне втручання в функціонування системи;
- За тяжкістю порушення: незначні помилки, дрібне хуліганство, серйозний злочин;
- По передбаченню наслідків порушників: умисне, неумисне;
- За мотивацією: зловмисне, незловмисне;
- За закінченістю: реалізовані, нереалізовані;
- За каналом проникнення: через слабкість ПО, через слабкість системи авторизації;
- За розміром збитку: незначні, значні, критичні;
- За видом реалізації загрози: перехоплення контролю, позбавлення контролю.

Сучасні системи каналів захисту зв'язку базуються на використанні методів та протоколів захисту, розглянуті далі [3].

WEP (Wired Equivalence Privacy) – це протокол шифрування, що базується на алгоритмі RC4. Алгоритм використовує ключі довжиною 64, 128, 256 та 512 біт. Чим більше біт використовується для зберігання ключа, тим більше можливих комбінацій ключів, а відповідно більша стійкість мережі до злому.

WPA (Wi–Fi Protected Access) – протокол, в основі якого покладено підмножину стандарту IEEE 802.11i. В WPA використовується декілька засобів й алгоритмів для вдосконалення методів керування ключем та шифрування. Ключ шифрування в бездротових точках доступу змінюється раз на 1-2 години.

У стандарті WPA передбачено використання захисних протоколів 802.1x, EAS, TKIP і RADIUS. Конфіденційність та цільність даних забезпечуються за допомогою протоколу TKIP (Temporal Key Integrity Protocol), який на відміну від протоколу WEP використовує інший механізм генерації ключів, щоправда він теж заснований на алгоритмі RC4. Якщо в WEP довжина вектору ініціалізації дорівнює 24 бітам, то в протоколі TKIP використовується 48 біт.

WPA2-шифрування – це система шифрування, заснована на остаточній редакції стандарту IEEE 802.11i. Алгоритм шифрування побудовано на блочному шифрі стандарту AES (Advanced Encryption Standard). Захисний протокол, що його використовує, отримав назву Counter-Mode CBC MAC Protocol (CCMP). *802.1X* – це стандарт безпеки, що включає декілька протоколів. Почнемо з протоколу EAP (Extensible Authentication Protocol). Протокол розширеної ідентифікації.

Протокол *RADIUS (Remote Authentication Dial-In User Server)*. Широко використовується в багатьох мережах. Його можна визначити як протокол безпеки, в якому для ідентифікації віддалених користувачів використовується модель клієнт-сервер. Він реалізується у вигляді серії запитів та відповідей, які клієнт передає від сервера доступу до мережі (Network Access Server - NAS) кінцевому користувачу.

Отже розглянувши усі доступні на сьогоднішній день методи захисту, можна виділити головні протоколи захисту, що реалізують ці методи: WEP, WPA, WPA2, 802.1X. Який саме метод вибрати залежить від мети, яку переслідує користувач, та від існуючого обладнання. Наприклад, протоколи захисту WPA2 та 802.1X – реалізують більш нові методи захисту, вони потребують потужного обладнання для криптографічних обчислень. Якщо пристрої системи спроможні підтримувати ці методи, то краще вибрати саме їх. Якщо ні, то можна зупинити свій вибір на WPA, якщо і цей стандарт обладнанням не підтримується, то слід використовувати WEP.

Оскільки більшість сучасних дронів виготовлені після 2007 року, то вони з високою вірогідністю мають підтримку протоколів захисту WPA2 та 802.1X.