논문접수 2023.11.21 | ISSN 1738-6144 | Journal of The Korea Association of Defense Industry Studies Vol. 30, No. 3(2023)
논문확정 2023.12.18 | http://journal.kadis.or.kr/ | 한국방위산업학회지 제30권 제3호 | https://doi.org/10.52798/KADIS.2023.30.3.4

무기체계 기술보호를 위한 안티탬퍼링 시험평가 방안

Test and Evaluation of Anti-tampering for Protecting Technology of Weapon Systems

주영진*, 손창근**, 송경호***, 류연승****, 임재덕*****, 최연준******
Youngjin Joo*, Changgeun Son**, Kyungho Song***, Yeonseung Ryu****, Jaedeok Lim*****, Yeonjun Choi******

ABSTRACT

Recently, advanced weapon systems such as 3,000-ton submarines and 4.5-generation fighter jets are being localized, and exports of various weapon systems are increasing significantly. Korea's defense science and technology level was ranked 9th in the world, and arms system exports were also ranked 9th in the world in 2020. Meanwhile, cyberattacks seeking advanced weapon system technology are also increasing, increasing the need for technology protection of export weapon systems as well as technology protection of defense companies. The Defense Industry Technology Protection Act enacted in 2015 defines defense technology as defense technology that needs protection among defense science and technology and enforces the establishment of defense technology protection systems for defense companies. However, there is no system to protect the technology of the weapons system, which is increasing in exports, and there is no test evaluation field until the pre-test evaluation stage of weapons system research and development. In this paper, as a way to protect the defense technology of weapons systems, we studied the weapon system anti-tamping test evaluation process applicable to the defense weapons system research and development process. The proposed method investigated the test evaluation trend of cryptographic modules similar to the anti-tampering test evaluation, and proposed a process including the organization and role necessary for the test evaluation of anti-tampering technology after research and development by referring to security requirements and test requirements.

* 이 논문은 2023년 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임(KRIT-CT-22-051).
This work was supported by Korea Research Institute for defense Technology planning and advancement(KRIT) - Grant funded by Defense Acquisition Program Administration (DAPA) (KRIT-CT-22-051)
* 주영진, 명지대학교 보안경영공학과 박사과정
** 손창근, 명지대학교 보안경영공학과 교수
*** 송경호, 명지대학교 보안경영공학과 교수
**** 류연승, 명지대학교 보안경영공학과 교수(교신저자. E-mail: ysryu@mju.ac.kr)
***** 임재덕, 한국전자통신연구원(ETRI)
****** 최연준, 한국전자통신연구원(ETRI)

논문접수 2023.11.21 | ISSN 1738-6144 | Journal of The Korea Association of Defense Industry Studies Vol. 30, No. 3(2023)
논문확정 2023.12.18 | http://journal.kadis.or.kr/ | 한국방위산업학회지 제30권 제3호 | https://doi.org/10.52798/KADIS.2023.30.3.1

초 록

최근 3000톤급 잠수함, 4.5세대 전투기 등의 첨단 무기체계가 국산화되고 있으며 다양한 무기체계의 수출이 크게 증가하고 있다. 우리나라의 국방과학기술 수준은 세계 9위로 평가되고 무기체계 수출도 2020년 세계 9위로 평가되었다. 한편, 첨단 무기체계 기술을 노리는 사이버 공격도 증가하고 있어 방산업체의 기술보호 뿐만 아니라 수출용 무기체계의 기술 보호도 필요성이 증가하고 있다. 2015년 제정된 방위산업기술보호법은 국방과학기술 중에서 보호가 필요한 기술을 방산기술로 정의하고 방산업체의 방산기술보호 체계 구축을 강제화하고 있다. 그러나, 방산업체의 기술보호체계에만 초점이 맞추어져 있고, 수출이 증가하고 있는 무기체계의 기술에 대한 보호를 위한 제도가 구체적이지 못하며 관련 연구도 무기체계 연구개발의 시험평가 이전단계 까지로 시험평가분야는 전무하다. 본 논문에서는 무기체계의 방산기술 보호를 위한 방안으로 국방 무기체계 연구개발 절차에 적용할 수 있는 무기체계 안티탬퍼링 시험평가 프로세스를 연구하였다. 제안한 방법은 안티탬퍼링 시험평가와 유사한 암호모듈의 시험평가 동향을 조사하여 보안요구사항 및 시험요구사항 등을 참고하여 안티탬퍼링 기술의 연구개발 후 시험평가를 하는데 필요한 조직 및 역할과, 단계별 행동절차 등을 포함하는 프로세스를 제안하였다.

Key Words : Weapon Systems(무기체계), Anti-tampering(안티탬퍼링), Systems Engineering(체계공학), Defense Technology Protection(방산기술보호), Reverse-engineering(역설계)

Ⅰ. 서 론

우리나라는 국방과학기술의 자체 연구개발 역량을 지속적으로 강화하는 한편 선진 기술의 도입 등을 통해 기술 수준이 높아져서 일부 무기체계는 선진국 수준에 이르고 있다. 국방기술진흥연구소가 발간한 「2021 국가별 국방과학기술 수준조사서」에 따르면 국방과학기술 수준은 세계 9위로 평가되고 있다.

국방과학기술 수준의 향상과 함께 최근 우크라이나-러시아 전쟁의 영향으로 자주포, 전차, 유도무기 등 방산물자의 해외 수출이 크게 증가하고 있으며, 2017~2021년 방산수출 규모가 세계 8위로 평가되고 있다.[1] 2022년 수출 수주액이 역대 최고 수준인 170억불 규모를 달성하였고 2023년에는 200억불 규모의 수출이 예상되고 있다. 이에 정부는 국정과제에 방위산업을 "국가 미래 먹거리 신산업"으로 선정하고 2027년까지 "국방과학기술 7대 강국" 도약과 "글로벌 4대 방산수출 국가" 진입을 목표로 하는 "23-27 방위산업발전 기본계획"을 수립하였다.

이처럼 선진 수준에 이른 국방과학기술을 노리는 해외의 사이버 공격이 크게 증가하고 있다. 2021년 10월 12일 국회 국방위원회 소속 김병기 더불어민주당 의원이 방사청으로부터 제출받은 자료에 따르면, 2020년 9월부터 2021년 8월까지 주요 방산업체 13개를 대상으로 총 121만 8981건의 외부 해킹시도가 있었다. 해킹 대상은 기아와 대한항공, ㈜한화, 한화에어로스페이스, 한화시스템, 한화디펜스, 현대로템, 현대중공업, LIG넥스원, 대우조선해양, 한국항공우주산업, 한진중공업, 풍산 등 우리 주요 방산업체를 총망라하는 것으로 조사됐다.[2] 2020년 대우조선해양 핵추진 잠수함 기술, 2021년 한국항공우주산업의 KF-21 전투기 기술 등 첨단 방산기술을 노리는 사이버 해킹 사고가 발생하였다.

또한, 무기체계 수출대상국에서 역공학 등으로 국방과학기술이 손쉽게 탈취되면, 수출경쟁력을 떨어뜨릴 뿐만 아니라 자국의 방위력개선 예산 증가와 대응전력 공백의 심각한 문제를 야기할 수 있다. 또한, 전장에서 무기체계가 적에게 탈취되어 탬퍼링을 통해 무기체계에 내장된 핵심 군사기밀이 유출되는 피해가 발생할 수 있다[3].

선진국인 미국은 무기체계의 역공학을 방지하기 위해 안티탬퍼링(Anti-Tampering) 제도를 운영하고 있다. 안티탬퍼링이란 시스템의 변경 또는 시스템에 저장되어 있는 기밀 정보를 유출하려는 비인가자의 불법적 탬퍼링을 방지 또는 지연시키는 공학적 조치를 말한다. 미 국방부는 안티탬퍼링을 미국 무기체계에 내장된 핵심기술의 유출을 방지 또는 지연하기 위한 체계 공학적 활동으로 정의하고 있다.[4]

우리나라도 무기체계의 수출이 증가하고 글로벌 4대 방산수출 국가를 목표로 함에 따라 무기체계의 기술보호를 위해 안티탬퍼링의 적용이 필요하다. 이에 방위사업청은 수출용 무기체계에 대한 안티탬퍼링 적용을 의무화할 예정이며, 안티탬퍼 기술의 연구개발 사업을 진행 중이다.

안티탬퍼링은 체계공학(system engineering) 기반의 무기체계 연구개발 프로세스와 연계하여 무기체계의 수명주기동안 진행되는 것으로 선행연구들이 있었지만 연구개발절차(프로세스)에서 기술구현단계까지가 대부분이며, 개발(구현)된 기술에 대한 시험평가단계는 연구된 내용이 없어서 본 연구를 통하여 안티탬퍼링 기술이 연구개발단계에서 정상적으로 개발되었는지를 시험평가하는데 필요한 최적의 조직과 역할 및 절차등의 방법론에 관해 연구를 하였다. 본 논문의 구성은 다음과 같다. 2장에서는 국내외 관련 연구를 소개한다. 3장에서 안티탬퍼링 기술 시험평가 프로세스를 제안하고 4장에서는 논문의 결론 및 정책 제언을 기술한다.

1) 아시아경제, K-방산 수출 세계 8위, 점유율 2.8%. 2022.12.09. (https://view.asiae.co.kr/article/2022120910353794122)

2) 뉴스1, 주요 방산업체 상대 해킹시도, 최근 1년새 '121만 건', 2021. 10.12. (https://www.news1.kr/articles/?4458147)

3) 2001년 미국 해군 EP-3 정찰기가 중국 F-8 전투기와 충돌하고 하이난에 비상착륙 함에 따라 중국은 정찰기를 검토하여 다수의 핵심기술을 확보함. 2011년 미국 드론 RQ-170이 이란 지역을 정찰하다가 GPS 교란 공격으로 추락하였고 이란은 드론을 역설계하여 기술을 확보함

4) Department of Defense. (2015). *Anti-Tamper(AT).* Department of Defense, Washington, DC, Directive, DoD Directive 5200.47E

Ⅱ. 관련 연구

2.1. 안티탬퍼링 개요

안티탬퍼링은 무기체계 프로그램 보호를 위한 보호 대책 중 하나로, 무기체계에 구현된 핵심 기술인 방위산업기술의 유출을 방지하기 위한 “억제, 방지, 감지 및 반응”의 대응조치를 구현하기 위한 기술이다.[5)]

억제 기술은 핵심 부품 또는 기술이 들어있는 장치의 개봉 등에 있어 임의로 개봉하는 행위를 억제하는 것으로 스티커 마스킹 등을 통해 임의 개봉 시에 대하여 경고하는 기술 등이 사용된다. 방지 기술은 핵심 부품 또는 기술이 포함된 구성체에 대하여 탬퍼링 시도를 어렵게 만드는 것으로 특수 제작 나사의 사용, 초음파 및 레이저 용접 기술 등을 이용하는 기술 등이 있다. 감지 기술은 장치 내의 센서 등을 이용하여 압력 등의 상태 변화를 통해 탬퍼링 시도를 감지하는 기술이며, 반응 기술은 탬퍼링 시도가 감지되면 핵심 기술의 유출 방지를 위해 하드웨어 파괴 또는 소프트웨어 삭제 등을 하는 기술을 의미한다.

적용된 기술은 연구개발 및 시험평가 과정에 비인가자가 접근하지 못하도록 보안을 유지해야하며, 최소한 보안모듈 연구개발수준으로 관리되어야 한다.

2.2. 관련 시험평가 제도

안티탬퍼링 시험평가 방안을 연구하기 위하여 안티탬퍼링 시험평가와 유사한 암호모듈의 시험평가 동향을 조사하였다. 조사 대상으로 KS X ISO/IEC 19790 암호모듈의 보안요구사항 및 시험요구사항을 확인하였다.

2.2.1 KS X ISO/IEC 19790 암호모듈 보안요구사항

KS X ISO/IEC 19790 암호모듈 보안요구사항[14]에는 암호모듈의 11개 보안 영역에 대한 4개의 보안 수준(security level)이 정의되어 있다. 보안 수준의 선택은 정보의 중요성 및 응용환경 등을 고려하는 한편 비용 대비 효과를 고려하여 선택되어야 한다.

보안 수준 1의 암호모듈은 보안의 기본적인 수준을 제공한다. 적어도 한 개 이상의 검증 대상 암호 알고리즘이나 보안 함수를 포함하거나, 검증 대상 중요 보안 매개변수 설정 방법을 포함한 암호모듈에 대한 기본 보안요구사항이 명시된다.

보안 수준 2의 암호모듈은 탬퍼 증명(tamper evidence)와 같은 요구사항을 추가하였으며, 보안 수준 3의 암호모듈은 암호모듈 내부에 포함되어있는 SSP 비인가 접근을 방어하는 요구사항이 추가된다. 마지막으로 보안 수준 4의 암호모듈은 암호모듈의 가장 높은 보안 수준으로, 암호모듈 주위를 안전하게 보호하는 방법을 추가하여 향상한 것으로 이를 참고하여 안티탬퍼링도 보호수준별 요구항목에 대해 요구수준을 구체적으로 설정하여 시험평가계획과 절차서에 반영시킬 수 있겠다.

2.2.2 암호모듈 시험요구사항 및 구현안내서

암호모듈의 시험요구사항[15]에는 시험기관이 사용하는 시험방법과 벤더(vendor)가 시험기관에 제출해야 하는 정보가 명세 되어있으며, 암호모듈 구현안내서는 보안 수준에 따른 구현 기준을 제시하고 있다.

암호모듈 구현안내서는 국가정보원, 국가보안기술연구소와 한국인터넷진흥원에서 발행 및 관리되는 암호모듈 검증제도 (KCMVP) 검증기준의 보조 문서로 각 항목에 대한 배경과 질의응답을 기술해 두었는데, 시험방법과 구현기준 등은 안티탬퍼링 시험계획서 및 시험절차서 작성시 참고하여 적용할 수 있겠다.

2.2.3 암호모듈 시험 확인결과

무기체계나 적용된 안티탬퍼링기술의 시험평가 프로세스는 국방전력발전업무훈령과 합참시험평가지침서의 기준과 절차에 의해 진행되기 때문에 일반적인 시험평가 프로세스와 다를 것은 없다.

다만, 암호모듈 시험을 위한 보안요구사항이나 시험요구사항 및 구현안내서 등은 안티탬퍼링의 구현기술별 난이도에 따라 “안티탬퍼링 개발 규격서, 안티탬퍼링 시험계획/

5) United States Government Accountability Office. (2008). *Departmentwide Direction Is Needed for implementation of the Anti-Tamper Policy*. United States Government Accountability Office, Washington, DC, Report, GAO-08-91.

절차서 등" 작성시 2.2.1(암호모듈 보안요구사항)과 2.2.2(암호모듈 시험요구사항 및 구현안내서)의 내용을 참고하여 작성하면 도움이 될 것으로 평가된다.

2.3. 체계공학 기반 안티탬퍼링 프로세스

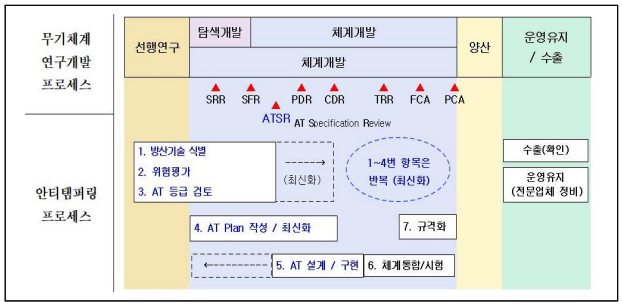
안티탬퍼링[6] 프로세스는 무기체계 획득 수명주기(lifecycle)간 체계공학 절차에 따라 진행되는 일련의 활동들로서 보호 대상인 방산기술의 식별, 위험평가, 안티탬퍼링 기법 검토 및 구현을 위한 위험관리 프로세스이다.

〈그림 1〉은 무기체계 획득 절차에 적용하는 체계공학 기반 안티탬퍼링 프로세스의 전체 개요를 간단하게 도식화하여 보여주고 있다.

무기체계 연구개발 프로세스와 연계하여 안티탬퍼링 적용 프로세스도 함께 진행한다. 사업관리기관(IPT)은 방산기술 보호의 통제기관으로 사업 착수단계부터 관리해야 한다. 소요군의 보호 요구 소요를 선행 연구단계부터 식별하며, 보안 검증기관의 지원을 받아 안티탬퍼링 보호 요구사항(대상/등급)을 명확하게 정의해서 연구개발주관기관으로 제공한다.

연구개발주관기관은 사업관리기관이 제공한 안티탬퍼링 요구사항 정의에 기초하여 안티탬퍼링 요구사항 내역을 안티탬퍼링 계획에 작성하여 ATSR[7](Anti-Tampering Specification Review)에서 보고/승인을 받는다.

ATSR 단계에서 안티탬퍼링 절차 적용을 위해 보호 요구사항(대상/등급)을 정의하여 보호 대상(기술/부품)을 식별하여 보호수준을 다음 그림과 같이 수명주기 단계에서 최신화하여 안티탬퍼링 계획에 반영하고, 주요 산출물을 최신화한다. 이후 안티탬퍼링을 개발 및 구현하여 체계에 통합 및 시험평가 후 규격화 과정을 거쳐 양산화 체계를 통합시킨다.



〈그림 1〉 체계공학 기반 안티탬퍼링 프로세스 개요 [3]

Ⅲ. 안티탬퍼링 시험평가 프로세스

3.1. 개념

무기체계에 적용되는 안티탬퍼링 기술은 체계공학(system engineering) 기반의 무기체계 연구개발 프로세스와 연계하여 무기체계의 수명주기동안 진행되는 연구개발절차(프로세스) 속에서 개발(구현)된 기술에 대한 시험평가 개념과 절차를 제시하고자 한다.

안티탬퍼링관련 모든 절차는 기술 적용에 대한 제원 노출이 되지 않도록 보안을 유지하여 제한된 조직과 인원 그리고 독립된 공간에서 독자적으로 연구 개발되고 시험평가되어야 하며, 모든 이력이 비밀에 준하여 관리되어야 한다.

따라서 안티탬퍼링 기술 개발에 대한 요구명세서, 개발규격서, 설계기술서와 시험평가를 위한 시험계획서, 시험절차서 등은 안티탬퍼링 계획 (AT plan)[8]에 부록으로 통합하여 관리하는 등의 조치가 필요하다. 무기체계 연구개발 준비단계부터 안티탬퍼링에 대한 소요를 식별하고, 연구개발 계획을 CDR까지 최신화해야 하며, 안티탬퍼링 연구개발에 관여하거나 참여하는 기관과 인원은 필수인원 위주로 최소화해야 한다. 안티탬퍼링 연구개발을 위한 장소는 독립되고 비인가자의 접근을 통제할 수 있는 장소이어야 하며, 무기체계 연구개발 PM이 안티탬퍼링 연구개발을 직접 통제해서 무기체계 연구개발과 안티탬퍼링 연구개발의 연계성이 유지되도록 조정·통제할 수 있어야 한다.

6) 안티탭퍼링(Anti-Tampering) = AT로 약칭(이하적용)

7) ATSR(Anti-Tampering Specification Review, 안티탬퍼링 요구조건 검토) : 안티탬퍼링 요구사항 정의서에 명시된 안티탬퍼링의 적용 요구소요와 추가식별된 보호대상 및 보호계획을 검토하고 결정하는 기술검토회의(신설).

8) 안티탬퍼링 계획(AT Plan) : AT의 적용기준, 적용계획 및 기술, 연구개발계획/설계서 등을 통합하여 관리하는 통합계획으로 연구결과 산출물로 제시(비밀에 준해서 관리)

3.2. 안티탬퍼링 관련 기관

무기체계의 연구개발을 위해 직·간접적으로 관련이 되어 있는 기관들은 국방과학연구소, 국방기술품질원, 방첩사령부, 시험평가기관(업체) 등 다양한 기관들과 수많은 방산업체가 관련되어있고 성공적인 연구개발을 위해 협조체계를 잘 유지하고 있다. 그런측면에서 안티탬퍼링의 성공적인 연구개발과 무기체계와의 통합을 위해서는 무기체계 연구개발 관련기관과 안티탬퍼링 연구개발 관련기관을 연관성 있게 유지하는 것이 발전적이라고 판단되어 아래 〈표 1〉과 같이 안티탬퍼링 연구개발 분야별 관련기관들의 역할을 검토하였다.

〈표 1〉에서 검토한 것과 같이 “기술 이해/검토”와 “취약성 분석”은 무기체계 연구개발과 연계해서 국방기술품질원과 방첩사령부가 사업 준비단계부터 역할 수행할 수 있고, “설계/개발/구현”과 “시험/검증”은 국방과학연구소가 개발업체를 통제하여 전담 기관으로서의 역할수행이 가능할 것으로 판단하였다.

〈표 1〉 안티탬퍼링 연구개발 관련 기관 및 역할

기관	AT 관련 역할(가능분야)			
	기술이해/검토	취약성 분석	설계/개발/구현	시험/검증
국정원	가능	가능	불가	불가
국가보안기술연구소	가능	제한	제한	가능
한국인터넷진흥원	제한	제한	불가	가능(모듈)
방첩사령부	가능	가능	불가	불가
국방보안연구소	제한	제한	불가	불가
국방과학연구소	가능	제한	가능(국방용)	가능
국방기술품질원	가능	제한	불가	가능
보안장비개발업체	가능	불가	가능	가능
방산업체	가능	불가	가능	가능

3.3. 안티탬퍼링 시험평가 조직 구성 방안

안티탬퍼링 구현 및 개발이 진행되는 동안 이루어지는 시험평가는 〈표 2〉에서와 같이, 안티탬퍼링 개발이 독자적으로 개발되는 경우 안티탬퍼링 개발규격서대로 개발되었는지를 안티탬퍼링 개발팀이 확인하는 것과 체계와 통합시험을 통해 체계개발 규격서대로 기능구현 되는지를 체계개발 부서와 확인하는 것 등으로 구분되어 진행된다. TRR이전에 실시되는 통합시험은 개발기관 자체적으로 실시되는 것으로 기존의 무기체계시혐평가에서는 시험평가로 인정되지않았지만, 계획한대로 개발되었는지와 ‘구성품, 부체계, 체계’와 정상적으로 통합되는지 AT개발/통합시험에 대해서는 통제 및 인정절차의 추가반영이 필요하다. 모든 체계의 개발이 완성되는 시점에 개발시험평가(DT&E)를 수행하게 되는데, 개발시험평가는 체계 요구 성능 및 개발목표 충족 여부를 개발시험평가 계획서 및 절차서에 근거하여 확인한다.

시험평가 조직은 무기체계가 표준 적합성 시험 대상체계일 경우 국방정보화업무훈령(180조 제3항)에 근거하여

〈표 2〉 시험평가 단계별 과업 및 확인 기준

구분	과업	확인 기준	주도기관(부서)
AT 구현(독자개발)	AT 기술 구현 확인	• AT 요구 명세서(ATRS)[9] • AT 설계기술서(ATDD)[10] • AT 개발규격서(ATDS)[11] • SW 신뢰성/보안성 시험계획	AT 개발팀
체계통합시험(통합개발 포함)	‘구성품/부체계/체계’와 통합된 AT기능 구현 확인	• ‘구성품/부체계/체계’ 개발규격서 (CIDS, PIDS, SSS) • 체계개발 규격서(SDS)	체계개발 부서
개발시험평가(DT&E)	체계 요구 성능 및 개발 목표 충족 확인	• 개발시험평가 계획서(DTEP)[12] • 개발시험평가 절차서(DTED)[13]	연구개발 기관

9) ATRS(AT Requirements Specification) : 소프트웨어 요구사항서
10) ATDD(AT Design Description) : AT설계기술서
11) ATDS(AT Design Specification) : AT개발규격서
12) DTEP(Development Test Evalution Plan) : 개발시험평가 계획서
13) DTED(Development Test Evalution Description) : 개발시험평가 절차서

표준 적합성 시험을 합동상호운용성기술센터가 해야 하며, 소요군에서는 운용시험평가(OT&E)의 계획 및 주도를 해야 하고, 이를 제외한 나머지 대부분의 시험은 일부 전문적 시험체계가 갖춰진 시설에서 해야만 하는 내용을 제외하고 기본적으로 〈표 3〉과 같이 연구개발기관이 주도적으로 실시해야 한다.

3.3.1 안티탬퍼링 구현(독자개발)단계 시험평가 조직

안티탬퍼링 구현(개발)단계의 시험평가는 안티탬퍼링 개발전담팀의 주도하에 실시해야 하며 그 구성은 개발전담팀의 개발 요소별 담당자와 협력업체, 그리고 지원기관으로 편성해야 한다. PM의 통제하에 안티탬퍼링 개발전담팀에서 개발 요소별 담당자를 지정하고 협력업체의 기술지원을 통해 시험평가를 진행한다.

담당자별 시험평가 역할을 패키징 분야를 예시로 부여한다면, 〈표 4〉와 같이 하드웨어 담당은 안티탬퍼링 개발규격서에 명시되어있는 패키징 기능구현 요소를 식별하고, 안티탬퍼링 개발규격서 및 시험계획서에 근거하여 패키징 시험절차서를 작성해야 한다, 이때 시험계획서의 항목별 조건이 충족되었는지 확인해야 한다. 소프트웨어 담당과 협력업체의 경우에는 시험계획서와 시험 절차서에 반영된 역할을 식별하고 관련 내용을 확인한 뒤, 신뢰성/보안성 시험을 시행한다. 마지막으로 안티탬퍼링 개발팀장은 시험계획서와 시험절차서의 내용을 검토 및 승인하고 시험평가의 준비상태를 점검해야 한다. 시험평가 진행간에 항목별 조건충족 여부를 확인하고 과정을 통제하여 다음 시험 항목으로 진행할 수 있도록 한다. 마지막으로 시험 종료 시 미비점을 확인하고 보완하여 시험(통제) 결과보고서를 작성해야 한다.

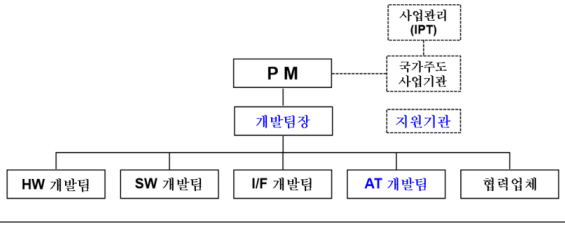
3.3.2 체계통합단계 시험평가 조직

체계통합단계의 시험평가는 구성품, 부체계, 체계 등과 통합될 때 공통으로 적용되는 것으로, 〈표 5〉와 같이 해당 체계개발팀의 주도하에 실시해야 한다. 구성품과 안티탬퍼링이 통합되어 개발될 때는 3.3.1의 안티탬퍼링 구현(개발)단계 시험평가 조직을 체계의 개발 분야별 담당팀과 협력업체, 지원기관으로 편성하고, 체계개발규격서에 따라

〈표 3〉 시험평가 단계별 담당 기관

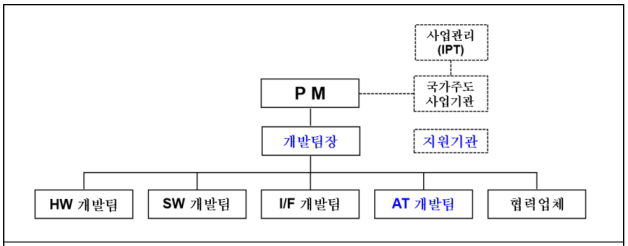
구 분	시험 주도	지원/협조	통제/검증(안)
AT 구현 (독자개발)	AT 연구개발팀	• 구성품/부체계 연구팀(I/F) • 개발 협력업체 (기술지원) • AT 통제기관(국과연, 기품원)	• PM : 시험 계획/절차 (통제) • 국가 주도 연구개발사업 시 사업관리 기관 (보고/승인) • IPT : 계획(승인), 결과(확인)
체계통합 시험 (통합개발 포함)	체계개발 부서	• AT 연구 개발팀(동참) • 부체계/체계 연구팀(동참) • 개발 협력업체(기술지원) • AT 통제기관(국과연, 기품원)	
개발시험 평가 (DT&E)	연구개발 기관	• AT 연구 개발팀(동참) • 개발 협력업체 (기술지원) • AT 통제기관(국과연, 기품원)	• 시험평가기본계획 (합참 → 국방부) • 시험평가 계획작성 (연구개발주관기관) • 시험평가 계획서 확정(합참) • 시험평가 수행 / 결과 작성(연구개발주관기관)

〈표 6〉 개발시험평가단계 시험평가 조직구성 및 역할



- 연구개발주관기관(PM) 주도하에 실시
- 개발분야별 담당팀 지정
- 협력업체 : 기술지원
- 지원기관 : 국과연, 기품원, 기타
- 통제기관 : 방사청(IPT), 국과연(국가주도사업)
- 검증 : 통제기관은 지원기관에 검증요구

〈표 5〉 체계통합단계 시험평가 조직구성 및 역할



- PM통제하에 "체계개발 전담팀"이 주도
- 개발분야별 담당팀 지정
- 협력업체 : 기술지원
- 지원기관 : 국과연, 기품원, 기타
- 통제기관 : 방사청(IPT), 국과연(국가주도사업)
- 검증 : 통제기관은 지원기관에 검증요구

시험계획서와 시험 절차서를 작성한다. 이때 안티탬퍼링 관련 항목에 대해 체계의 규격서에서 목표한 안티탬퍼링 관련 기능에 대한 시험평가가 이루어질 수 있도록 안티탬퍼링 개발팀장이 담당자별 역할을 분담하여 참여하고 안티탬퍼링 관련 시험평가 절차를 수행해야 한다.

3.3.3 개발시험평가(DT&E) 시험평가 조직

개발시험평가(DT&E)단계의 시험평가는 체계개발 목표 및 소요군의 요구사항 충족 여부 확인에 주안을 두고, 연구개발주관기관은 개발시험평가 절차서를 작성하여 사업관리기관에 보고 후 TRR 이전까지 확정해야 한다. 시험평가 조직은 체계의 개발 분야별 담당팀과 협력업체, 지원기관으로 편성하고 체계 개발규격서에 따라 시험계획서와 사업관리기관에서 승인한 시험 절차서대로 역할을 부여하고, 시행 여부를 확인 통제해야 한다.

3.4. 안티탬퍼링 시험평가 절차

안티탬퍼링 연구개발 및 시험평가도 무기체계 개발과 동일하게 국방전력발전업무훈령 (제6절 연구개발, 제8절 시험평가)에 근거하고, 체계공학 기반의 프로세스 절차를 적용하여 진행하되, 〈표 6〉과 같이 연구개발 및 시험평가에 필수적인 인원 위주로 편성하여 노출되지 않은 분리된 공간에서 실시해야 한다.

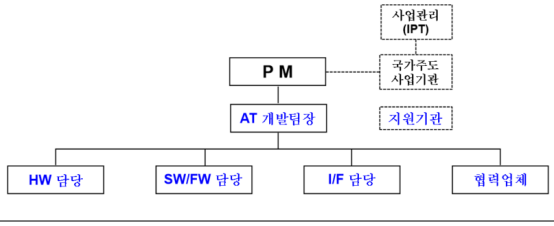
시험평가는 합참의 무기체계 시험평가 업무 지침에 근거하여 절차를 진행하며, 시험평가 기본계획서 작성 시부터 안티탬퍼링 시험평가 관련 내용을 반영하고, AT 개발 규격서에 작성한 규격대로 기능이 정상 작동하는지 AT 시험계획서를 작성해야 하며, 구체적인 시험을 위한 AT 시험 절차서를 작성하여 시험평가를 수행한다.

안티탬퍼링 관련 시험평가는 체계공학 기반의 무기체계 연구개발 절차 속에서 AT 구현단계, 무기체계 통합 단계, 개발시험평가 단계, 운용시험평가 단계를 실시하게 되지만, 운용시험평가 단계는 기술적인 요소보다는 전술적 운용에 필요한 기능 발휘 여부에 주안을 두고 소요군 주도로 계획/실시되기 때문에 AT 기술에 주안을 두고 있는 본 시험평가 방안에서는 포함하지 않는다.

체계공학기반의 프로세스에 적용한 안티탬퍼링 시험평가 프로세스는 시험평가기본계획(TEMP, Test and Evaluation Master Plan) 수립, 연구개발 시험평가, 시험평가결과 제출, 시험평가기준 충족여부 판정, 방위사업추진위원회 보고, 소요군 정책회의 보고의 순서로 진행된다.

시험평가기본계획서(TEMP)는 연구개발하는 무기체계의 시험평가계획을 종합적으로 명시한 문서로, 최초 체계개발 수행 시 작성해야 하며, 시험평가기본계획서는 개발시험평가와 운용시험평가의 기준문서가 된다. 작성 시에는 체계개발실행계획서, 체계요구사항명세서 등에 근거하여 작성해야 하며, 이 중 안티탬퍼링 관련 내용은 AT 요구사항 정의서에 근거하여 작성된 안티탬퍼링 계획의 안티탬퍼링 요구사항 명세서, 안티탬퍼링 개발규격서 등을 참고하여 안티탬퍼링 시험평가 기본계획서(AT-TEMP)를 작성한다. 이렇게 작성된 안티탬퍼링 관련 내용은 분리 작성하여 공유나 노출이 되지 않도록 관리해야 한다.

〈표 4〉 AT 시험평가 조직구성 및 역할



- PM통제하에 "AT개발 전담팀"이 주도
- AT 개발요소별 담당자 지정
- 협력업체 : 기술지원
- 지원기관 : 국과연, 기품원, 기타
- 통제기관 : 방사청(IPT), 국과연(국가주도사업)
- 검증 : 통제기관은 지원기관에 검증요구

3.4.1 안티탬퍼링 구현(개발)단계 시험절차

안티탬퍼링 기술을 구현한 결과에 대한 시험평가는 안티탬퍼링 개발규격서에 근거해서 기술 요소별 요구 기준 충족 여부를 개발팀장의 주도하에 시험절차서를 작성하고 담당자별 역할을 분담하여 진행하는데, 안티탬퍼링 시험평가 기본계획서(AT-TEMP)에 기본적인 내용을 반영하여야 하며, 안티탬퍼링 구현단계 시험절차는 아래 〈표 7〉과 같다.

〈표 7〉 안티탬퍼링 구현(개발)단계 시험절차

시험절차(역할)	비 고
① AT 시험절차서 작성 (담당분야별)	AT-TEMP AT 개발규격서(기준)
② AT 시험절차서 검토/ PM보고 (AT개발팀장)	참여인원 역할확인(통제)
③ AT 시험평가(시험 참여/지원(인원) * "시험절차서" 항목별 확인	신뢰성/보안성 시험 포함 (정적시험, 동적시험)
④ 미비점 보완/확인시험(개발팀장 통제)	
⑤ AT 시험결과 보고(개발팀장)	PM, IPT

3.4.2 체계통합단계 시험절차

안티탬퍼링 기술을 구현한 이후에 체계통합시험을 하는 단계에는 해당 체계규격서에서 설정한 개발 목표대로 기능 구현이 되었는지에 주안을 두고 해당 체계개발팀의 주도하에 안티탬퍼링 관련 분야의 기능구현 시험항목에 대한 담당자별 역할을 분담하여 진행한다. 이때 세부 진행 절차는 안티탬퍼링 구현(개발)단계의 프로세스를 준용하며 구성품과 체계가 통합 개발했을 경우 안티탬퍼링 구현(개발)단계의 절차와 통합하여 시험을 진행한다.

3.4.3 개발시험평가(DT&E) 시험절차

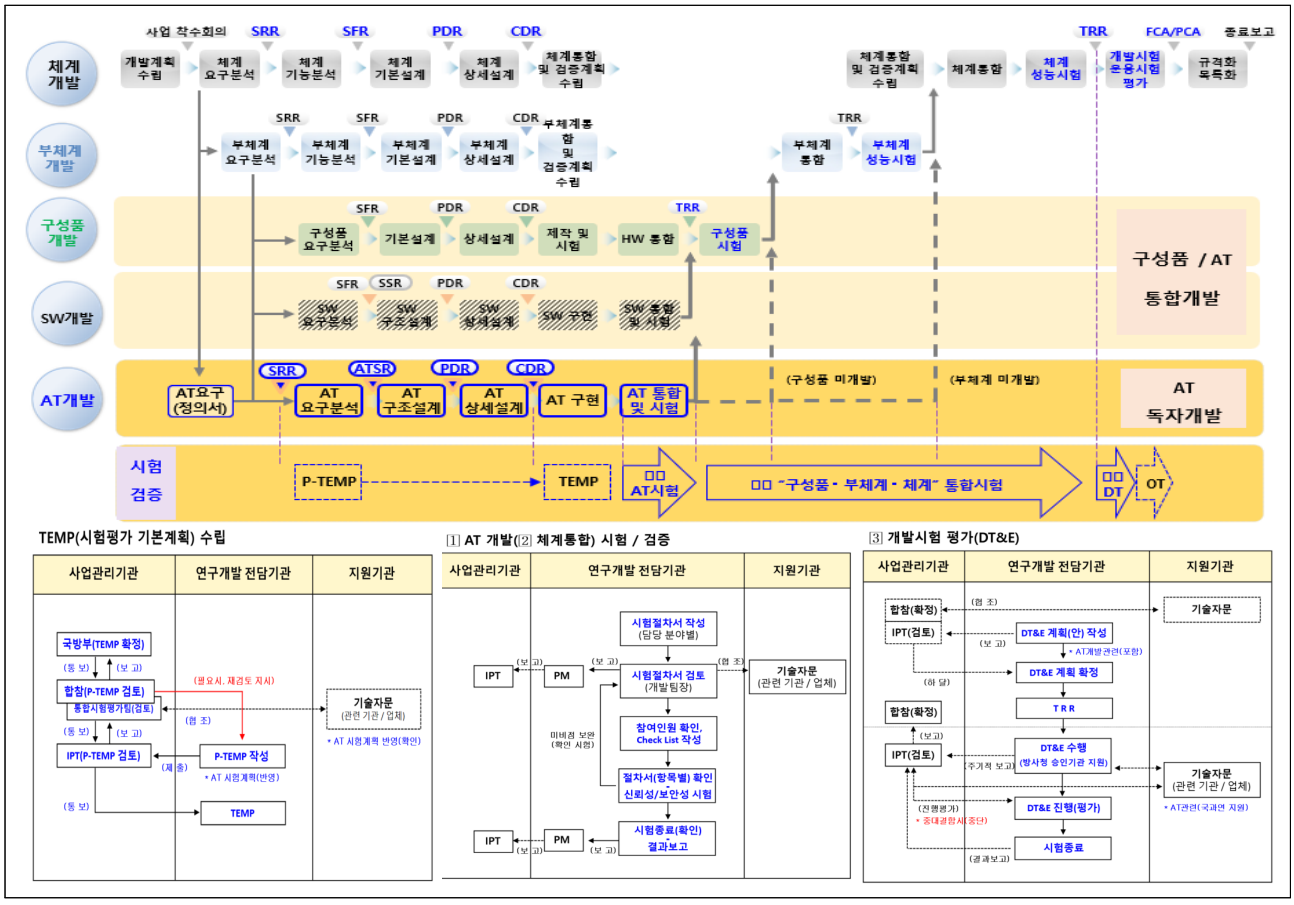
개발시험평가 단계는 TEMP에 근거하여 ATTP를 포함한 개발시험평가 계획을 작성하여 IPT의 검토 후에 합참 시험평가부에서 확정되면 TRR(Test Readmess Review, 시험 준비상태 점검) 시행 후에 착수한다.

개발시험평가 단계의 시험절차는 〈표 8〉과 같다. 우선 연구개발주관기관에서 DT&E 계획(안)의 작성을 진행하면 IPT에서 DT&E 계획(안)을 검토하고 검토된 계획(안)을 시험평가부에 접수한다. 접수된 계획(안)을 기반으로 통합시험평가팀에서 검토회의를 진행하고 DT&E 계획을 확정한다. 이후 TRR을 수행하고 연구개발주관기관의 주도하에, 개발시험평가에 착수한다. 시험평가의 진행사항은 IPT를 거쳐서 시험평가부에 보고되어야 하며 IPT에서는 시험평가 진행사항을 평가하여 시험평가에 결함이 있는지 확인한다. 시험평가 종료 이후에는 시험평가 결과보고서를 작성하여 시험평가부에 보고한다.

〈표 8〉 개발시험평가(DT&E)단계 시험/검증 절차

SE 단계	시험/검증 절차(역할)	AT 시험/검증
	① DT&E 계획(안) 작성 (연구개발주관기관)	• AT 시험계획서(ATTP) 작성, AT-TEMP/개발규격서 (근거) * ATTP 작성양식 [별지 #2]참조
	② DT&E 계획(안) 검토 (방사청) * 필요시 검토회의 (합참/소요군 등 참석)	
D-60일 (이전)	③ DT&E 계획(안) 접수 (합 시험평가부) * 관련기관/통합시험평가팀 의견수렴	• 반영내용(확인)
D-45일	④ 통합시험평가팀 검토회의 (합참 시험평가부)	
D-30일	⑤ DT&E 계획 확정/통보 (합참 시험평가부)	• AT 시험절차서(ATTD) 작성
D-15일	⑥ TRR	
D일	⑦ DT&E 착수 (연구개발주관기관) * 진행현황 보고 : 개발기관 → 방사청 → 합참	• 검증 : 국과연 (기품원) 적절 * 공인시험기관의뢰 가능 • 필요시, 소요제기기관 입회
	⑧ 시험평가진행 평가 (방사청) * 보완이 불가한 결함발생 시 중단, 합참통보	
D+30일	⑨ 시험평가 종료 / 결과 보고 (연구개발주관기관) * 결과보고 : 연구개발기관 → 방사청 → 합참	

이상의 안티탬퍼링 시험평가 프로세스를 도식화하면 〈그림 2〉와 같다.



〈그림 2〉 체계공학기반 AT기술 시험평가 프로세스

Ⅳ. 결론

본 연구는 안티탬퍼링 기술의 연구개발단계에서 정상적으로 개발되었는지를 시험평가하는데 필요한 최적의 조직과 역할 및 절차등의 프로세스에 관해 연구하였다.

안티탬퍼링기술의 시험평가 프로세스는 국방전력발전업무훈령과 합참시험평가지침서의 기준과 절차에 의해 진행되기 때문에 일반적인 시험평가 프로세스와 다를 것 없이 개발주도기관(업체)의 수준과 의지가 중요하다.

그런측면에서 시험평가의 구체적인 기준이 되는 "안티탬퍼링 개발규격서"를 어떻게 작성하고, 어떻게 시험할 것인지를 계획한 "안티탬퍼링 시험계획서 및 시험절차서"를 개발전담기관(업체)에서 작성할때 통제(관리)기관의 검토(승인)와 확인(검증)이 매우 중요하다.

그리고, 표준 적합성 시험 대상 무기체계일 경우 국방정보화업무훈령(180조 제3항)에 근거하여 표준 적합성 시험을 합동상호운용성기술센터가 별도로 해야 하는 점과, SW에 대한 신뢰성 / 보안성 시험을 정적 / 동적으로 어떻게 시험할 것인지, 그리고 항공안전기준을 위한 감항인증관련 절차 등을 안티탬퍼링 프로세스에 어떻게 적용해야할지에 대한 추가 연구가 필요하다.

참고문헌

1) 류연승, “무기체계 소프트웨어 핵심기술 보호 방안”, 방위사업청 획득업무발전 컨퍼런스, 2018.
2) 이민우, “국방 무기시스템 기술보호를 위한 수명주기 프로세스 모델 개발”, 아주대학교 박사학위 논문, 2019년 8월.
3) 송경호, 허아라, 류연승. “체계공학 기반 안티탬퍼링 프로세스.” 韓國防衛産業學會誌 28.3 (2021): 77-91.
4) 송경호, 허아라, 류연승. (2021). “무기체계 안티탬퍼링을 위한 기술 식별 및 위험평가 방안”. 한국방위산업학회지, 28(2), 41-50.
5) 김민욱. (2023). “안티탬퍼링의 동향 및 발전 방향 연구”. 한국산학기술학회 논문지, 24(9), 82-88.
6) Lt Col Arthur F. Huber, et al, “The Role and Nature of Anti-tamper Techniques in US Defense Acquisition,” Acquisition Review Quarterly, Fall 1999.
7) GAO-04-302, “DoD Needs to Better Support Program Managers’ Implementation of Anti-Tamper Protection,” March, 2004.
8) GAO-08-91, “Departmentwide Direction is needed for Implementation of the Anti-tamper Policies,” January, 2008.
9) Melinda Reed, “System Security Engineering and Program Protection Integration into SE,” 17th Annual NDIA Systems Engineering Conference, October, 2014.
10) Thomas Hurt, “DoD Software Assurance (SwA) Overview,” 17th Annual NDIA Systems Engineering Conference, October, 2014.
11) Raymond Shanahan, “Identification and Protection of Critical Program Information (CPI),” 18th Annual NDIA Systems Engineering Conference, October, 2015.
12) Vincent Immler, et al., “Secure Physical Enclosures from Covers with Tamper-Resistance,” In: IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019
13) Ninja Donatelli, “Critical Program Information (CPI) Workshop”, CPI Workshop, June, 2019.
14) Thomas Hurt, “Software Assurance Throughout the System Life Cycle,” 22nd Annual NDIA Systems and Mission Engineering Conference, October, 2019.
15) EN ISO/IEC 19790:2020 - 정보 기술 - 보안 기술 - 암호화 모듈에 대한 보안 요구 사항
16) KSXISOIEC19790 정보기술 — 보안기술 — 암호모듈 보안 요구사항
17) KSXISOIEC24759 정보기술 — 보안기술 — 암호모듈 시험 요구사항
18) 방위사업청, “전장관리 정보체계 연구개발 (업체주관) 사업관리 절차도”, 2009년 9월.
19) 방위사업청, “무기체계 획득단계별 M&S 활용 실무지침서”, 2013년 12월.
20) 방위사업청, “국방과학기술 정보관리업무 지침”, 2014년 11월.
21) 방위사업청, “SE기반 기술검토회의 가이드북”. 2017년 7월.
22) 방위사업청, “무기체계 RAW 업무지침”, 2018년 8월.
23) 방위사업청, “SE기반 위험관리 가이드북”, 2018년 10월.
24) 방위사업청, “과학적사업관리 수행지침”, 2019년 9월.
25) 방위사업청, “연구개발 실행계획서 작성 절차도”, 2020년 2월.
26) 방위사업청, “함정건조 사업관리 절차도”, 2020년 8월.
27) 방위사업청, “방위사업관리규정”, 2020년 12월.
28) 방위사업청, “방위산업기술 보호 지침”. 2020년 12월.
29) 방위사업청, “업체주관 연구개발 사업관리 절차도”, 2020년 12월.
30) 방위사업청, “국관연주관 연구개발 사업관리 절차도”, 2021년 4월.
31) 방위사업청, “핵심기술연구개발 (기초/응용/시험개발) 사업관리 절차도”, 2021년 4월.
32) MDA Directive 5200.05, “Anti-Tamper Policy,” July, 2006.
33) DoDI 5000.02, “Operation of Defense Acquisition System,” January, 2020.
34) DoDI 5200.01, “DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI) and associated manuals (DoDM 5200.01 Vol 1-4),” Feburary, 2012.
35) DoDI 5200.1-H, “Handbook for writing Security Classification Guidance,” September, 2018.
36) DoDI 5200.39, “Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E),” May, 2015.
37) DoDI 5200.39, “Required Use of Standardized Process for the Identification of Critical Program

Information (CPI) in DON Acquisition Programs," September, 2007.
38) DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November, 2012.
39) DoDM 5200.45, "Instructions for Developing Security Classification Guides," September, 2020.
40) DoDD 5200.47E, "Anti-Tamper (AT)," September, 2015.
41) DoDD 5200.05, "Anti-Tamper Policy, Missile Defense Agency," July, 2006.
42) DoDI 4140.67, "DoD Counterfeit Prevention Policy," April, 2013.
43) DoDI 8500.01, "Cybersecurity," March, 2014
44) DoDI 8500.01, "Cybersecurity Test and Evaluation Guidebook," July, 2015.
45) DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology," March, 2014.
46) DoDI 8510.01, "Defense Acquisition Guidebook (DAG)," October, 2017.
47) DoDI 8510.01, "Program Protection Plan Outline & Guidance," July, 2011.
48) DoDI 8510.01, "USAF Weapon Systems Program Protection and SSE Guidebook, Version 2.0," August, 2020.
49) USAF "Weapon System Program Protection / System Security Engineering Guidebook," Version 2.0, March, 2020.
50) MDA Directive 5200.05, "Anti-Tamper Policy," July, 2006.
51) DAU, "Hardware Assurance (HwA) Through the Lifecycle," Octorber, 2018.
52) DAU, "Defense Acquisition Guidebook," September, 2020.
53) Berlato, S., Ceccato, M. (2020). A large-scale study on the adoption of anti-debugging and anti-tampering protections in android apps. Journal of Information Security and Applications, 52, 102463.
54) Chou, Y., Anggriani, K., Wu, N., Hwang, M. (2021). Research on E-book Text Copyright Protection and Anti-tampering Technology. International Journal of Network Security, 23(5), 739-749.