вання мобільних додатків. *Передові наукові розробки – 2020:* Матеріали XVI Міжн. наук.-практ. конференції (Чехія, Прага, 22 серпня 2020 р.). Прага: Видавничий Дім "Education and Science", 2020. Volume 5. 68 с. С. 60–62.

2. Ходаков В.Є., Кругла Н.А., Веселовська Г.В., Кучмійчук М.М. Аналіз семантичної складової інформаційних технологій комп'ютеризованого навчання проектуванню мобільних додатків. *Передові наукові розробки – 2020:* Матеріали XVI Міжн. наук.-практ. конференції (Чехія, Прага, 22 серпня 2020 р.). Прага: Видавничий Дім "Education and Science", 2020. Volume 5. 68 с. С. 63–65.

DOI https://doi.org/10.30525/978-9934-588-79-2-1.23

МЕТОДИКА ОЦІНЮВАННЯ РІВНЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ МЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Чевардін В. Є.
доктор технічних наук, старший науковий співробітник,
начальник кафедри захисту інформації та кіберзахисту
Військового інституту телекомунікацій та інформатизації
імені Героїв Крут

Мазулевський О. Є.
кандидат технічних наук,
доцент кафедри захисту інформації та кіберзахисту
Військового інституту телекомунікацій та інформатизації
імені Героїв Крут

Сова О. Я.
доктор технічних наук, старший науковий співробітник,
начальник кафедри автоматизованих систем управління
Військового інституту телекомунікацій та інформатизації
імені Героїв Крут
м. Київ, Україна

Вступ. Досвід операцій (бойових дій) останніх років свідчить про зростаючу роль інформаційно-телекомунікаційних систем (ІТС) спеціального призначення у досягненні мети операції (бойових дій).

Специфічність ІТС спеціального призначення полягає в тому, що з однієї сторони вони вирішують завдання передачі та обробки інфор-

мації, а з іншої вони повинні відповідати вимогам з живучості при впливі на них противника.

З метою здійснення дезорганізації управління та досягнення інформації переваги противником широко застосовуються засоби радіоелектронної боротьби та кібернетичного впливу на ІТС спеціального призначення [1-5].

З огляду на це, кібератаки на ІТС стали реальною загрозою і є однією з пріоритетних проблем національної безпеки та управління ризиками.

Кібербезпека охоплює всі заходи безпеки, які можуть бути вжиті для захисту від цих нападів. Значне зростання складності та інтенсивності кібератак в останні роки змусило більшість розвинених країн посилити свій захист і прийняти національні стратегії кібербезпеки. Тому актуальною є проблема забезпечення захисту кіберпростору в світі.

З метою вироблення заходів протидії кібернетичним впливам на ІТС спеціального призначення авторами пропонується провести розробку методики оцінювання кібербезпеки в ІТС спеціального призначення.

Саме тому метою зазначеної доповіді слід вважати методику оцінювання кібербезпеки в інформаційно-телекомунікаційній системі спеціального призначення.

Виклад основного матеріалу дослідження

Методика оцінювання кібербезпеки в ІТС спеціального призначення складається з наступних основних етапів:

1. Введення вихідних даних. На даному етапі вводиться оперативна обстановка та наявні дані про можливості кібернетичного впливу на ІТС спеціального призначення.

2. Аналіз кіберзагроз. В ході виконання зазначеної процедури виконуються наступні дії: 1) встановлення контексту ІТС; 2) проведення аудиту безпеки в ІТС, що включає в себе: анкетування; виявлення кіберзагроз в активах ІТС; оцінювання активів ІТС; виявлення загроз; виявлення типових векторів атак та формування концептів сценарію.

Аналіз кіберзагроз в методиці здійснюється за допомогою порівняння виявлених кіберзагроз з кіберзагрозами, які наявні в базі знань. Також на даному етапі формується перелік критичних активів та виявлених вразливостей, що відповідають кібезагрозі, а також типові вектори атак, що представляють собою ланчюжок вразливостей, загроз та цільових активів .

На основі отриманого результату формуються концепти та зв’язки між ними для подальшої побудови сценаріїв.

3. Формування сценаріїв екстремальних ситуацій в ІТС, що викликані реалізацією кіберзагроз.

Зазначена процедура заснована на системному аналізі та дослідженнях інформаційної безпеки. В якості інструменту сценарного аналізу впливу кібезагроз на виникнення екстремальних ситуацій в ІТС спеціального призначення пропонується використовувати нейронечіткі моделі.

4. Оцінювання ризиків порушення кібербезпеки в ІТС.

Зазначена процедура направлена на виявлення ризиків, їх якісне та кількісне оцінювання, а також ранжування розглянутих об'єктів по встановленим критеріям, в якості яких можуть виступати величини як інтегрального показника ризиків по об'єкту, так і показники окремих типів ризиків.

Зазначена процедура містить рекомендації по опису ризику, якісному та кількісному оцінюванню, вибору шкал оцінювання та ранжуванню енергетичних об'єкту. Процедура оцінювання ризиків порушення кібербезпеки в інформаційно-телекомунікаційних системах включає 3 основні етапи: опис ризиків; якісне та/або кількісне оцінювання ризиків; ранжування об'єктів.

5. Ранжування об'єктів в ІТС.

В рамках зазначеної технології ранжування об'єктів відбувається у відповідності до величини ризиків, що можуть бути нанесені кібернетичним впливом, інформація про які закладена в базі даних про зовнішні та внутрішні загрози або фактори.

Висновки

1. Сьогодні головною темою обговорення у світі має стати зміцнення кібербезпеки та скорочення кількості кібератак в кіберпросторі.

Дана проблема потребує якнайшвидшого вирішення, оскільки створені зразки кіберзброї вирізняються глобальною досяжністю, практично миттєвим впливом без будь-якого способу отримання попередження про її застосування.

Кіберзахист – це єдине, що може запобігти втратам інформації та втручанню одних країн в безпеку інших.

2. В ході проведеного авторами дослідження авторами було проведено розробку методики оцінювання кібербезпеки в інформаційно-телекомунікаційній системі спеціального призначення.

Відмінність запропонованої методики від відомих, що визначає її новизну полягає у можливості:

– виявленні та якісної інтерпретації кіберзагроз;

– моделюванні сценаріїв екстремальних ситуацій, викликаних реалізацією кіберзагроз;

– оцінюванні ризиків, що мають ознаки декількох классів і ранжування активів інформаційно-телекомунікаційної системи за ступенем їх критичності;

– виконати оцінку кількості критично вразливих активів інформаційно-телекомунікаційної системи;

– обґрунтувати склад і ймовірність реалізації кіберзагроз, здатних викликати екстремальні ситуації в інформаційно-телекомунікацій системі;

– проведення оцінювання ризиків від їх реалізації в інформаційно-телекомунікацій системі.

3. Застосування запропонованої методики дозволяє автоматизувати процес аналізу кіберзагроз та оцінки ризиків порушення кібербезпеки інформаційно-телекомунікацій системі.

Напрямками подальших досліджень слід вважати розробку методики підвищення кібернетичної захищеності інформаційно-телекомунікаційної системи.

Література:

1. Шишацький А. В., Башкиров О. М., Костина О. М. Розвиток інтегрованих систем зв'язку та передачі даних для потреб Збройних Сил. Озброєння та військова техніка: науково-технічний журнал. Київ, ЦНДІ ОВТ ЗС України, 2015. № 1(5). С. 35–40.

2. Міщенко А. О., Шишацький А. В., Бондаренко Т. В., Бігун Н. В., Ляшенко Г. Т. Аналіз використання сучасних технологій радіозв'язку у збройних силах провідних країн світу. *Системи обробки інформації*. 2019. № 4(159). С. 50-57. https://doi.org/10.30748/ soi.2019.159.06.

3. Сальник С. В., Сальник В. В., Сова О. Я., Стемпковська Я. А. Модель вторгнень в мобільні радіомережі класу MANET. Збірник наукових праць Харківського національного університету Повітряних Сил. 2016. № 1(46). С. 79-84.

4. Romanenko, I.O., Shyshatskyi, A.V., Zhyvotovskyi, R.M. and Petruk, S.M. (2017), The concept of the organization of interaction of elements of military radio communication systems, Science and Technology of the Air Force of Ukraine, No. 1(26), pp. 97–100. https://doi.org/10.30748/nitps.2017.26.20.

5. Сальник С. В., Сальник В. В., Симоненко О. А., Сова О. Я. Метод виявлення вторгнень в мобільні радіомережі на основі нейронних

мереж. Наука і техніка Повітряних Сил Збройних Сил України. 2015. № 4(21). С. 82–90.

6. Симоненко О. А., Ошурко В. М., Міночкін Д. А., Сова О. Я. Загрози безпечній передачі інформації в мобільних радіомережах класу MANET та методи їх усунення. Наука і техніка Повітряних Сил Збройних Сил України. 2015. № 1(18). С. 109–113.