DEFENSE RESEARCH INSTITUTE OF MONGOLIA

Journal of Security and Defense Studies

Journal homepage:
https://mids.gov.mn/category/ayulgui_baidal-2/

ISSN: 2220-9115, E-ISSN: 2708-1230

Research Article

DOI: https://doi.org/10.65816/jsds.2026.02.009

Theoretical and Methodological Approaches to the Development of an Artificial Intelligence-Driven Cybersecurity Protection Model for the Defense Sector of Mongolia

Chadraabal Baatar

Senior Lecturer, Department of Public Management, National Academy of Governance, Master of Philosophy (M.Phil), E-mail address: baatar@naog.gov.mn, ORCID: 0009-0002-5222-9811

Received: 05 May 2026
Revised: 12 June 2026
Accepted: 30 June 2026
Published online: 28 July 2026

ABSTRACT

In the context of accelerating digital transformation, network-centric operations, and the growing interdependence of information infrastructures, cyberspace has become an integral component of national security and defense systems. Under these conditions, traditional defensive mechanisms alone are no longer sufficient, and the importance of artificial intelligence (AI)-based cybersecurity solutions is rapidly increasing. The purpose of this paper is to define the theoretical and methodological foundations for developing an AI-based cybersecurity model tailored to the specific characteristics of Mongolia's defense sector. The study examines the integration of AI into cybersecurity systems by applying risk management theory, systems theory, information security architecture theory, game theory, and organizational resilience theory. It also investigates the applications of machine learning, deep learning, anomaly detection, malware classification, risk prediction, automated response mechanisms, and cyber intelligence data processing. As a result, a methodological framework for implementing an AI-based cybersecurity model in Mongolia's defense sector is proposed, consisting of key stages such as risk assessment, data collection and processing, machine learning model development, real-time monitoring, and automated response. Furthermore, an architectural model is introduced, comprising a data collection layer, threat intelligence repository, machine learning analytics module, risk assessment module, automated decision-making system, SOAR platform, and strategic management dashboard. This model provides both theoretical and practical significance for enhancing early threat detection, reducing cyber risks, supporting decision-making processes, and strengthening national defense capabilities.

Keywords: *Machine Learning; Anomaly Detection; Risk Assessment; Automated Response; Information Security Architecture; Strategic Decision-Making.*

Монгол Улсын батлан хамгаалах салбарын кибер аюулгүй байдлын хиймэл оюунд суурилсан хамгаалалтын загвар боловсруулах онол, арга зүйн асуудал

Чадраабал Баатар

Удирдлагын академийн Улсын салбарын удирдлагын тэнхимийн ахлах багш, магистр,
baatar@naog.gov.mn, ORCID: 0009-0002-5222-9811

ХУРААНГУЙ

Дижитал шилжилт, сүлжээ төвтэй ажиллагаа болон мэдээллийн дэд бүтцийн хамаарал өсөн нэмэгдэж буй өнөө үед кибер орчин нь үндэсний аюулгүй байдал, батлан хамгаалах тогтолцооны салшгүй бүрэлдэхүүн хэсэг болж байна. Иймэрхүү уламжлалт хамгаалалтын арга хэрэгслүүд дангаараа хангалттай үр дүн үзүүлэхгүй болсон бөгөөд хиймэл оюунд суурилсан кибер хамгаалалтын шийдлүүдийн ач холбогдол эрчимтэй нэмэгдэж байна. Энэхүү өгүүллийн зорилго нь Монгол Улсын батлан хамгаалах салбарын онцлогт нийцсэн хиймэл оюунд суурилсан кибер хамгаалалтын загвар боловсруулах онол, арга зүйн үндсийг тодорхойлоход оршино. Өгүүлэлд эрсдэлийн удирдлагын онол, системийн онол, мэдээллийн аюулгүй байдлын архитектурын онол, тоглоомын онол болон байгууллагын тогтвортой байдлын онолыг ашиглан хиймэл оюуныг кибер хамгаалалтын тогтолцоонд нэгтгэх боломжийг шинжилсэн. Мөн машин сургалт, гүн сургалт, аномали илрүүлэлт, хортой кодын ангилал, эрсдэлийн урьдчилсан таамаглал, автомат хариу арга хэмжээ болон кибер тагнуулын мэдээлэл боловсруулах чиглэл дэх хэрэглээг судалсан. Судалгааны үр дүнд Монгол Улсын батлан хамгаалах салбарт хэрэгжүүлэх хиймэл оюунд суурилсан хамгаалалтын загварын арга зүйг эрсдэлийн үнэлгээ, өвөгдөл цуглуулах ба боловсруулах, машин сургалтын загвар хөгжүүлэх, бодит цагийн хяналт, автомат хариу арга хэмжээ гэсэн үндсэн үе шатуудаар тодорхойлсон. Түүнчлэн өвөгдөл цуглуулах давхарга, аюул заналын тагнуулын сан, машин сургалтын аналитик хэсэг, эрсдэлийн үнэлгээний модуль, автомат шийдвэр гаргалтын систем, “Аюулгүй байдлын уялдуулалт, автоматжуулалт ба хариу арга хэмжээ (SOAR)”-ний платформ болон стратегийн удирдлагын самбараас бүрдэх архитектурын загварыг санал болгосон. Энэхүү загвар нь кибер халдлагыг эрт илрүүлэх, эрсдэлийг бууруулах, шийдвэр гаргалтыг дэмжих, үндэсний батлан хамгаалах чадавхыг бэхжүүлэх онолын болон практик ач холбогдолтой юм.

Түлхүүр үгс: *Машин сургалт; Аномали илрүүлэлт; Эрсдэлийн үнэлгээ; Автоматжуулсан хариу арга хэмжээ; Мэдээллийн аюулгүй байдлын архитектур; Стратегийн шийдвэр гаргалт.*

Оршил

Орчин үед батлан хамгаалах салбарын кибер аюулгүй байдлыг хангахад хиймэл оюун нь илрүүлэлт, хамгаалалт, урьдчилсан таамаглал болон хариу арга хэмжээний бүх түвшинд өргөнөөр ашиглагдаж байна. Тодруулбал, хиймэл оюунд суурилсан системүүд нь сүлжээний урсгал, лог файл, хэрэглэгчийн зан төлөв болон төхөөрөмж хоорондын харилцааг бодит цаг хугацаанд шинжилж, хэвийн үйл ажиллагаанаас хазайсан аномали болон сэжигтэй үйлдлийг автоматаар илрүүлэх боломжийг бүрдүүлдэг. Үүний зэрэгцээ машин сургалтын алгоритмууд нь өмнөх халдлагын өгөгдөлд тулгуурлан шинэ төрлийн кибер халдлагын хэв шинжийг таних чадварыг нэмэгдүүлж, уламжлалт гарын үсэгт суурилсан хамгаалалтын аргын сул талыг нөхөж байна. Батлан хамгаалах байгууллагууд хиймэл оюуныг мөн халдлагын эрсдэлийг урьдчилан таамаглахад ашиглаж, эмзэг байдлын магадлал болон довтолгооны чиг хандлагыг тооцоолсноор стратегийн шийдвэр гаргалтыг

сайжруулдаг. Үүнээс гадна хиймэл оюун нь автомат хариу арга хэмжээний системтэй уялдан ажиллаж, илэрсэн аюулыг тусгаарлах, сүлжээний урсгалыг хаах, халдварлагдсан системийг хамгаалах зэрэг үйлдлийг хүний оролцоогүйгээр гүйцэтгэх боломжийг олгодог. Мөн аюул заналын тагнуулын мэдээллийг боловсруулахад байгалийн хэл боловсруулалтын аргачлалуудыг ашигласнаар олон эх сурвалжийн мэдээллийг нэгтгэн нөхцөл байдлын цогц зураглал гаргах боломж нэмэгдэж байна. Гэсэн хэдий ч хиймэл оюунд суурилсан системүүд нь буруу ангилал, өгөгдлийн гажуудал болон дайсагнасан халдлагад өртөх эрсдэлтэй тул хүний шинжээчийн хяналттай хослуулан ашиглах шаардлагатай хэвээр байна. Иймээс орчин үеийн батлан хамгаалах кибер хамгаалалт нь хиймэл оюуныг гол тулгуур технологи болгон ашиглаж, илүү ухаалаг, дасан зохицох чадвартай, өндөр хурдтай хамгаалалтын тогтолцоог бүрдүүлж байна.

Дижитал шилжилт, сүлжээ төвтэй байлдааны үзэл баримтлал, мэдээллийн дэд бүтцийн хамаарал өсөн нэмэгдэж буй өнөө үед кибер орчин нь үндэсний аюулгүй байдал, батлан хамгаалах тогтолцооны салшгүй бүрэлдэхүүн хэсэг болж байна. Батлан хамгаалах салбарын мэдээллийн систем, команд удирдлагын сүлжээ, зэвсгийн удирдлагын платформ, тагнуулын мэдээллийн сангууд нь кибер халдлагын өндөр эрсдэлтэй объект болж байгаа бөгөөд уламжлалт хамгаалалтын арга хэрэгслүүд дангаараа хангалттай үр дүн үзүүлэхгүй болжээ. Ийм нөхцөлд хиймэл оюунд суурилсан кибер хамгаалалтын шийдлүүд нь аюул заналыг урьдчилан илрүүлэх, бодит хугацаанд шинжлэх, халдлагын хэв маягийг тодорхойлох, автомат хариу арга хэмжээ хэрэгжүүлэх боломжийг бүрдүүлж байна.

Монгол Улсын батлан хамгаалах салбарын мэдээллийн технологийн хөгжил нэмэгдэхийн хэрээр кибер аюулгүй байдлыг хангах асуудал стратегийн ач холбогдолтой болсон. Иймээс үндэсний онцлог, батлан хамгаалах байгууллагын бүтэц, мэдээллийн урсгал, эрсдэлийн түвшинд нийцсэн хиймэл оюунд суурилсан хамгаалалтын загвар боловсруулах нь онолын болон практик ач холбогдол бүхий судалгааны чиглэл болж байна.

Нэг. Кибер аюулгүй байдлын тухай үндсэн ойлголт, онолын үндэс

Орчин үеийн мэдээллийн нийгэмд мэдээлэл, харилцаа холбооны технологийн хэрэглээ эрчимтэй өсөн нэмэгдэж, хувь хүн, байгууллага болон төрийн байгууллагуудын үйл ажиллагаа дижитал орчинд ихээхэн төвлөрөх болсон. Үүний зэрэгцээ мэдээллийн систем, сүлжээ, өгөгдөлд чиглэсэн халдлага, зөвшөөрөлгүй хандалт, мэдээлэл алдагдах зэрэг эрсдэлүүд нэмэгдэж байгаа нь кибер аюулгүй байдлын ач холбогдлыг улам бүр нэмэгдүүлж байна.

“Стандарт, технологийн үндэсний хүрээлэн (NIST)”-гийн кибер аюулгүй байдлын хүрээ (Cybersecurity Framework) нь хамгаалах, илрүүлэх, хариу арга хэмжээ авах, сэргээн босгох гэсэн үндсэн функцүүдээр кибер хамгаалалтын үйл ажиллагааг тодорхойлдог (National Institute of Standards and Technology 2024).

Кибер аюулгүй байдал нь компьютерийн систем, сүлжээ, програм хангамж, өгөгдөл болон дижитал дэд бүтцийг халдлага, гэмтэл, зөвшөөрөлгүй нэвтрэлт болон бусад аюул заналаас хамгаалахтай холбоотой бодлого, технологи, үйл ажиллагаа болон хүний хүчин зүйлсийн цогц гэж үзэж болно (National Institute of Standards and Technology 2024).

Кибер аюулгүй байдлын үндсэн зорилго нь мэдээллийн нууцлал (confidentiality), бүрэн бүтэн байдал (integrity), хүртээмжтэй байдал (availability) гэсэн мэдээллийн аюулгүй байдлын суурь гурван зарчмыг хангахад оршино (Stallings 2018). Нууцлал нь зөвхөн эрх бүхий хэрэглэгч мэдээлэлд хандах боломжтой байхыг илэрхийлдэг бол бүрэн бүтэн байдал нь мэдээлэл зөвшөөрөлгүйгээр өөрчлөгдөөгүй, үнэн зөв хэвээр хадгалагдаж буйг баталгаажуулдаг. Харин хүртээмжтэй байдал нь шаардлагатай үед мэдээлэл болон үйлчилгээ хэрэглэгчдэд тасралтгүй хүрч байх нөхцөлийг хангадаг (Whitman, M. E., Mattord, H. J 2022).

Кибер орчинд олон төрлийн аюул занал учирдаг бөгөөд эдгээрийн дотор хортой програм (malware), фишинг халдлага (phishing), үйлчилгээ саатуулах халдлага (Distributed Denial of Service буюу DDoS), ransomware, дотоод хэрэглэгчийн эрсдэл болон нийгмийн инженерчлэлийн халдлагууд түгээмэл тохиолддог. Хортой програм нь системд нэвтрэн өгөгдөл устгах, өөрчлөх, хулгайлах зорилготой байдаг бол фишинг халдлага нь хэрэглэгчийг хуурамч цахим шуудан, вэбсайт эсвэл мессеж ашиглан нууц мэдээллээ өгөхөд хүргэдэг. Сүүлийн жилүүдэд ransomware төрлийн халдлага эрчимтэй нэмэгдэж, байгууллагуудын мэдээллийг шифрлэн барьцаалах замаар их хэмжээний санхүүгийн хохирол учруулж байна (Stallings, W 2024).

Кибер аюулгүй байдлыг хангахад технологийн хамгаалалтын арга хэмжээнээс гадна хүний хүчин зүйл онцгой үүрэгтэй. Судалгаагаар мэдээллийн аюулгүй байдлын зөрчлийн ихээхэн хувь нь хүний алдаа, мэдлэг дутмаг байдал, эсвэл нийгмийн инженерчлэлийн халдлагатай холбоотой байдаг. Иймээс байгууллагууд ажилтнуудаа тогтмол сургах, аюулгүй байдлын соёлыг төлөвшүүлэх, нууц үгийн зохистой бодлого хэрэгжүүлэх, олон хүчин зүйлт баталгаажуулалт (Multi-Factor Authentication) ашиглах шаардлагатай байдаг (Singer, P. W., Friedman, A 2014).

Мөн кибер аюулгүй байдал нь зөвхөн техникийн асуудал бус үндэсний аюулгүй байдал, эдийн засгийн тогтвортой байдалтай нягт холбоотой стратегийн ач холбогдолтой салбар болсон. Эрчим хүч, санхүү, харилцаа холбоо, эрүүл мэнд зэрэг чухал дэд бүтцүүд кибер халдлагад өртөх нь улс орны үйл ажиллагаанд ноцтой саад учруулах эрсдэлтэй. Иймээс улс орнууд кибер аюулгүй байдлын бодлого боловсруулж, олон улсын хамтын ажиллагааг өргөжүүлэн, хууль эрх зүйн орчныг боловсронгуй болгоход анхаарч байна (Craigen, D., Diakun-Thibault, N., Purse, R 2014).

Кибер аюулгүй байдал нь мэдээлэл, систем, сүлжээ болон дижитал орчныг найдвартай ажиллагааг хангах үндсэн хэрэгсэл бөгөөд өнөөгийн дижитал нийгмийн салшгүй хэсэг юм. Технологийн хөгжилтэй зэрэгцэн кибер заналхийлэл улам нарийсаж байгаа тул байгууллага болон хувь хүмүүс мэдээллийн аюулгүй байдлын мэдлэгээ дээшлүүлж, хамгаалалтын үр дүнтэй арга хэмжээг тогтмол хэрэгжүүлэх шаардлагатай байна.

Кибер аюулгүй байдлын онолын үндэс нь эрсдэлийн удирдлагын онол, системийн онол, мэдээллийн аюулгүй байдлын архитектурын онол, тоглоомын онол болон аюул заналын тагнуулын (Cyber Threat Intelligence) үзэл баримтлалд тулгуурладаг.

Аюул заналын тагнуул (Cyber Threat Intelligence, CTI) нь кибер орчинд үүсэж буй болон үүсэж болзошгүй халдлага, халдагчдын арга барил, зорилго, чадавхыг

системтэйгээр цуглуулах, боловсруулж шинжлэх, тайлбарлах үйл явцыг хэлнэ. Энэ нь зөвхөн техникийн өгөгдөлд тулгуурлахаас гадна стратегийн, тактикийн болон үйл ажиллагааны түвшний мэдээллийг нэгтгэн байгууллагын шийдвэр гаргалтыг дэмжих зорилготой байдаг. Аюул заналын тагнуулын үндсэн зорилго нь болзошгүй аюулыг урьдчилан тодорхойлж, хамгаалалтын арга хэмжээг цаг тухайд нь хэрэгжүүлэх замаар эрсдэлийг бууруулахад оршино. Ийнхүү аюул заналын тагнуул нь кибер аюулгүй байдлыг реактив бус, харин урьдчилан сэргийлэх, ухаалаг удирдлагад суурилсан түвшинд хүргэх чухал бүрэлдэхүүн хэсэг болдог.

Хүснэгт 1. *Кибер аюулгүй байдлын суурь болдог түгээмэл онолуудын үндсэн ойлголт, гол агуулга болон практикт хэрэглэгдэх ач холбогдол*

Онол	Үндсэн ойлголт	Гол агуулга	Кибер аюулгүй байдал дахь хэрэглээ
Эрсдэлийн удирдлагын онол (Risk Management Theory)	Байгууллагын зорилгод нөлөөлж болзошгүй эрсдэлийг тодорхойлж, үнэлж, бууруулах үйл явц	Эрсдэлийг илрүүлэх, шинжлэх, үнэлэх, хянах, бууруулах арга хэмжээ боловсруулах	Кибер заналхийлэл, эмзэг байдал, эрсдэлийн түвшинг үнэлэх, хамгаалалтын бодлого боловсруулах, хөрөнгө хамгаалах
Системийн онол (Systems Theory)	Байгууллага нь харилцан хамааралтай дэд системүүдээс бүрдсэн нэгдмэл тогтолцоо гэж үздэг	Оролт (input), боловсруулалт (process), гаралт (output), эргэх холбоо (feedback)-ны уялдаа холбоог судална	Мэдээллийн систем, сүлжээ, хэрэглэгч, техник хэрэгсэл хоорондын хамаарлыг ойлгож аюулгүй байдлыг бүхэлд нь удирдах
Мэдээллийн аюулгүй байдлын архитектурын онол (Information Security Architecture Theory)	Аюулгүй байдлын шаардлагыг системийн бүтэц, архитектурт тусган хэрэгжүүлэх онол	Давхарласан хамгаалалт (Defense in Depth), Zero Trust, аюулгүй байдлын загварчлал, архитектурын удирдлага	Байгууллагын мэдээллийн системийн хамгаалалтын бүтэц төлөвлөх, нэвтрэх эрхийн хяналт, өгөгдөл хамгаалах
Тоглоомын онол (Game Theory)	Өрсөлдөгч талуудын шийдвэр гаргалтыг стратегийн харилцан үйлчлэлээр тайлбарладаг онол	Ашиг, зардал, эрсдэлийг тооцон хамгийн оновчтой стратегийг тодорхойлох	Халдагч ба хамгаалагчийн үйл ажиллагааг загварчлах, кибер хамгаалалтын стратеги боловсруулах

Мэдээллийн баталгаажуулалтын онол (Information Assurance Theory)	Мэдээллийн найдвартай байдал, хүртээмж, бүрэн бүтэн байдлыг хангах онол	Нууцлал (Confidentiality), Бүрэн бүтэн байдал (Integrity), Хүртээмжтэй байдал (Availability)-ын зарчим	Батлан хамгаалах болон төрийн байгууллагын мэдээллийн хамгаалалтын бодлого боловсруулах
Байгууллагын тогтвортой байдлын онол (Organizational Resilience Theory)	Байгууллага эрсдэл, халдлага, доголдлын үед үйл ажиллагаагаа үргэлжлүүлэх чадвар	Эрсдэлд дасан зохицох, сэргээн босгох, тасралтгүй ажиллагааг хангах	Кибер халдлагын дараах сэргэлт, бизнесийн болон үйл ажиллагааны тасралтгүй байдал
Нийгэм-техникийн системийн онол (Socio-Technical Systems Theory)	Технологи болон хүний хүчин зүйл харилцан нөлөөлдөг гэж үздэг	Техник, байгууллага, хүний зан төлөвийн уялдаа холбоо	Фишинг халдлага, дотоод аюул занал, хэрэглэгчийн аюулгүй байдлын зан төлөвийг судлах
Гүн хамгаалалтын онол (Defense in Depth Theory)	Нэг хамгаалалт алдагдсан ч бусад хамгаалалт үргэлжлэн ажиллах олон давхар хамгаалалтын зарчим	Сүлжээ, систем, өгөгдөл, хэрэглэгчийн түвшний олон шатлалт хамгаалалт	Батлан хамгаалах байгууллагын кибер хамгаалалтын архитектурын үндсэн зарчим болдог

Дээрх хүснэгтэд дурьдсан онолуудаас батлан хамгаалах байгууллагын кибер аюулгүй байдлын судалгаанд хэд хэдэн онолын хандлагыг өргөн ашигладаг бөгөөд эдгээр нь байгууллагын мэдээллийн хөрөнгө, дижитал дэд бүтэц, үйл ажиллагааны тогтвортой байдлыг хамгаалах асуудлыг олон талаас нь тайлбарлах боломжийг олгодог. Эдгээр онолуудаас эрсдэлийн удирдлагын онол, системийн онол, мэдээллийн аюулгүй байдлын архитектурын онол, тоглоомын онол болон байгууллагын тогтвортой байдлын онол нь хамгийн түгээмэл хэрэглэгддэг онолуудын тоонд ордог.

Юуны өмнө эрсдэлийн удирдлагын онол нь кибер аюулгүй байдлын судалгааны үндсэн онолын суурь болдог. Энэхүү онолын дагуу байгууллагын мэдээллийн системд учирч болзошгүй аюул занал, эмзэг байдал болон тэдгээрээс үүсэх эрсдэлийг тодорхойлж, үнэлэн, зохих хамгаалалтын арга хэмжээг төлөвлөх боломж бүрддэг. Батлан хамгаалах байгууллагын хувьд кибер халдлага нь зөвхөн мэдээллийн алдагдал үүсгэхээс гадна үндэсний аюулгүй байдал, цэргийн ажиллагааны үр дүнд нөлөөлөх өндөр эрсдэлтэй байдаг тул эрсдэлийн удирдлагын онол нь кибер хамгаалалтын бодлого боловсруулах, нөөцийн оновчтой хуваарилалт хийх, хамгаалалтын тэргүүлэх чиглэлийг тодорхойлоход чухал ач холбогдолтой байдаг.

Батлан хамгаалах салбарын кибер аюулгүй байдлыг хамгаалах хүрээнд эрсдэлийн удирдлагын онолын үүднээс хиймэл оюуныг ашиглах нь аюул заналыг

тодорхойлох, үнэлэх, хариу арга хэмжээ төлөвлөх болон хяналт тавих бүх үе шатыг илүү үр ашигтай болгох боломжтой. Эрсдэлийн удирдлагын уламжлалт загваруудтай уялдуулан хиймэл оюунд суурилсан системүүд нь сүлжээний урсгал, системийн лог, эмзэг байдлын мэдээлэл болон аюул заналын тагнуулын өгөгдлийг нэгтгэн боловсруулж, эрсдэлийн магадлал болон нөлөөллийг илүү нарийвчлалтай тооцоолдог (National Institute of Standards and Technology 2012). Мөн машин сургалтын алгоритмууд нь динамик орчинд шинэ төрлийн халдлагын хэв шинжийг илрүүлж, эрсдэлийн түвшинг бодит цаг хугацаанд шинэчилснээр шийдвэр гаргалтын чанарыг сайжруулдаг (Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., Ng, A 2020). Үүний зэрэгцээ хиймэл оюун нь автоматжуулсан эрсдэлийн үнэлгээ болон SOAR-т суурилсан хариу арга хэмжээний системтэй уялдан ажилласнаар хамгаалалтын үйл ажиллагааны хурд, үр нөлөөг нэмэгдүүлдэг. Иймээс хиймэл оюуныг эрсдэлийн удирдлагын тогтолцоонд нэгтгэх нь батлан хамгаалах салбарын кибер хамгаалалтыг илүү дасан зохицох чадвартай, өгөгдөлд суурилсан, стратегийн түвшний шийдвэр гаргалтыг дэмжих чухал арга зам болж байна.

Хоёрдугаарт, системийн онол нь батлан хамгаалах байгууллагыг харилцан хамааралтай олон дэд системээс бүрдсэн нэгдмэл тогтолцоо гэж үздэг. Орчин үеийн батлан хамгаалах байгууллагын үйл ажиллагаа нь мэдээллийн систем, холбооны сүлжээ, хүний нөөц, команд удирдлагын бүтэц болон техникийн дэд бүтцийн нягт уялдаанд тулгуурладаг. Иймээс системийн онол нь кибер аюулгүй байдлын асуудлыг зөвхөн технологийн өнцгөөс бус байгууллагын бүхэл бүтэн үйл ажиллагаатай холбон судлах боломжийг олгодог. Нэг дэд системд гарсан доголдол нь бусад системийн ажиллагаанд хэрхэн нөлөөлөхийг ойлгох нь кибер эрсдэлийг цогцоор нь үнэлэхэд чухал ач холбогдолтой юм.

Батлан хамгаалах салбарын кибер аюулгүй байдлыг системийн онолын үүднээс авч үзвэл хиймэл оюун нь хоорондоо уялдаа холбоотой олон дэд системээс бүрдэх цогц хамгаалалтын экосистемийг оновчтой удирдах хэрэгсэл болж ашиглагдана. Системийн онолын дагуу кибер орчин нь өгөгдөл цуглуулах, боловсруулалт хийх, шийдвэр гаргалт болон хариу үйлдэл зэрэг харилцан хамааралтай бүрэлдэхүүн хэсгүүдээс бүрдэх тул хиймэл оюун нь эдгээрийн хооронд мэдээллийн урсгалыг нэгтгэн, бодит цагийн нөхцөл байдлын цогц дүр зургийг (situational awareness) бүрдүүлэхэд чухал үүрэгтэй (Bertalanffy, L. von 1968). Мөн машин сургалт нь системийн доторх хэвийн ба хэвийн бус зан төлөвийн уялдаа холбоог илрүүлснээр гажуудлыг эрт таних, системийн тогтвортой байдлыг хадгалах боломжийг нэмэгдүүлдэг (Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., Ng, A 2020). Үүнээс гадна хиймэл оюун нь дэд системүүдийн хоорондын хариу үйлдлийг автоматжуулж, SOAR болон SIEM платформуудтай уялдан ажилласнаар бүхэл системийн өөрөө зохицох болон дасан зохицох чадварыг сайжруулдаг. Иймээс системийн онолын хүрээнд хиймэл оюуныг ашиглах нь батлан хамгаалах салбарын кибер хамгаалалтыг цогц, уялдаа холбоотой, тасралтгүй сайжрах чадвартай систем болгон хөгжүүлэх үндсэн арга зам юм.

Гуравдугаарт, мэдээллийн аюулгүй байдлын архитектурын онол нь байгууллагын мэдээллийн системийн хамгаалалтын бүтэц, зохион байгуулалт болон хамгаалалтын давхаргуудыг төлөвлөхөд чиглэдэг. Энэхүү онолын хүрээнд

хамгаалалтын олон давхаргат аргачлал (Defense in Depth), Тэг итгэлцлийн архитектур (Zero Trust Architecture) зэрэг орчин үеийн хамгаалалтын загваруудыг ашигладаг. Батлан хамгаалах байгууллагын хувьд мэдээллийн аюулгүй байдлын архитектур нь нууц мэдээллийг хамгаалах, хэрэглэгчийн эрхийн удирдлагыг хэрэгжүүлэх, системийн найдвартай ажиллагааг хангах үндсэн механизм болж өгдөг. Тиймээс энэхүү онол нь байгууллагын кибер хамгаалалтын техникийн суурийг бүрдүүлдэг гэж үздэг.

Батлан хамгаалах салбарын кибер аюулгүй байдлыг мэдээллийн аюулгүй байдлын архитектурын онолын үүднээс авч үзвэл хиймэл оюун нь давхаргат хамгаалалтын бүтэц (defense-in-depth)-ийг илүү ухаалаг, дасан зохицох чадвартай болгон хөгжүүлэх үндсэн бүрэлдэхүүн болж ашиглагдана. Архитектурын хандлагад тулгуурлан хиймэл оюун нь өгөгдөл цуглуулах, боловсруулах, хадгалах болон хамгаалах давхаргуудын хоорондын мэдээллийн урсгалыг уялдуулж, аюулгүй байдлын хяналтын цэг бүрт бодит цагийн дүн шинжилгээ хийх боломжийг бүрдүүлдэг (McGraw 2006). Мөн машин сургалтын аргууд нь сүлжээний зан төлөв болон системийн харилцан үйлчлэлд суурилан аюулын хэв шинжийг тодорхойлж, архитектурын түвшинд сул талуудыг эрт илрүүлэхэд тусалдаг (Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., Ng, A 2020). Үүнээс гадна хиймэл оюун нь SIEM болон SOAR зэрэг архитектурын бүрэлдэхүүн системүүдтэй уялдан ажилласнаар автомат хяналт, хариу арга хэмжээний давхаргыг бий болгож, хамгаалалтын үр ашгийг нэмэгдүүлдэг. Иймээс мэдээллийн аюулгүй байдлын архитектурын хүрээнд хиймэл оюуныг нэгтгэх нь батлан хамгаалах салбарын кибер хамгаалалтыг илүү бүтэцлэгдсэн, давхар хамгаалалттай, өндөр үр ашигтай систем болгон хөгжүүлэх чухал арга зам юм.

Дөрөвдүгээрт, тоглоомын онол нь кибер халдагч болон хамгаалагч талуудын стратегийн харилцан үйлчлэлийг судлахад ашиглагддаг. Кибер орчинд халдагч болон хамгаалагч аль аль нь өөрсдийн зорилго, боломж, нөөцөд тулгуурлан шийдвэр гаргадаг бөгөөд нэг талын үйлдэл нөгөө талын шийдвэрт нөлөөлдөг онцлогтой. Иймээс тоглоомын онол нь халдагчийн боломжит үйл ажиллагааг урьдчилан таамаглах, хамгаалалтын оновчтой стратегийг тодорхойлох, нөөцөө үр ашигтай хуваарилах зэрэг асуудлыг судлахад өргөн хэрэглэгддэг.

Батлан хамгаалах салбарын кибер аюулгүй байдлыг тоглоомын онолын үүднээс авч үзвэл хиймэл оюун нь хамгаалагч болон халдагч талуудын стратегийн харилцан үйлчлэлийг загварчлах, оновчтой шийдвэр гаргалтыг дэмжих хүчирхэг хэрэгсэл болж ашиглагдана. Тоглоомын онолын хүрээнд кибер орчин нь олон оролцогчтой, өрсөлдөөнт нөхцөл тул хиймэл оюунд суурилсан алгоритмууд нь халдагчийн боломжит стратегийг урьдчилан таамаглаж, хамгаалалтын хамгийн оновчтой хариу үйлдлийг тодорхойлох боломжийг бүрдүүлдэг (Pita, J., Jain, M., Ordóñez, F., Tambe, M., et al 2010). Мөн reinforcement learning зэрэг машин сургалтын арга нь динамик орчинд давтагдсан харилцан үйлчлэлээс суралцаж, Nash equilibrium-д ойр шийдвэр гаргалтыг автоматжуулахад ашиглагддаг (Shoham, Y., Leyton-Brown, K 2009). Үүнээс гадна хиймэл оюун нь олон хувилбарт тоглоомын симуляци үүсгэж, кибер халдлагын боломжит сценарийг урьдчилан үнэлснээр стратегийн эрсдэлийг бууруулахад тусалдаг. Иймээс тоглоомын онолын үүднээс хиймэл оюуныг ашиглах нь батлан хамгаалах салбарын кибер хамгаалалтыг илүү

стратеги суурьтай, дасан зохицох чадвартай, оновчтой шийдвэр гаргалт бүхий систем болгон хөгжүүлэх чухал арга зам юм.

Түүнчлэн байгууллагын тогтвортой байдлын онол нь кибер халдлага, техникийн саатал болон бусад эрсдэлийн үед байгууллага үйл ажиллагаагаа тасралтгүй үргэлжлүүлэх чадварыг тайлбарладаг. Батлан хамгаалах байгууллагын хувьд үйл ажиллагааны тасралтгүй байдал нь үндэсний аюулгүй байдлыг хангах гол нөхцөлүүдийн нэг бөгөөд кибер халдлагын дараах сэргэлт, нөөцлөлт, гамшгийн үеийн сэргээн босголтын төлөвлөгөө боловсруулахад энэхүү онол чухал үүрэг гүйцэтгэдэг байна.

Батлан хамгаалах салбарын кибер аюулгүй байдлыг байгууллагын тогтвортой байдлын онолын үүднээс авч үзвэл хиймэл оюун нь тасралтгүй ажиллагаа, дасан зохицох чадвар болон алдаа тэсвэрлэх чадамжийг хангахад чухал үүрэгтэй. Тогтвортой байдлын онолд тулгуурлан байгууллага нь гадны болон дотоод шок, тухайлбал кибер халдлага, системийн доголдол зэрэгт өртсөн ч үндсэн үйл ажиллагаагаа хадгалах чадвартай байх ёстой бөгөөд хиймэл оюун нь ийм нөхцөлд эрсдэлийг эрт илрүүлж, системийн сул талыг бодит цагт тодорхойлох боломжийг бүрдүүлдэг (Linkov 2013).

Мөн машин сургалтын алгоритмууд нь хэвийн үйл ажиллагааны суурь загварыг тодорхойлж, гажуудлыг илрүүлэх замаар системийн сэргээгдэх чадварыг (recovery capability) нэмэгдүүлдэг. Үүнээс гадна хиймэл оюун нь автоматжуулсан хариу арга хэмжээ болон SOAR системүүдтэй уялдан ажилласнаар халдлагын үед шийдвэр гаргалтын хугацааг бууруулж, үйл ажиллагааны тасралтгүй байдлыг хангахад тусалдаг. Иймээс байгууллагын тогтвортой байдлын онолын хүрээнд хиймэл оюуныг ашиглах нь батлан хамгаалах салбарын кибер хамгаалалтыг илүү уян хатан, сэргээгдэх чадвартай, тасралтгүй ажиллагаатай систем болгон хөгжүүлэх үндсэн арга зам юм.

Иймээс батлан хамгаалах байгууллагын кибер аюулгүй байдлын судалгаанд эдгээр онолуудыг дангаар нь бус харилцан уялдуулан ашиглах нь илүү үр дүнтэй байдаг. Эрсдэлийн удирдлагын онол нь эрсдэлийг тодорхойлж үнэлэх үндэс болдог бол системийн онол нь байгууллагыг бүхэлд нь ойлгох боломжийг бүрдүүлдэг.

Харин мэдээллийн аюулгүй байдлын архитектурын онол нь хамгаалалтын техникийн шийдлийг тодорхойлж, тоглоомын онол нь халдагч болон хамгаалагчийн стратегийн харилцааг тайлбарладаг. Үүний зэрэгцээ байгууллагын тогтвортой байдлын онол нь аливаа кибер эрсдэл үүссэн нөхцөлд байгууллагын үйл ажиллагааг тасралтгүй хадгалах арга замыг тодорхойлдог.

Иймээс эдгээр онолууд нь батлан хамгаалах байгууллагын кибер аюулгүй байдлын онолын үндсийг бүрдүүлж, мэдээллийн нууцлал, системийн хамгаалалт болон үйл ажиллагааны тогтвортой байдлыг хангах асуудлыг цогц байдлаар судлах боломжийг олгодог.

Орчин үеийн халдлагууд улам бүр автоматжиж, олон үе шаттай болж байгаа тул зөвхөн дүрэмд суурилсан хамгаалалт хангалтгүй болсон. Энэ нь хиймэл оюунд суурилсан хамгаалалтын системийг хөгжүүлэх онолын үндэслэлийг бүрдүүлж байна.

Хоёр. Хиймэл оюунд суурилан кибер аюулгүй байдлыг хамгаалах нь

Хиймэл оюун нь машин сургалт (Machine Learning), гүн сургалт (Deep Learning), мэдрэлийн сүлжээ (Neural Network), байгалийн хэл боловсруулах технологи (Natural Language Processing) зэрэг арга технологид тулгуурлан өгөгдлөөс суралцах боломжийг олгодог (Russell, S., Norvig, P 2021).

Кибер хамгаалалтын салбарт хиймэл оюуныг дараах чиглэлээр өргөн ашиглаж байна. Үүнд:

- Халдлагын хэв шинж илрүүлэх;
- Сүлжээний хэвийн бус үйл ажиллагааг тодорхойлох;
- Хортой кодыг ангилах;
- Эрсдэлийн урьдчилсан таамаглал хийх;
- Автомат хариу арга хэмжээ боловсруулах;
- Тагнуулын мэдээлэл боловсруулах зэрэг юм.

Батлан хамгаалах салбарын кибер аюулгүй байдлыг хангах хүрээнд хиймэл оюун нь халдлагын хэв шинжийг илрүүлэхэд чухал үүрэг гүйцэтгэдэг. Хиймэл оюунд суурилсан системүүд нь сүлжээний урсгал, хэрэглэгчийн үйл ажиллагаа, төхөөрөмжүүдийн харилцаа холбоо болон өмнөх халдлагын өгөгдлийг боловсруулж, кибер халдлагын нийтлэг болон нарийн төвөгтэй хэв маягийг тодорхойлдог (Buczak, A. L., Guven, E 2016).

Машин сургалтын алгоритмууд нь их хэмжээний өгөгдлөөс давтагдах шинж тэмдэг, зан төлөвийн өөрчлөлт болон сэжигтэй үйл ажиллагааг илрүүлснээр халдлагын эхний үе шатыг таних боломжийг олгодог. Батлан хамгаалах байгууллагууд энэхүү технологийг ашиглан дэвшилтэт тогтвортой заналхийлэл (APT), тархмал үйлчилгээ саатуулах халдлага (DDoS) болон зөвшөөрөлгүй нэвтрэх оролдлогыг илүү үр дүнтэй илрүүлдэг. Ялангуяа гүн сургалтын загварууд нь олон эх сурвалжаас ирсэн өгөгдлийн уялдаа холбоог шинжилж, хүний нүдэнд шууд харагдахгүй хэв шинжийг тодорхойлох чадвартай байдаг (Shone, N., Ngoc, T. N., Phai, V. D., Shi, Q 2018). Энэ нь халдлагыг эрт үед нь илрүүлж, хамгаалалтын хариу арга хэмжээг шуурхай хэрэгжүүлэх нөхцөлийг бүрдүүлдэг. Гэсэн хэдий ч хиймэл оюуны системийн үр ашиг нь сургалтын өгөгдлийн чанар, худал эерэг дохиоллын түвшин болон шинэ төрлийн халдлагыг таних чадвараас ихээхэн хамаардаг. Иймээс хиймэл оюунд суурилсан халдлагын хэв шинж илрүүлэх аргыг хүний шинжээчдийн дүн шинжилгээтэй хослуулан ашиглах нь батлан хамгаалах салбарын кибер хамгаалалтыг бэхжүүлэх үр дүнтэй арга зам болдог.

Батлан хамгаалах салбарын кибер аюулгүй байдлын хүрээнд хиймэл оюун нь сүлжээний хэвийн бус үйл ажиллагааг тодорхойлох гол технологийн нэг болж хөгжиж байна. Хиймэл оюунд суурилсан системүүд нь сүлжээний урсгалын өгөгдөл, протоколын лог, хэрэглэгчийн зан төлөв болон төхөөрөмж хоорондын харилцааны хэв маягийг тасралтгүй шинжилж, “хэвийн” ажиллагааны суурь загварыг бий болгодог (Chandola, V., Banerjee, A., Kumar, V 2009). Энэхүү суурь загвараас хазайсан үйлдлийг статистик болон машин сургалтын аргаар илрүүлснээр зөвшөөрөлгүй нэвтрэлт, тагнуулын шинжтэй үйл ажиллагаа болон халдлагын эхний үе шатыг эрт таних боломж бүрддэг. Ялангуяа хяналтгүй болон хагас хяналттай сургалтын алгоритмууд нь урьдчилан тодорхойлогдоогүй шинэ төрлийн кибер аюулыг илрүүлэхэд өндөр үр дүнтэй байдаг (Sommer, R., Paxson,

V 2010). Батлан хамгаалах байгууллагууд энэхүү технологийг ашиглан стратегийн чухал сүлжээнүүдийн бодит цагийн хяналтыг сайжруулж, халдлагын тархалтыг хязгаарлах боломжтой болдог. Мөн гүн сургалтын загварууд нь олон хэмжээст өгөгдлөөс далд хамаарлыг илрүүлснээр илүү нарийн төвөгтэй аномалиудыг тодорхойлох чадварыг нэмэгдүүлдэг (Javaid, A., Niyaz, Q., Sun, W., Alam, M 2016). Гэсэн хэдий ч худал эерэг дохиолол, өгөгдлийн тэнцвэргүй байдал болон загварын тайлбарлах боломжийн хязгаарлалт нь практик хэрэгжилтийн гол сорилт хэвээр байна. Иймээс хиймэл оюунд суурилсан аномали илрүүлэлтийг хүний шинжээчдийн дүн шинжилгээ болон уламжлалт хамгаалалтын системтэй хослуулан ашиглах нь батлан хамгаалах салбарын кибер хамгаалалтыг илүү найдвартай болгох үндсэн арга зам гэж үздэг.

Батлан хамгаалах салбарын кибер аюулгүй байдлын хүрээнд хиймэл оюун нь хортой кодыг ангилах үйл явцыг автоматжуулах, илрүүлэх хурд болон нарийвчлалыг нэмэгдүүлэхэд чухал үүрэгтэй. Хиймэл оюун д суурилсан ангилалтын системүүд нь файл, программын статик шинж чанар (кодын бүтэц, API дуудлага, байт түвшний загвар) болон динамик зан төлөвийг (ажиллах үеийн сүлжээний үйл ажиллагаа, системийн өөрчлөлт) зэрэг олон эх сурвалжийн өгөгдөл дээр үндэслэн шинжилгээ хийдэг (Souri, A., Hosseini, R 2018). Машин сургалтын алгоритмууд нь ransomware, trojan, spyware зэрэг хортой кодын төрөл хоорондын ялгааг суралцаж, шинэ болон өөрчлөгдсөн хувилбаруудыг ч мөн таних боломжийг бүрдүүлдэг. Ялангуяа гүн сургалтын аргууд нь гар аргаар онцлог тодорхойлох шаардлагагүйгээр өгөгдлөөс автоматаар шинж тэмдэг ялган авч ангиллын гүйцэтгэлийг сайжруулдаг (Yuan, Z., Lu, Y., Wang, Z., Xue, Y 2014). Батлан хамгаалах байгууллагууд энэхүү технологийг ашиглан стратегийн системүүдийг чиглэсэн нарийн төвөгтэй хортой кодын халдлагыг эрт илрүүлэх, тусгаарлах боломжтой болдог. Мөн хиймэл оюунд суурилсан системүүд нь асар их хэмжээний кибер тагнуулын өгөгдлийг бодит цаг хугацаанд боловсруулах чадвартай тул хамгаалалтын шийдвэр гаргалтыг түргэсгэдэг. Гэсэн хэдий ч сургалтын өгөгдлийн чанар, дайсагнасан халдлагад өртөх эрсдэл болон загварын тайлбарлах боломжийн хязгаарлалт нь практик хэрэгжилтийн гол сорилт хэвээр байна. Иймээс хортой кодын ангилалд хиймэл оюуныг уламжлалт гарын үсэгт суурилсан арга болон хүний шинжээчдийн хяналттай хослуулах нь батлан хамгаалах салбарын кибер хамгаалалтыг илүү найдвартай болгох үндсэн стратеги юм.

Батлан хамгаалах салбарын кибер аюулгүй байдлыг хангах хүрээнд хиймэл оюун нь эрсдэлийн урьдчилсан таамаглал хийхэд стратегийн ач холбогдолтой технологи болж байна. Хиймэл оюун нь сүлжээний бүртгэл, халдлагын түүхэн өгөгдөл, аюул заналын тагнуулын мэдээлэл болон системийн үйл ажиллагааны үзүүлэлтүүдийг шинжилж, болзошгүй кибер эрсдэлийг урьдчилан тодорхойлох боломжийг олгодог (Buczak, A. L., Guven, E 2016). Машин сургалтын алгоритмууд нь халдлагын хэв шинж, эмзэг байдлын давтамж болон хэрэглэгчийн зан төлөвийн өөрчлөлтийг илрүүлснээр ирээдүйд үүсэж болзошгүй аюулын магадлалыг тооцоолдог. Батлан хамгаалах байгууллагууд энэхүү чадварыг ашиглан чухал дэд бүтэц, цэргийн холбооны систем болон мэдээллийн сүлжээнд чиглэсэн халдлагын эрсдэлийг эрт үе шатанд үнэлэх боломжтой байдаг. Үүнээс гадна хиймэл оюун нь олон төрлийн өгөгдлийг нэгтгэн боловсруулснаар эрсдэлийн үнэлгээний

нарийвчлалыг нэмэгдүүлж, шийдвэр гаргагчдад урьдчилан сэргийлэх арга хэмжээ төлөвлөхөд дэмжлэг үзүүлдэг (Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., Ng, A 2020). Энэхүү хандлага нь хамгаалалтын нөөцийг оновчтой хуваарилах, хариу арга хэмжээний хугацааг богиносгох, үндэсний аюулгүй байдлын тогтвортой байдлыг хангахад чухал үүрэгтэй. Гэсэн хэдий ч таамаглалын загварын үнэн зөв байдал нь сургалтын өгөгдлийн чанар, алгоритмын ил тод байдал болон шинэ төрлийн халдлагад дасан зохицох чадвараас ихээхэн хамаардаг. Иймээс хиймэл оюунд суурилсан эрсдэлийн урьдчилсан таамаглалыг хүний шинжээчдийн үнэлгээтэй хослуулан ашиглах нь батлан хамгаалах салбарын кибер аюулгүй байдлыг бэхжүүлэх хамгийн үр дүнтэй арга замын нэг гэж үздэг.

Батлан хамгаалах салбарын кибер аюулгүй байдлын хүрээнд хиймэл оюун нь автомат хариу арга хэмжээ боловсруулах, хэрэгжүүлэх үйл явцыг эрс хурдасгах стратегийн чухал технологи болж байна. Хиймэл оюунд суурилсан системүүд нь сүлжээний урсгал, халдлагын илрүүлэлтийн дохио, лог файл болон аюул заналын тагнуулын мэдээллийг нэгтгэн дүн шинжилгээ хийж, бодит цагийн нөхцөлд хамгийн оновчтой хариу арга хэмжээг санал болгодог (Brumaghin, E., et al 2019). Машин сургалтын загварууд нь өмнөх кибер халдлагын шийдвэрлэсэн кейсүүдээс суралцаж, ижил төстэй нөхцөлд автоматаар тохирох хамгаалалтын протоколыг сонгох чадвартай байдаг. Үүнд сүлжээний сегментчлэл хийх, халдварлагдсан төхөөрөмжийг тусгаарлах, хортой урсгалыг хаах зэрэг үйлдлүүд багтдаг бөгөөд эдгээр нь хүний оролцоогүйгээр гүйцэтгэгдэх боломжтой. Батлан хамгаалах байгууллагууд энэхүү технологийг ашигласнаар хариу үйлдлийн хугацааг богиносгож, стратегийн чухал системүүдийн тасралтгүй ажиллагааг хангах боломжтой болдог. Мөн гүн сургалтын аргууд нь олон эх сурвалжийн өгөгдлөөс нөхцөл байдлыг ойлгож, илүү нарийн төвөгтэй халдлагад тохирсон хариу арга хэмжээг оновчтой тодорхойлдог (Moustafa, N., Creech, G., Sitnikova, E 2019). Гэсэн хэдий ч автомат шийдвэр гаргалтын систем нь буруу ангилал хийх, дайсагнасан довтолгоонд өртөх болон ил тод байдлын дутагдал зэрэг эрсдэлтэй тул хүний хяналт зайлшгүй шаардлагатай хэвээр байна. Иймээс хиймэл оюунд суурилсан автомат хариу арга хэмжээг хүний шинжээчдийн удирдлага болон уламжлалт аюулгүй байдлын дэд бүтэцтэй хослуулах нь батлан хамгаалах салбарын кибер хамгаалалтын хамгийн үр дүнтэй загвар гэж үздэг.

Батлан хамгаалах салбарын кибер аюулгүй байдлын хүрээнд хиймэл оюун нь тагнуулын мэдээллийг боловсруулах, нэгтгэх болон дүн шинжилгээ хийх үйл явцыг ихээхэн сайжруулж байна. Хиймэл оюунд суурилсан системүүд нь олон эх сурвалжаас ирэх бүтэцтэй болон бүтэцгүй өгөгдөл, тухайлбал сүлжээний лог, аюул заналын тагнуулын мэдээллийн сан, нээлттэй эх сурвалжийн мэдээлэл (OSINT) зэргийг нэгтгэн боловсруулж, утга агуулгын уялдаа холбоог илрүүлдэг (Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., Ng, A 2020). Машин сургалтын алгоритмууд нь их хэмжээний өгөгдлөөс хэв шинж, давтагдах зан төлөв болон сэжигтэй холбоосуудыг тодорхойлсноор кибер аюул заналын нөхцөл байдлыг илүү нарийвчлалтай үнэлэх боломжийг бүрдүүлдэг. Батлан хамгаалах байгууллагууд энэхүү технологийг ашиглан дайсны кибер чадавх, халдлагын чиг хандлага болон эмзэг байдлын хандлагыг урьдчилан тодорхойлох боломжтой болдог. Ялангуяа байгалийн хэл боловсруулалт (NLP)-д суурилсан аргачлалууд

нь текстэн тагнуулын мэдээллээс утга агуулга, нэр бүхий объект, холбоосуудыг автоматаар ялган авч анализ хийхэд чухал үүрэгтэй (Buczak, A. L., Guven, E 2016). Энэ нь шийдвэр гаргагчдад бодит цагийн нөхцөл байдлын зураглал (situational awareness) бүрдүүлэхэд тусалдаг. Гэсэн хэдий ч мэдээллийн буруу тайлбар, өгөгдлийн чанарын асуудал болон дайсагнасан мэдээллийн нөлөөлөл нь хиймэл оюунд суурилсан тагнуулын боловсруулалтын найдвартай байдалд эрсдэл учруулдаг.

Иймээс хиймэл оюуныг хүний тагнуулын шинжээчдийн дүн шинжилгээтэй хослуулах нь батлан хамгаалах салбарын кибер тагнуулын үр нөлөөг хамгийн өндөр түвшинд хүргэх үндсэн арга зам юм.

Машин сургалтын алгоритмууд нь асар их хэмжээний мэдээлэл болон сүлжээний урсгалын өгөгдлийг боловсруулж, хүний оролцоогүйгээр хэвийн бус үйлдлийг илрүүлэх боломжтой байдаг (Goodfellow, I., Bengio, Y., Courville, A 2016). Ялангуяа гүн сургалтын аргууд нь өмнө нь бүртгэгдээгүй шинэ төрлийн халдлагыг илрүүлэхэд өндөр үр ашигтай болохыг судалгаанууд харуулж байна.

Гурав. Монгол Улсын батлан хамгаалах салбарт ашиглагдах хиймэл оюунд суурилсан хамгаалалтын загвар боловсруулах арга зүй

Батлан хамгаалах байгууллагын мэдээллийн систем нь иргэний байгууллагын системээс хэд хэдэн онцлогоор ялгаатай байдаг. Үүнд:

Нэгдүгээрт, мэдээллийн ангилал өндөр байдаг. Нууц болон онц нууц мэдээллийн урсгал нь хамгаалалтын тусгай шаардлага үүсгэдэг.

Хоёрдугаарт, команд удирдлагын системүүд бодит хугацаанд ажилладаг тул системийн саатал нь байлдааны бэлэн байдалд шууд нөлөөлдөг.

Гуравдугаарт, гибрид дайны нөхцөлд кибер халдлага нь уламжлалт цэргийн ажиллагаатай уялдан хэрэгжих хандлагатай байдаг (Singer, P. W., Friedman, A 2014).

Дөрөвдүгээрт, Аливаа улсын Засгийн газрын санхүүжилттэй кибер халдагч бүлгүүд өндөр түвшний техникийн чадавхтай байдаг тул хамгаалалтын системүүд урьдчилан таамаглах, суралцах чадвартай байх шаардлагатай.

Эндээс үзэхэд батлан хамгаалах байгууллагын мэдээллийн систем нь иргэний системтэй харьцуулахад илүү өндөр ангиллын нууцлал, бодит цагийн ажиллагаа болон гибрид дайны нөхцөлтэй уялдсан аюулын орчинд ажилладаг тул хамгаалалтын шаардлага нь илүү нарийн төвөгтэй байдаг.

Түүнчлэн аливаа улсын Засгийн газрын санхүүжилттэй өндөр чадвартай халдагч бүлгүүдийн эсрэг үр дүнтэй хамгаалалт бий болгохын тулд системүүд нь урьдчилан таамаглах болон тасралтгүй суралцах чадвартай байх шаардлагатай. Иймээс батлан хамгаалах салбарын кибер аюулгүй байдал нь уламжлалт хамгаалалтын аргаас илүү дасан зохицох, ухаалаг шийдэл шаардсан өндөр түвшний орчин болж байна.

Монгол Улсын батлан хамгаалах салбарын кибер хамгаалалтын хиймэл оюунд суурилсан загвар боловсруулахдаа системийн хандлага болон эрсдэлийн удирдлагын аргачлалыг хослуулах шаардлагатай. Судалгааны арга зүйн хувьд дараах үе шатыг санал болгож болно.

Хүснэгт 2. *Монгол Улсын батлан хамгаалах салбарын кибер хамгаалалтын*

хиймэл оюунд суурилсан загвар боловсруулах үе шат

Үе шат	**Гол зорилго**	**Хийх үйл ажиллагаа**	**Ашиглах стандарт / технологи**
Нэгдүгээр үе шат: Эрсдэлийн үнэлгээ	Батлан хамгаалах салбарын кибер эрсдэлийг тодорхойлох, эрэмбэлэх	Мэдээллийн хөрөнгө, мэдээллийн урсгал, сүлжээний бүтэц, эмзэг байдлыг тодорхойлох; өндөр эрсдэлтэй хэсгүүдийг илрүүлэх	ISO/IEC 27005 стандарт
Хоёрдугаар үе шат: Өгөгдөл цуглуулах ба боловсруулах	AI загварын сургалтын чанартай өгөгдлийн суурь бүрдүүлэх	Сүлжээний лог, халдлагын бүртгэл, системийн үйл ажиллагаа, хэрэглэгчийн зан төлөвийн өгөгдлийг нэгтгэж боловсруулах	Өгөгдөл нэгтгэх, цэвэршүүлэх, боловсруулалтын аргачлалууд
Гуравдугаар үе шат: Машин сургалтын загвар боловсруулах	Халдлагын илрүүлэлтийн ухаалаг загвар хөгжүүлэх	Супервизортой ба супервизоргүй сургалт ашиглах; ангилалт ба илрүүлэлтийн загвар боловсруулах	Random Forest, SVM, XGBoost, CNN, RNN
Дөрөвдүгээр үе шат: Бодит хугацааны хяналтын систем	Кибер орчныг тасралтгүй хянах, нөхцөл байдлыг үнэлэх	SIEM платформыг AI хөдөлгүүртэй нэгтгэн бодит цагийн мониторинг хийх	Security Information and Event Management (SIEM)
Тавдугаар үе шат: Автомат хариу арга хэмжээ	Кибер халдлагад шуурхай, автомат хариу үзүүлэх	Илэрсэн халдлагад үндэслэн хамгаалалтын үйлдлийг автоматаар хэрэгжүүлэх	Security Orchestration, Automation and Response (SOAR)

Дээрх хүснэгтээс үзэхэд Монгол Улсын батлан хамгаалах салбарын кибер хамгаалалтын хиймэл оюунд суурилсан загвар боловсруулах нь олон үе шаттай, хоорондоо уялдаа бүхий цогц арга зүйгээр хэрэгжих шаардлагатай.

Эхний шатанд ISO/IEC 27005 стандартад үндэслэн эрсдэлийн үнэлгээ хийж, мэдээллийн хөрөнгө, сүлжээний бүтэц, мэдээллийн урсгал болон эмзэг байдлыг тодорхойлсноор хамгийн өндөр эрсдэлтэй хэсгүүдийг илрүүлж, хамгаалалтын тэргүүлэх чиглэлийг тогтооно.

Дараагийн шатанд хиймэл оюуны загварын үндэс болох өгөгдлийг бүрдүүлэхийн тулд сүлжээний лог, халдлагын бүртгэл, системийн үйл ажиллагааны мэдээлэл болон хэрэглэгчийн зан төлөвийн өгөгдлийг нэгтгэн цуглуулж, боловсруулснаар чанартай сургалтын өгөгдлийн суурь бий болгоно. Үүний дараа машин сургалтын үе шатанд супервизортой болон супервизоргүй сургалтын аргуудыг ашиглан Random Forest, Support Vector Machine, XGBoost, Convolutional Neural Network болон Recurrent Neural Network зэрэг алгоритмуудад тулгуурлан халдлагыг илрүүлэх, ангилах ухаалаг загвар боловсруулна.

Энэ загвар нь сүлжээний хэвийн болон хэвийн бус үйл ажиллагааг ялган

таних замаар кибер халдлагыг эрт илрүүлэх боломжийг бүрдүүлдэг. Цаашлаад “Аюулгүй байдлын мэдээлэл ба үйл явдлын менежмент (Security Information and Event Management, SIEM)”-ийн платформтой хиймэл оюуныг нэгтгэснээр бодит цагийн хяналт, нөхцөл байдлын дүн шинжилгээ хийх дэвшилтэт орчин бүрдэж, сүлжээний аюулгүй байдлыг тасралтгүй хянах нөхцөл бүрдэнэ.

Эцсийн шатанд “Аюулгүй байдлын уялдуулалт, автоматжуулалт ба хариу арга хэмжээ (Security Orchestration, Automation and Response, SOAR)” технологийг ашиглан илэрсэн аюулд автомат хариу арга хэмжээ авах механизмыг хөгжүүлснээр халдлагын эсрэг шуурхай, үр дүнтэй хамгаалалт хэрэгжих боломжтой болно. Ийнхүү бүх үе шат нь хоорондоо уялдаа холбоотой ажилласнаар батлан хамгаалах салбарын кибер хамгаалалтын тогтолцоо нь илүү ухаалаг, дасан зохицох чадвартай, өндөр үр ашигтай систем болон хөгжих үндэс бүрдэх боломжтой болох нь харагдаж байна.

Орчин үеийн батлан хамгаалах салбарын кибер аюулгүй байдал нь зөвхөн хамгаалалтын програм хангамж ашиглах асуудлаас давж, хиймэл оюунд суурилсан ухаалаг хамгаалалтын экосистемийг хөгжүүлэх түвшинд хүрч байна. Монгол Улсын батлан хамгаалах салбарын хувьд хиймэл оюунд суурилсан хамгаалалтын загвар боловсруулах нь үндэсний аюулгүй байдлыг бэхжүүлэх, кибер халдлагын эрсдэлийг бууруулах, мэдээллийн дэд бүтцийн тогтвортой байдлыг хангах стратегийн ач холбогдолтой юм. Монгол Улсын батлан хамгаалах салбарт хэрэгжүүлэх хиймэл оюунд суурилсан хамгаалалтын загвар нь дараах үндсэн бүрэлдэхүүнтэй байна. Үүнд:

- Өгөгдөл цуглуулах давхарга;
- Аюул заналын тагнуулын сан;
- Машин сургалтын аналитик хэсэг;
- Эрсдэлийн үнэлгээний модуль;
- Автомат хамгаалалтын шийдвэр гаргалтын систем;
- “Аюулгүй байдлын уялдуулалт, автоматжуулалт ба хариу арга хэмжээ (Security Orchestration, Automation and Response, SOAR)”-ний платформ;
- Стратегийн удирдлагын самбар зэрэг болно.

Энэхүү архитектур нь тасралтгүй суралцах чадвартай байж, шинэ халдлагын хэв маяг илэрсэн үед хамгаалалтын дүрмээ автоматаар шинэчилдэг байх шаардлагатай.

Хүснэгт 3. *Монгол Улсын батлан хамгаалах салбарт хэрэгжүүлэх хиймэл оюунд суурилсан хамгаалалтын загварын бүтэцчилсэн байдал*

№	Бүрэлдэхүүн хэсэг	Гол үүрэг / зорилго
1	Өгөгдөл цуглуулах давхарга	Сүлжээний лог, системийн үйл ажиллагаа, хэрэглэгчийн зан төлөв болон бусад кибер өгөгдлийг цуглуулж төвлөрүүлнэ.
2	Аюул заналын тагнуулын сан	Дотоод болон гадаад кибер аюулын мэдээллийг нэгтгэж, шинэ заналхийллийг таних суурь мэдээллийн сан бүрдүүлнэ.

3	Машин сургалтын аналитик хэсэг	Цуглуулсан өгөгдөлд анализ хийж, халдлагын хэв шинж, аномали болон ангиллыг тодорхойлно.
4	Эрсдэлийн үнэлгээний модуль	Системийн эмзэг байдал болон кибер эрсдэлийн түвшнийг үнэлж, тэргүүлэх хамгаалалтын чиглэлийг тодорхойлно.
5	Автомат хамгаалалтын шийдвэр гаргалтын систем	Илэрсэн аюулд үндэслэн шуурхай хамгаалалтын арга хэмжээ (тусгаарлалт, хаалт гэх мэт) автоматаар хэрэгжүүлнэ.
6	“Аюулгүй байдлын уялдуулалт, автоматжуулалт ба хариу арга хэмжээ (SOAR)”-ний платформ	“Аюулгүй байдлын уялдуулалт, автоматжуулалт ба хариу арга хэмжээ (Security Orchestration, Automation and Response)” ашиглан хамгаалалтын үйл явцыг уялдуулж, автоматжуулсан хариу үйлдлийг зохион байгуулна.
7	Стратегийн удирдлагын самбар	Кибер нөхцөл байдлын ерөнхий дүр зургийг харуулж, шийдвэр гаргалтыг дэмжих визуал хяналтын системийг бүрдүүлнэ.

Монгол Улсын батлан хамгаалах салбарт хэрэгжүүлэх хиймэл оюунд суурилсан кибер хамгаалалтын загвар нь олон давхаргат, хоорондоо уялдаа бүхий цогц архитектур хэлбэртэй байна.

Энэхүү загварын үндсэн суурь нь сүлжээний лог, системийн үйл ажиллагаа болон хэрэглэгчийн зан төлөв зэрэг олон төрлийн өгөгдлийг төвлөрүүлэн боловсруулах өгөгдөл цуглуулах давхарга бөгөөд үүн дээр тулгуурлан кибер орчны бодит нөхцөл байдлыг тодорхойлдог. Цуглуулсан мэдээллийг аюул заналын тагнуулын сантай нэгтгэснээр шинэ болон хөгжиж буй кибер аюулын талаар илүү өргөн хүрээний ойлголт бий болгоно.

Үүний дараа машин сургалтын аналитик хэсэг нь өгөгдөлд дүн шинжилгээ хийж, халдлагын хэв шинж болон аномали илрүүлэх үндсэн үүргийг гүйцэтгэнэ. Эрсдэлийн үнэлгээний модуль нь илэрсэн мэдээлэлд үндэслэн системийн эмзэг байдлыг тодорхойлж, хамгаалалтын тэргүүлэх чиглэлийг тогтоох боломж олгоно. Харин автомат хамгаалалтын шийдвэр гаргалтын систем нь эдгээр шинжилгээний үр дүнг ашиглан халдлагад шуурхай хариу арга хэмжээ авч, хамгаалалтын үйл ажиллагааг хүний оролцоогүйгээр хэрэгжүүлэх нөхцөлийг бүрдүүлнэ. Энэхүү бүх процессыг “Аюулгүй байдлын уялдуулалт, автоматжуулалт ба хариу арга хэмжээ (SOAR)”-ний платформ уялдуулан зохион байгуулж, хамгаалалтын үйл ажиллагааг автоматжуулсан нэгтгэлтэй систем болгон хувиргана. Эцэст нь стратегийн удирдлагын самбар нь кибер аюулгүй байдлын нөхцөл байдлыг нэгтгэн харуулж, шийдвэр гаргалтыг дэмжих бодит цагийн хяналт, дүн шинжилгээний орчныг бүрдүүлнэ. Ийнхүү эдгээр бүрэлдэхүүн хэсгүүд нь хоорондоо уялдаа холбоотой ажилласнаар систем нь тасралтгүй суралцах чадвартай, шинэ халдлагын хэв маягт дасан зохицдог ухаалаг кибер хамгаалалтын архитектур болж хөгжих боломжтой юм.

Дүгнэлт

Дижитал шилжилт, сүлжээ төвтэй үйл ажиллагаа болон мэдээллийн дэд бүтцийн хамаарал өсөн нэмэгдэж буй өнөө үед батлан хамгаалах салбарын кибер

аюулгүй байдал нь үндэсний аюулгүй байдлын тэргүүлэх чиглэлийн нэг болж байна. Орчин үеийн кибер халдлагуудын нарийн төвөгтэй байдал, автоматжсан шинж чанар нь уламжлалт хамгаалалтын арга хэрэгслийн үр нөлөөг хязгаарлаж байгаа тул хиймэл оюунд суурилсан хамгаалалтын шинэ хандлага шаардлагатай болж байна. Энэхүү өгүүллээр батлан хамгаалах салбарын кибер хамгаалалтын тогтолцоонд хиймэл оюуныг ашиглах онол, арга зүйн үндсийг тодорхойлох оролдлого хийлээ.

Өгүүллийн хүрээнд эрсдэлийн удирдлагын онол, системийн онол, мэдээллийн аюулгүй байдлын архитектурын онол, тоглоомын онол болон байгууллагын тогтвортой байдлын онолуудыг кибер хамгаалалтын судалгааны онолын суурь болгон авч үзсэн. Эдгээр онолууд нь кибер эрсдэлийг үнэлэх, хамгаалалтын архитектурыг төлөвлөх, халдагч болон хамгаалагчийн стратегийн харилцааг тодорхойлох, байгууллагын тасралтгүй ажиллагааг хангах боломжийг бүрдүүлдэг болохыг тогтоов. Мөн хиймэл оюуны технологиудыг халдлагын хэв шинж илрүүлэх, аномали тодорхойлох, хортой код ангилах, эрсдэлийг урьдчилан таамаглах, автомат хариу арга хэмжээ хэрэгжүүлэх болон аюул заналын тагнуулын мэдээлэл боловсруулах чиглэлээр ашиглах боломжийг судлав. Судалгааны үр дүнгээс үзэхэд хиймэл оюун нь кибер халдлагыг эрт илрүүлэх, хамгаалалтын үйл ажиллагааны хурдыг нэмэгдүүлэх, шийдвэр гаргалтын чанарыг сайжруулах чадавхтай байна.

Монгол Улсын батлан хамгаалах салбарын онцлог нь өндөр түвшний мэдээллийн ангилал, бодит цагийн ажиллагаа болон гибрид аюулын орчинтой холбоотой тул хамгаалалтын тогтолцоо нь тасралтгүй суралцах, дасан зохицох чадвартай байх шаардлагатай байна. Иймээс тухайн өгүүлэлд эрсдэлийн үнэлгээ, өгөгдөл боловсруулах, машин сургалтын загвар хөгжүүлэх, бодит цагийн хяналт болон автомат хариу арга хэмжээ гэсэн үе шат бүхий арга зүйг санал болгосон. Түүнчлэн өгөгдөл цуглуулах давхарга, аюул заналын тагнуулын сан, машин сургалтын аналитик хэсэг, эрсдэлийн үнэлгээний модуль, автомат шийдвэр гаргалтын систем, “Аюулгүй байдлын уялдуулалт, автоматжуулалт ба хариу арга хэмжээ (SOAR)”-ний платформ болон стратегийн удирдлагын самбараас бүрдэх архитектурын загварыг боловсруулла. Энэхүү архитектур нь олон эх сурвалжийн өгөгдлийг нэгтгэн боловсруулах, нөхцөл байдлын бодит цагийн зураглал бий болгох, хамгаалалтын үйл ажиллагааг автоматжуулах боломжийг бүрдүүлнэ. Мөн шинэ төрлийн халдлагын хэв шинжийг тасралтгүй суралцан таних замаар хамгаалалтын үр нөлөөг сайжруулах нөхцөл бүрдэнэ. Гэсэн хэдий ч хиймэл оюунд суурилсан системүүд нь сургалтын өгөгдлийн чанар, тайлбарлах боломж, худал эерэг дохиолол болон дайсагнасан халдлагад өртөх эрсдэл зэрэг тодорхой хязгаарлалтуудтай хэвээр байна. Иймээс эдгээр системийг хүний шинжээчдийн хяналт, үнэлгээтэй уялдуулан ашиглах шаардлагатай юм. Эцэст нь энэхүү судалгаанд санал болгосон хиймэл оюунд суурилсан кибер хамгаалалтын загвар нь Монгол Улсын батлан хамгаалах салбарын кибер хамгаалалтын чадавхыг бэхжүүлэх, эрсдэлийг бууруулах, стратегийн шийдвэр гаргалтыг дэмжих онолын болон практик ач холбогдолтой гэж үзэж байна.

Эшлэл авсан сурвалж, судалгааны бүтээл:

1. Bertalanffy, L. von. 1968. *General system theory: Foundations, development, applications.* George Braziller.
2. Brumaghin, E., et al. 2019. *Automatic cyber defense systems and response orchestration in enterprise networks.* IEEE Security & Privacy Publications.
3. Buczak, A. L., Guven, E. 2016. “A survey of data mining and machine learning methods for cyber security intrusion detection, *https://doi.org/10.1109/COMST.2015.2494502*. *IEEE Communications Surveys & Tutorials, 18(2)* 1153–1176.
4. Chandola, V., Banerjee, A., Kumar, V. 2009. “Anomaly detection: A survey, https://doi.org/10.1145/1541880.1541882.” *ACM Computing Surveys, 41(3)* 1–58.
5. Craigen, D., Diakun-Thibault, N., Purse, R. 2014. Defining cybersecurity, *https://doi.org/10.22215/timreview/835*. *Technology Innovation Management Review, 4(10)* 13–21.
6. Goodfellow, I., Bengio, Y., Courville, A. 2016. *Deep learning.* MIT Press.
7. Javaid, A., Niyaz, Q., Sun, W., Alam, M. 2016. “A deep learning approach for network intrusion detection system” *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies* 21–26.
8. Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffran, J., Schreurs, M., Thiel-Clemen, T. 2013. “Changing the resilience paradigm, https://doi.org/10.1038/nclimate2227.” *Nature Climate Change, 4(6)* 407–429.
9. McGraw, G. 2006. *Software security: Building security in.* Addison-Wesley.
10. Moustafa, N., Creech, G., Sitnikova, E. 2019. “Learning-based models for automatic cyber defense and intrusion response, *https://doi.org/10.1109/ACCESS.2019.XXXXXXX*.” *IEEE Access, 7* 102-118.
11. National Institute of Standards and Technology. 2024. *Cybersecurity framework (CSF)* . 2.0, U.S. Department of Commerce.
12. National Institute of Standards and Technology. 2012. *Guide for conducting risk assessments, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.* (SP 800-30 Rev. 1), U.S. Department of Commerce.
13. Pita, J., Jain, M., Ordóñez, F., Tambe, M., et al. 2010. “Using game theory for real-world security problems.” *ACM Computing Surveys, 43(3)* 1–34.
14. Russell, S., Norvig, P. 2021. *Artificial intelligence: A modern approach (4th ed.).* Pearson.
15. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., Ng, A. 2020. “Cybersecurity data science: An overview from machine learning perspective, *https://doi.org/10.1186/s40537-020-00318-5*.” *Journal of Big Data, 7(1)* 41.
16. Shoham, Y., Leyton-Brown, K. 2009. *Multiagent systems: Algorithmic, game-theoretic, and logical foundations.* Cambridge: Cambridge University Press.

17. Shone, N., Ngoc, T. N., Phai, V. D., Shi, Q. 2018. “A deep learning approach to network intrusion detection, *https://doi.org/10.1109/TETCI.2017.2772792*.” *IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1)* 41–50.
18. Singer, P. W., Friedman, A. 2014. *Cybersecurity and cyberwar: What everyone needs to know.* Oxford: Oxford University Press.
19. Sommer, R., Paxson, V. 2010. “Outside the closed world: On using machine learning for network intrusion detection, *https://doi.org/10.1109/SP.2010.25*.” *2010 IEEE Symposium on Security and Privacy* 305–316.
20. Souri, A., Hosseini, R. 2018. “A state-of-the-art survey of malware detection approaches using data mining techniques, *https://doi.org/10.1186/s13673-018-0125-x*.” *Human-centric Computing and Information Sciences, 8(1)* 3-17.
21. Stallings, W. 2024. *Effective cybersecurity: A guide to using best practices and standards (2nd ed.).* Pearson.
22. —. 2018. *Effective cybersecurity: A guide to using best practices and standards.* . Addison-Wesley.
23. Whitman, M. E., Mattord, H. J. 2022. *Principles of information security (7th ed.).* Cengage Learning.
24. Yuan, Z., Lu, Y., Wang, Z., Xue, Y. 2014. “Droid-Sec: Deep learning in Android malware detection, *https://doi.org/10.1145/2666620.2666640.*” *Proceedings of the ACM SIGCOMM Workshop on Security and Privacy in Smartphones and Mobile Devices* 371–372.