ЦУРКО Юрій Володимирович
РАХІМОВ Володимир Володимирович

Національний університет оборони України імені Івана Черняховського, Київ, Україна

КІБЕРЗАГРОЗИ ФУНКЦІОНУВАННЮ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ БЕЗПІЛОТНОЇ АВІАЦІЇ

Виклад основного матеріалу дослідження

В даний момент інформаційно-телекомунікаційних систем безпілотної авіації надає всі послуги для обміну інформацією в внутрішній мережі. Проте особливості побудови ІТС безпілотної авіації відкриває для противника.

Питання кібернетичних загроз та кібернетичного захисту гостро стоїть в інформаційно-телекомунікаційних системах безпілотної авіації, з причини того, що управління безпілотною авіацією наразі майже неосвітлене.

Для дослідження кібернетичних загроз в інформаційно-телекомунікаційних системах безпілотної авіації визначимось з сегментом захисту [1, 2]. Типовим сегментом в інформаційно-телекомунікаційних системах безпілотної авіації будемо вважати ВЗ, з типовими підключеннями та об'єктами захисту. Загальна схема топології ВЗ складається з таких елементів:

1. Кореневий маршрутизатор, маршрутизатор для підключення мережевого обладнання та абонентів ІТС ЗС України.
2. Сервери: WEB (для забезпечення функціонування інформаційних ресурсів), стану зв'язку (для моніторингу стану зв'язку на ВЗ), DHCP (для динамічного виділення IP адрес), VPN (для побудови VPN тунелів), MAIL (для забезпечення функцій обміну поштовими повідомленнями в мережах ІТС ЗС України), DNS1 (сервер для забезпечення проходження запитів за відповідними протоколами), DNS2 (резервний сервер), Proxy (сервер для виконання непрямих запитів до мережевих сервісів).
3. Абоненти підключені до ІТС ЗС України в межах відповідальності даного ВЗ

Засобами захисту будемо вважати:

1. Міжмережевий екран (Firewall) – пристрій або набір пристроїв, налаштований, щоб допускати, відмовляти, шифрувати, пропускати через проксі весь комп'ютерний трафік між областями різної безпеки згідно з набором правил та інших критеріїв.
2. Політики безпеки на серверах та маршрутизаторах.
3. Комплекси для моніторингу стану кібернетичної безпеки (сервери та агенти моніторингу).
4. Адміністратори з кібернетичної безпеки на ВЗ, позаштатну службу захисту інформації та кібернетичної безпеки у військовій частині.

В рамках загальної комп'ютеризації ЗС України та переходу від аналогового зв'язку до цифрового, все більшої уваги потребує кіберпростір, який тою чи іншою мірою створених інформаційно-телекомунікаційних система безпілотної авіації.

На сьогоднішній день провідні армії світу та суспільство в цілому все більшою мірою покладаються і, відповідно, залежать від безперешкодного функціонування п'ятого простору – кіберпростору, під яким пропонується розглядати сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз та банків даних, що обробляються в комп'ютерних мережах і пов'язаній з ними інфраструктурі, разом з об'єктами, що підпадають під їх контроль та управління [3, 4].

Контроль та управління безпілотною авіацією більшою мірою досягається за допомогою ІТС. За умов гібридної війни ІТС безпілотної авіації стали предметом посиленого кібернетичного впливу. Розглянемо основні види кібернетичних загроз, які можуть вплинути на функціонування ІТС безпілотної авіації.

За умов загальної класифікації кібернетичних загроз, способами реалізації атак, та проведення кібернетичного впливу на ІТС безпілотної авіації можна виділити такі атаки та спроби реалізації їх:

1. Атаки підготовчих періодів (дії зловмисників, які передують масштабним атакам, або викраденням інформації);
2. Високотехнологічні атаки (які потребують навичок, довготривалої підготовки та великих обчислювальних потужностей);
3. Вірусні спроби виконання атак (ШПЗ є не менш технологічними, проте їх реалізація розрахована насамперед на "допомогу" користувача);
4. Соціальна інженерія (як прояв збору, викрадення потрібної зловмисникам інформації методами, які опираються на психологію та дослідження поведінки людей).

Дослідивши наявні кібернетичні загрози, в рамках роботи пропоную розглянути кібернетичні загрози для сегменту ІТС безпілотної авіації з алгоритмом їх впровадження та першопричинами, які спонукають зловмисників до їх реалізації [5].

Яскравим прикладом для впровадження атак на ІТС безпілотної авіації є використання вразливостей телекомунікаційного обладнання, яке встановлене на типових ВЗ.

Розглянемо, "нервові нитки" безпілотної авіації – телефонний зв'язок. Технічний прогрес та

простота у використанні, зумовила перехід до використання цифрового телефонного зв'язку. В рамках цієї роботи мова піде про відкритий телефонний зв'язок. Хоча він і вважається відкритим проте деструктивного впливу на ІТС безпілотної авіації може нанести великого.

Сервер зазвичай по протоколу SIP з використанням SIP серверу з відкритим програмним кодом Asterisk. Регіональний сервер є зменшеною копією головного серверу телефонії. Обладнання (шлюзи та IP-телефони) не є типізованим та окрім бекдорів та власних вразливостей може мати ряд набутих вразливостей, під час налаштування його адміністратором [6].

В ході проведення дослідження було встановлено, що основними типами кібернетичних загроз ІТС безпілотної авіації є: атаки підготовчих періодів, високотехнологічні атаки, вірусні атаки (ШПЗ) та соціальна інженерія. Також було проведено аналіз наявних кібернетичних загроз та вразливостей на сегмент ІТС безпілотної авіації, зокрема вразливості телекомунікаційних систем, атаки типу інсайдерства, використання даних якими обмінюються в глобальній мережі інтернет, а також дослідили проблему підключення сторонніх пристроїв. В розрізі дослідження були проаналізовані можливі сценарії проведення кібернетичного впливу на ІТС безпілотної авіації з можливістю використання виявлених загроз.

Висновок

Таким чином, провівши дослідження можна зробити висновки, що ІТС безпілотної авіації мають ряд вразливостей, використання яких може призвести до втрати важливої інформації, деструктивного впливу на систему зв'язку ЗС України, компрометації інформації, яка циркулює в ІТС безпілотної авіації та деструктивному впливу на систему управління.

Список використаних джерел

1. Ларина Е. Овчинский В. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М.: Книжный мир. 2014 – 352 с.

2. Маккарти Л. IT-безопасность: стоит ли рисковать корпорацией. – М.: КУДИЦ-ОБРАЗ. 2004. – 208 с.

3. Ричард Кларк, Роберт Нейк Третья мировая война. Какой она будет. СПб.: Питер. 2014 – 142 с.

4. Руссинович М., Маргозис А. Утилиты Sysinternals. Справочник администратора. – СПб.: БХВ-Петербург. 2012.

5. Стивен Норкатт и др. Защита сетевого периметра. – К.: издательство DiaSoft. 2004.

6. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ИД "Форум". 2008.