DOI 10.33099/2786-7714-2023-1-4-27-31
УДК 623.486

Ясинецький Василь Павлович **(кандидат військових наук, доцент)**
https://orcid.org/0009-0005-6274-0738
Хажанець Юрій Анатолійович **(доктор філософії)**
https://orcid.org/0000-0002-8926-2474
Павлюченко Володимир Олексійович

Національний університет оборони України, Київ, Україна

АНАЛІЗ ФАКТОРІВ ТА ЗАГРОЗ, ЩО ВПЛИВАЮТЬ НА КІБЕРЗАХИЩЕНІСТЬ СИСТЕМИ ЗВ'ЯЗКУ, РАДІОТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ ТА АВТОМАТИЗАЦІЇ УПРАВЛІННЯ ПОВІТРЯНОГО КОМАНДУВАННЯ В ОБОРОННІЙ ОПЕРАЦІЇ

У статті проведено аналіз факторів та загроз, що впливають на кіберзахищеність системи зв'язку, радіотехнічного забезпечення та автоматизації управління повітряного командування в оборонній операції. Також в статті було описано види кібератак та визначено чинники, що можуть збільшувати ризики кібератак на систему зв'язку, радіотехнічного забезпечення та автоматизації управління (далі - СЗ, РТЗ та АУ) повітряного командування в оборонній операції. В процесі дослідження було проаналізовано потенційні небезпеки, які можуть стати причиною кібератак або інших подій, які негативно вплинуть на функціонування СЗ, РТЗ та АУ і встановлено, що основними факторами, що впливають на кіберзахищеність СЗ, РТЗ та АУ є людський фактор, вразливості програмного забезпечення та недостатнє забезпечення захисту та контролю за СЗ, РТЗ та АУ. Результати проведеного аналізу можуть бути використані для подальших досліджень з розробки пропозицій та заходів щодо кіберзахисту СЗ,РТЗ та АУ повітряного командування в оборонній операції.

Ключові слова: *систему зв'язку, радіотехнічного забезпечення та автоматизації управління, кіберзахист, кібератаки, кіберпростір, оборонна операція.*

Вступ

У сучасних умовах повномасштабного вторгнення російської федерації на територію України військова сфера стала об'єктом постійних кібератак зі сторони російської федерації, що створює загрозу для національної безпеки та обороноздатності нашої держави.

Система зв'язку, радіотехнічного забезпечення та автоматизації управління є невід'ємною складовою системи управління повітряного командування і будь-який зовнішній чи внутрішній дестабілізуючий вплив на неї може загрожувати втратою управління зі значними негативними наслідками. Інформаційні технології глибоко проникли в СЗ, РТЗ та АУ та разом зі зручністю, функціональністю та швидкістю передавання даних ця система отримала і ризики кібернетичних загроз. Кібератаки можуть негативно впливати на ефективність функціонування СЗ, РТЗ та АУ і створювати вкрай небезпечні ситуації, наприклад, кібератака на сервери де обробляється розвідувальна інформація про повітряну обстановку може призвести до втратити чи значного погіршення контролю за повітряним простором та мати катастрофічні наслідки для всієї оборонної операції. Тому дослідження кіберзахисту є вкрай важливим питанням сьогодення для систем зв'язку та інформаційних систем Збройних Сил України загалом і для СЗ, РТЗ та АУ повітряного командування зокрема.

Мета цієї статті полягає в проведенні аналізу факторів та загроз, що впливають на кібербезпеку СЗ, РТЗ та АУ повітряного командування, що дозволить в подальшому розробити пропозиції та рекомендації щодо забезпечення її кіберзахисту.

Матеріали та методи

У даному дослідженні застосовуються наукові методи системного аналізу та синтезу.

Результати

Фактично напередодні широкомасштабного вторгнення російської федерації на територію України було здійснено кібератаку на систему супутникового зв'язку, внаслідок якої значна кількість рухомих підрозділів, де супутниковий зв'язок був основним видом зв'язку і давав змогу повноцінно управляти цими підрозділами було порушено, використовувати КХ та УКХ радіозв'язок було вкрай небезпечно, а в деяких випадках неможливо у зв'язку з роботою засобів РЕБ противника. Таким чином функціонування системи зв'язку, РТЗ та АУ було частково порушено, що мало певні негативні наслідки.

Провівши аналіз кібератак російської федерації на військові об'єкти та об'єкти критичної інфраструктури протягом останніх 5 років можна їх класифікувати за різними чинниками:

За типом атакуючої програми:

Віруси: це програми, які можуть розповсюджуватися через мережу і вбудовуватися в інші програми. Віруси можуть запускатися після

певної дати або події та завдавати шкоди системам або важливим даним.

Черв'яки: це програми, які розповсюджуються через мережу, не вбудовуючись в інші програми. Черв'яки можуть використовувати вразливості систем для розповсюдження та завдавати шкоди системам або важливим даним.

Троянські коні: це програми, які видають себе за корисні програми, але насправді містять шкідливий код. Троянські коні можуть дозволяти злочинцям отримувати доступ до системи та важливих даних.

Шпигунські програми: це програми, які призначені для збору конфіденційної інформації з комп'ютерів або мобільних пристроїв та передачі її злочинцям.

Рекламні програми: це програми, які показують небажану рекламу та можуть завантажувати додатковий шкідливий код на комп'ютер або мобільний пристрій.

Додатки-вимагачі: це програми, які блокують доступ до важливих даних на комп'ютері або мобільному пристрої та вимагають викуп для їх відновлення.

За видом атаки:

Phishing: це атака, при якій злочинець використовує підроблений веб-сайт, щоб зібрати особисту інформацію, таку як паролі та інші конфіденційні дані.

DDoS-атаки: атаки на сервер або мережу з метою перевантаження їх ресурсів, щоб заборонити користувачам використовувати їх.

Man-in-the-middle атаки: використовуються для перехоплення комунікацій між двома сторонами з метою отримання конфіденційної інформації.

Ransomware: атаки, що шифрують файли на комп'ютері жертви, що може призвести до вимоги викупу за їх розшифрування.

Мальвара (Malware): це загальний термін, який охоплює широкий спектр шкідливих програм, таких як віруси, черв'яки, троянські коні, шпигунське програмне забезпечення та інші. Мальвара встановлюється на комп'ютері без згоди користувача і може завдати шкоди, викрадаючи дані, перешкоджаючи нормальній роботі системи або використовуючи ресурси пристрою для зловмисних цілей.

Соціальна інженерія: це атаки, які спираються на маніпулювання психологією та довірою людей з метою отримання конфіденційної інформації або здійснення несанкціонованого доступу. Наприклад, зловмисники можуть використовувати соціальні мережі, електронну пошту або телефонні дзвінки для підступу до особистої інформації або паролів.

Zero-day атаки: це атаки, які використовують вразливості в програмному забезпеченні, які ще не відомі розробникам або не виправлені. Зловмисники використовують ці вразливості, щоб отримати несанкціонований доступ до системи або мережі.

Атаки "зненацька" (Drive-by Downloads): це атаки, коли користувачі самостійно завантажують шкідливий код або мальвару, відвідуючи підозрілі веб-сайти або взаємодіючи зі шкідливими рекламними банерами. Це може призвести до встановлення шкідливого програмного забезпечення на їхні комп'ютери або пристрої.

Атаки на вбудовані системи (IoT): зловмисники можуть націлюватися на вразливості в підключених до Інтернету речах (IoT) пристроях, таких як розумні телевізори, домашні роутери, веб-камери тощо. Це може призвести до викрадення особистих даних, злому домашньої мережі або використання пристроїв у ботнетах для злочинних цілей.

Атаки на віддалені робочі місця (Remote Desktop Attacks): зловмисники можуть спробувати зламати системи віддаленого доступу, які використовуються для підключення до робочих місць із-за меж корпоративної мережі. Це може дозволити їм отримати доступ до цінної корпоративної інформації або поширити шкідливе програмне забезпечення всередині мережі.

Проте кіберзлочинці постійно розробляють нові методи атак і використовують різні комбінації технік для досягнення своїх цілей.

За об'єктом атаки:

Комп'ютери та сервери: атаки на комп'ютери та сервери мають на меті отримання доступу до конфіденційної інформації, перехоплення контролю над системою або завдання шкоди.

Мережі: атаки на мережі можуть включати в себе проникнення шкідливого програмного забезпечення, перехоплення мережевого трафіку та викрадення конфіденційної інформації.

Мобільні пристрої: атаки на мобільні пристрої, такі як смартфони та планшети, можуть включати в себе викрадення особистої інформації, установку шкідливих додатків або перехоплення комунікації.

Критична інфраструктура: атаки на критичну інфраструктуру, таку як електроенергетичні мережі та транспортні системи, можуть викликати серйозну шкоду та вплинути на безпеку та здоров'я громадян.

Інтернет-сервіси: атаки на інтернет-сервіси, такі як соціальні мережі та онлайн-магазини, можуть включати в себе викрадення даних користувачів, крадіжку грошей та переривання роботи сервісів.

Люди: атаки на людей можуть включати в себе соціальний інжиніринг та фішинг, які намагаються переконати людей розкрити свої конфіденційні дані або виконати дії, які можуть завдати шкоди.

Ці атаки можуть бути як внутрішніми, які виконуються з внутрішньої сторони системи, зазвичай посадовими особами або іншими особами, які мають дозвіл на доступ до комп'ютерних систем та мереж. Внутрішні кібератаки можуть бути призначені для отримання конфіденційної інформації, внесення змін до даних або завдання шкоди системі, тобто проводитися залежно від рівня доступу користувача в системі, так і зовнішніми, які виконуються ззовні системи. Їх здійснюють зловмисники або хакери, які намагаються проникнути до системи, щоб отримати конфіденційну інформацію або завдати

шкоди. Зовнішні кібератаки можуть виконуватися з використанням різноманітних технік, включаючи фішинг, соціальний інжиніринг, використання вразливостей програмного забезпечення та інших методів. Важливо розуміти, що кожен тип атаки може бути спрямований на різні об'єкти і мати різну мету. Для кожного типу атаки необхідно використовувати відповідні методи захисту і протидії.

Тож із аналізу загроз можливо зробити висновок, що вплив на СЗ, РТЗ та АУ повітряного командування може бути як внутрішній, так і зовнішній. Внутрішній вплив, як правило, виникає із-за недотримання інструкцій з кібербезпеки самими користувачами і адміністраторами системи та з причини недостатнього контролю та моніторингу за станом СЗ, РТЗ та АУ. Невиконання заходів з кібербезпеки користувачами і адміністраторами СЗ, РТЗ та АУ в ході оборонної операції може призвести до витоку інформації та до розкриття задумів командування. Тому особовий склад, що використовує та адмініструє СЗ, РТЗ та АУ повинен підлягати постійному контролю по дотриманню заходів з кібербезпеки. Не виключено можливість і навмисних диверсій із боку користувачів та адміністраторів – це особовий склад, який таємно працює на ворога або був ним завербований. Такі дії є найбільш небезпечними тому необхідно здійснювати ретельну перевірку особового складу та забезпечувати постійний контроль за їх діяльністю за допомогою обов'язкової авторизації з подальшою можливістю відслідковування діяльності як користувача, так і адміністратора.

Нижче наведено результати аналізу внутрішніх факторів, що впливають на кібербезпеку СЗ, РТЗ та АУ повітряного командування:

недбалість працівників: недбалість у використанні паролів, відкриття небезпечних електронних листів або завантаження небезпечного програмного забезпечення;

недостатня кібербезпекова культура: якщо в організації не приділяють достатньої уваги до кібербезпеки, особовий склад може не розуміти необхідність виконання заходів безпеки та надійності;

недостатня організація заходів з кібербезпеки: організації часто мають прогалини в їх кібербезпеці, наприклад, недостатньої кількості та якості бекапів, застарілої програмної архітектури та захисту;

внутрішні кібератаки: це можуть бути дії здійснені особовим складом та працівниками організацій, що надають свої послуги та мають доступ до конфіденційної інформації, систем управління комутації та каналоутворення;

недостатня охорона даних: питання щодо зберігання, передавання та обробки даних, які можуть призвести до незаконного доступу до цих даних;

системні помилки та вразливості: слабкі місця в програмному забезпеченні та інфраструктурі, які можуть бути використані для здійснення кібератак або крадіжки даних;

недостатній контроль доступу: питання з управлінням доступом до конфіденційної інформації та інфраструктури, які можуть призвести до незаконного доступу та витоку даних;

недостатній моніторинг та виявлення кібератак: якщо організація не має ефективної системи моніторингу та виявлення кібератак, то це може призвести до затримки виявлення кіберпорушень, а також до збільшення ризику витоку даних та інших наслідків;

недостатній захист мобільних пристроїв: використання мобільних пристроїв у роботі може стати джерелом кіберзагроз, якщо пристрої не захищені належним чином;

недостатній захист від соціальної інженерії: соціальна інженерія є однією з найбільш ефективних технік кібератак. Недостатнє навчання працівників та відсутність процедур для захисту від цієї загрози можуть призвести до успішної атаки;

недостатній захист мережі: захист мережі є ключовим елементом кібербезпеки, і недостатній захист мережі може призвести до втрати даних, витоку конфіденційної інформації та інших наслідків;

недостатній захист від DDoS-атак: DDoS-атаки є однією з найбільш поширених форм кібератак, і недостатній захист від них може призвести до відмови в роботі важливих систем та сервісів.

Зовнішні чинники спровоковані, як правило, кібервійськами противника, які можуть створити загрози для СЗ, РТЗ та АУ через пошук вразливих місць. Система зв'язку, радіотехнічного забезпечення та автоматизації управління є доволі розгалуженою, основою її є транспортна мережа загального та спеціального користування. Також слід звернути увагу на те, що сучасна СЗ, РТЗ та АУ через VPN тунелі поєднана з мережею Інтернет, що дозволяє ворогу здійснювати кібератаки із будь-якого місця на планеті. Тож із зовні СЗ, РТЗ та АУ може бути атакована наступним чином:

хакерські атаки: атаки на комп'ютерні системи з метою отримання неповного чи повного доступу до конфіденційної інформації;

віруси, черв'яки та троянські програми: шкідливі програми, які можуть заражати комп'ютерні системи та поширюватися мережами, що призводить до втрати даних та іншого збереженого матеріалу;

фішинг та соціальний інженерінг: ці методи залучення людей до передачі своїх конфіденційних даних та інформації можуть бути використані для здійснення кіберзлочинів;

кібершпигунство: це можуть бути спроби отримати конфіденційну інформацію про певну компанію чи державу, яка може використовуватися в наступному для шкідливих дій;

державні кібератаки: атаки можуть бути здійснені з боку інших країн, з метою збору конфіденційної інформації або завдання шкоди економіці або інфраструктурі;

ботнети: мережі комп'ютерів, що управляються хакерами, які можуть використовувати їх для здійснення атак та розсилки спаму;

кібертероризм: використання кібератак для завдання шкоди великим компаніям, державним установам чи іншим важливим об'єктам.

Обговорення

Виходячи з аналізу класифікації кіберінцидентів та факторів, які впливають на кіберзахищеність СЗ, РТЗ та АУ можна виділити два фактори, які найбільше впливають на кіберзахищеність СЗ, РТЗ та АУ, а саме:

1. Недостатня кібергігієна.

Найбільша кількість кіберінцидентів виникає саме через вплив цього фактору, який може бути викликаний багатьма причинами, такими як застаріла програмна або апаратна складова, відсутність регулярного оновлення програмного забезпечення або недостатній рівень знань та навичок у сфері кібербезпеки.

Недостатній рівень кібергігієни може серйозно підірвати кіберзахищеність СЗ, РТЗ та АУ, призвести до зламу мережі, крадіжки конфіденційної інформації, атак вірусів та інших шкідливих програм. Крім того, якщо в системи зв'язку, РТЗ та АУ виявляється вразливість, то кіберзлочинці можуть експлуатувати цю вразливість для здійснення атак на цільову систему.

Щоб підвищити кіберзахищеність СЗ, РТЗ та АУ, необхідно вживати заходів з поліпшення кібергігієни. Це може включати такі заходи, як регулярне оновлення програмного та апаратного забезпечення, навчання користувачів правильним методам збереження паролів та інших конфіденційних даних, використання шифрування даних та застосування заходів забезпечення безпеки мережі.

2. Недостатнє забезпечення захисту мережі.

Причинами є відсутність відповідних заходів безпеки, недостатня конфігурація мережі, відсутність захисту від DDoS атак, інші.

Система зв'язку, радіотехнічного забезпечення та автоматизації управління, яка не має достатнього рівня захисту від кібератак та інших кіберзагроз, які здійснюються шляхом застосування як програмних, так і апаратних методів може призвести до негативних наслідків з витоку інформації чи втрати управління. Якщо система не має достатнього захисту, то вона стає вразливою до різноманітних кібератак, які можуть призвести до крадіжки конфіденційної інформації, втрати даних, втрати грошей та інших шкідливих наслідків.

Таким чином із загального переліку факторів виділено два, які найбільше впливають на кіберзахищеність СЗ, РТЗ та АУ.

Висновки

Таким чином в роботі проведено аналіз факторів, які впливають на кіберзахищеність СЗ, РТЗ та АУ та при цьому виділено ті фактори, що найбільше впливають на кібезахищеність та мають стати передумовою для розуміння поточного рівня кібербезпеки СЗ, РТЗ та АУ і прийняття відповідних управлінських рішень щодо його підвищення.

Виходячи із зазначеного можливо сформулювати загальні принципи кібербезпеки, основні загрози та уразливості, а також роль людей, технологій та політики у забезпеченні кібербезпеки, що і буде подальшим дослідженням. Під політикою в контексті кібербезпеки мається на увазі набір правил, норм та законів, які створюються та впроваджуються для захисту кіберпростору від загроз та забезпечення безпеки користувачів.

Список використаних джерел

1. Національний інститут стандартів та технологій (NIST) США: Cybersecurity Framework. URL: https://www.nist.gov/cyberframework

2. Європейська агенція з кібербезпеки (ENISA): Good practices for Security of Internet of Things in the context of Smart Manufacturing. URL: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-in-smart-manufacturing

3. Інтернет-організація по кібербезпеці (ICSPA): Cyber Security Tips for Individuals. URL: https://www.icspa.org/cyber-security-tips-for-individuals/

4. Міжнародний союз телекомунікацій (ITU): Cybersecurity and Cybercrime. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

5. Наказ командувача Військ зв'язку та кібербезпеки Збройних Сил України від 10 лютого 2021 року № 83/накп «Про затвердження класифікації інцидентів та порушень захисту інформації в інформаційно-телекомунікаційних системах, системах спеціального зв'язку Збройних Сил України».

6. Інструкція з організації антивірусного захисту в інформаційно-телекомунікаційних системах Міністерства оборони України та Збройних Сил України. URL: https://www.mil.gov.ua/content/mou_orders/mou_2023/153_nm_2023.pdf

7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави", Указ Президента України No 446/2021 (2021) (Україна). URL: https://zakon.rada.gov.ua/laws/show/ 446/2021 #Text.

8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", Указ Президента України No 447/2021 (2021) (Україна). URL: https://zakon.rada.gov.ua/laws/show/447/2021.txt

ANALYSIS OF FACTORS AND THREATS IMPACTING THE CYBERSECURITY OF COMMUNICATION SYSTEMS, RADIO TECHNICAL SUPPORT, AND AUTOMATION OF AIR COMMAND IN OPERATIONS

Vasyl Yasinetskyi **(Candidate of Military Sciences, Associate Professor)**
https://orcid.org/0009-0005-6274-0738
Yuri Khazhanets **(Ph.D.)**
https://orcid.org/0000-0002-8926-2474
Volodymyr Pavliuchenko

The National Defence University of Ukraine, Kyiv, Ukraine

The article provides an analysis of factors and threats that influence the cybersecurity of communication systems, radio technical support, and automation of air command in defense operations. The article also describes types of cyber-attacks and identifies factors that can increase the risks of cyber-attacks on the communication systems, radio technical support, and automation (hereinafter referred to as CS, RTS, and AU) of air command in defense operations. During the research, potential hazards that can lead to cyber attacks or other events disrupting the functioning of CS, RTS, and AU were analyzed. It was determined that the main factors affecting the cybersecurity of CS, RTS, and AU are the human factor, software vulnerabilities, and insufficient protection and control measures for CS, RTS, and AU. The results of the analysis can be used for further research in developing proposals and measures for the cybersecurity of CS, RTS, and AU in air command during defense operations.

Keywords: *communication systems, radio technical support, automation, cybersecurity, cyber-attacks, cyberspace, defense operation.*

References

1. Natsionalnyi instytut standartiv ta tekhnolohii (NIST) SShA: Cybersecurity Framework. URL: https://www.nist.gov/cyberframework
2. Ievropeiska ahentsiia z kiberbezpeky (ENISA): Good practices for Security of Internet of Things in the context of Smart Manufacturing. URL: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-in-smart-manufacturing
3. Internet-orhanizatsiia po kiberbezpetsi (ICSPA): Cyber Security Tips for Individuals. URL: https://www.icspa.org/cyber-security-tips-for-individuals/
4. Mizhnarodnyi soiuz telekomunikatsii (ITU): Cybersecurity and Cybercrime. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
5. Nakaz komanduvacha Viisk zviazku ta kiberbezpeky Zbroinykh Syl Ukrainy vid 10 liutoho 2021 roku № 83/nakp «Pro zatverdzhennia klasyfikatsii intsydentiv ta porushen zakhystu informatsii v informatsiino-telekomunikatsiinykh systemakh, systemakh spetsialnoho zviazku Zbroinykh Syl Ukrainy».
6. Instruktsiia z orhanizatsii antyvirusnoho zakhystu v informatsiino-telekomunikatsiinykh systemakh Ministerstva oborony Ukrainy ta Zbroinykh Syl Ukrainy.
7. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro nevidkladni zakhody z kiberoborony derzhavy", Ukaz Prezydenta Ukrainy No 446/2021 (2021) (Ukraina). URL: https://zakon.rada.gov.ua/laws/show/446/2021 #Text.
8. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy", Ukaz Prezydenta Ukrainy No 447/2021 (2021) (Ukraina). URL: https://zakon.rada.gov.ua/laws/show/447/2021.txt