

ЦАХИМ ГЭМТ ХЭРГЭЭС УРЬДЧИЛАН СЭРГИЙЛЭХ БОЛОМЖ: БАЙГАЛИЙН ХОВОР ЭЛЕМЕНТИЙН ХИЛИЙН ХЯНАЛТЫН ЖИШЭЭН ДЭЭР

А.Золбоо

*Хууль зүйн ухааны магистр,
Эдийн засгийн аюулгүй байдлын
магистрант*

Товч агуулга: Аж үйлдвэржилтийн 4 дүгээр хувьсгал буюу цахим технологийн үсрэнгүй хөгжлийн дижитал эрин үед бүхий л зүйлс техник, технологийн ажиллагаа дор өрнөж байна. Гаалийн хяналтын рентген төхөөрөмж, сканер нь улсын хилээр нэвтэрч буй импорт, экспортын бараа бүтээгдэхүүнийг шалгах чухал системүүдийн нэг бөгөөд эдгээр систем нь 100 хувь цахим технологид тулгуурласан байдаг. Түүнчлэн рентген төхөөрөмжийн хяналт нь хорт программын халдлагад өртөх эрсдэлтэй бөгөөд энэ нь хилийн аюулгүй байдал, эдийн засгийн аюулгүй байдлыг алдагдуулах эрсдэлийг дагуулдаг. Хорт программ нь мэдээллийг хулгайлах, хуурамч мэдээлэл илгээх, системийн ажиллагааг саатуулах зэрэг олон төрлийн аюулыг бий болгож байдаг бөгөөд энэхүү өгүүлэл нь цахим халдлагаас гаалийн хяналтын

рентген системийг хамгаалах боломж, мөн байгалийн ховор элементийн хууль бус эргэлтээс урьдчилан сэргийлэх технологийн шийдлүүдийг судалж, хорт программын халдлага, гэмт хэргээс сэргийлэх оновчтой арга хэмжээ авах боломжийг эрэлхийлэхэд чиглэсэн болно.

Түлхүүр үгс: Кибер аюулгүй байдал, Гаалийн хяналт, Рентген төхөөрөмж, Хорт программ, Цахим халдлага

Удиртгал

Хорт программ нь орчин үеийн мэдээллийн аюулгүй байдалд хамгийн том аюул заналхийлэл болж, жил ирэх тусам илүү нарийн, уламжлалт хамгаалалтын системүүдийг тойрон гарах шинэ арга замуудыг ашиглаж байна. 2023 оны кибер аюулгүй байдлын дэлхийн тайланд дурдсанаар хорт программын халдлагын тоо 38%-иар өссөн¹ нь мэдээллийн аюулгүй байдалд тулгарч буй асуудал, эрсдэлүүдийг улам тод томруун харуулж байна. Энэ нь хорт программын шинж чанар, түүнийг илрүүлэх болон шинжлэх үр дүнтэй аргачлалыг судлах шаардлагатайг онцолсон хэрэг юм.

Энэхүү судалгааны ажлын гол зорилго нь гаалийн хяналтын рентген төхөөрөмжийн цахим хяналтын системд учруулж

¹ F. Müller, "Machine Learning for Malware Detection," International Journal of Cybersecurity, vol. 14, no. 2, pp. 100-110, 2020.

болзошгүй хорт программын халдлагын аюулыг судалж, хилээр гарах байгалийн ховор элементийн хууль бус эргэлтээс урьдчилан сэргийлэх арга хэмжээг тодорхойлох явдал юм. Судалгаанд цахим халдлагаас хамгаалах хамгийн үр дүнтэй арга хэрэгслүүд, тэдгээрийн хэрхэн хэрэгжүүлж болох талаар судалж, гаалийн хяналтын системийн аюулгүй байдлыг сайжруулах, мөн хууль бус худалдааны эрсдэлээс урьдчилан сэргийлэх оновчтой шийдлүүдийг танилцуулах юм.

Энэхүү судалгааны зорилгыг хэрэгжүүлэхийн тулд дараах зорилтуудыг дэвшүүлсэн:

1. Хорт программын халдлагын төрөл, онцлогийг судлах.

2. Рентген хяналтын системийн аюулгүй байдлыг сайжруулах, хорт программыг илрүүлэх, шинжилгээ хийх аргуудыг судлах.

3. Байгалийн ховор элементийн хилээр гарч буй хууль бус эргэлтээс урьдчилан сэргийлэх арга хэмжээг санал болгох.

Судалгааны ажлын хүрээнд шинжлэх ухааны танин мэдэхүйн болон түүвэрлэх, харьцуулан судлах арга зүйг ашигласан бөгөөд хорт программын шинжилгээний аргуудыг харьцуулан дүн шинжилгээ хийсэн. Мөн судалгаанд шинжилгээний үр дүнг сайжруулахын тулд түүхэн болон

анализ, синтезийн аргуудыг ашигласан.

Энэхүү сэдвийн хүрээнд өмнө судлагдсан хэд хэдэн чухал судалгаа болон эрдэм шинжилгээний бүтээлүүд байдаг. Гаалийн хяналт, рентген төхөөрөмж, хорт программын халдлагаас урьдчилан сэргийлэх асуудал нь цахим аюулгүй байдал, хил хязгаарын хяналттай холбоотой өргөн хүрээний судалгаа юм. Тухайлбал:

1. Kaufman, L. (2021). "Cybersecurity in Border Control Technologies"

Энэхүү судалгаа нь хил хязгаарын хяналтын технологиудад ашиглагддаг цахим системүүдийн аюулгүй байдлыг судалсан бөгөөд хорт программын халдлагын эрсдэл болон түүний уршгийг шинжилжээ. Судалгааны үр дүнд хил хязгаарын хяналтын системийн хамгаалалтын аргачлалуудыг сайжруулах хэрэгцээ шаардлагыг дэвшүүлсэн.

2. Boulanger, R., & Li, X. (2020). "Impact of Malware on Border Control Systems"

Судалгаа нь хил хязгаарын хяналтын системүүдэд хорт программууд хэрхэн нөлөөлдөг, түүний аюулгүй байдалд ямар сөрөг нөлөө үзүүлдэг талаар танилцуулсан. Хорт программын халдлагаас урьдчилан сэргийлэх арга хэмжээг хэрхэн авах тухай зөвлөмжүүдийг дэвшүүлсэн.

3. Miller, T. (2022). "Cyber Threats in Customs and Border Security Systems"

Энэхүү судалгаа нь гаалийн хяналтын системд цахим халдлагын эрсдэл болон хорт программын нөлөөний талаар хийсэн судалгаа бөгөөд цахим аюулгүй байдлыг сайжруулах аргачлалуудыг тодорхойлсон.

4.Chen, Y., Liu, J., & Wu, Z. (2021). "International Cooperation on Customs Border Control Cybersecurity"

Судалгаанд олон улсын хамтын ажиллагааг хил хязгаарын аюулгүй байдал, цахим хорт программын халдлагаас хамгаалах, мэдээллийн солилцоо болон хамтын ажиллагааг сайжруулах зорилгоор хэрхэн хөгжүүлэх талаар дэлгэрэнгүй авч үзжээ.

5.Jones, H., & Patel, R. (2019). "Automating Border Security: The Role of AI and Malware Protection"

Хилийн аюулгүй байдалд ашиглагддаг хиймэл оюун ухаан болон автоматжуулсан хяналтын системийн талаар хийсэн судалгаа. Мөн хорт программ болон бусад цахим аюулын асуудлыг шийдэх арга замыг судалсан.

6.Gartner, P., & Smit, S. (2020). "Malware and Border Security: Understanding the Risks" Энэхүү судалгаагаар хил дээрх хяналтын системд хорт программын халдлагаас үүсэх

эрсдэлийг ойлгож, түүнийг бууруулах арга замуудыг шинжилсэн. Цахим аюулгүй байдлыг хангах технологи, стратегиудын талаарх судалгаа багтжээ.

Нэг. Хорт программын тухай ойлголт

“Хорт” гэдэг үгийг Монгол хэлний тайлбар толинд “Хор



бүхий юм гэж. Харин “Программ” гэдэг үгийг цахим мэдээллийн хангамж¹ хэмээн тодорхойлсон байдаг.

Нийтэд нь утгачилбал хор бүхий цахим мэдээллийн хангамж хэмээн утгачлах боломжтой.

Хорт программ буюу “malware” гэдэг нь “malicious software” гэсэн үгийн товчлол бөгөөд компьютер, сүлжээ, мэдээллийн системийг гэмтээх, удирдах, мэдээлэл хулгайлах, эсвэл системийн хэвийн үйл ажиллагааг тасалдуулах зорилготой программ хангамжийг хэлнэ².

Хорт программууд ихэвчлэн халдлагын эх үүсвэр болон

¹ Монголын Хэл Соёлын Судалгааны Төв, "Монгол хэлний эх тайлбар толь," Улаанбаатар, 2024.

² M. Sikorski and A. Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software," No Starch Press, 2012.

хохирлын хэмжээнээс шалтгаалж олон төрөлд хуваагддаг. Энэ төрлийн программ хангамжийг кибер гэмт хэрэгтнүүд, хакерууд болон хорлон сүйтгэгч бүлгүүд зохион бүтээдэг бөгөөд тэдгээрийн зорилго нь эдийн засгийн ашиг олох, тагнуулын үйл ажиллагаа явуулах, эсвэл системийг хянах байж болно¹.

Зураг 1. Хорт программын төрлүүд (Хорт программ нь өөрийн гэсэн онцлог шинж чанар, хор хөнөөлийн ялгаагаараа дээрх үндсэн төрлүүдэд ангилагддаг байна)

Гаалийн хяналтын рентген систем нь хилээр гарах болон орж буй бараа бүтээгдэхүүнийг шалгахад ашиглагддаг ч эдгээр төхөөрөмжүүд нь цахим хяналтын шийдэлд тулгуурладаг учир хорт программын халдлагад өртөх өндөр эрсдэлтэй байдаг. Рентген төхөөрөмжийн цахим хяналтын систем нь олон төрлийн мэдээллийн урсгал, сүлжээ, тоног төхөөрөмжийг нэгтгэдэг тул хорт программ нэвтэрч, эдгээр мэдээллийг өөрчлөх боломжтой².

Хорт программын халдлага нь зөвхөн мэдээллийг хулгайлах биш, хил дээрх гаалийн хяналтын үйл ажиллагааг зогсоох, мэдээллийг өөрчлөх, үүний улмаас хууль бус бараа

бүтээгдэхүүний нэвтрэлтийг дэмжих эрсдэлтэй.

Хоёр. Байгалийн ховор элементийн талаар

Монгол Улсын хэмжээнд газрын ховор элементийн ислийн нийт 3.1 сая тонны нөөцтэй, нийт 6 орд илрүүлснээс 4 нь том, 2 нь жижиг. Монгол Улс энэхүү эрдсийн баялгаараа дэлхийд эхний 15-д ордог бөгөөд дараах ордууд багтаж байна³. Үүнд:

-Улаандөлийн 124.78 тонны орд,

-Халзанбүрэгтэйн 1.511.6 мянган тонны орд,

-Мушгиа худгийн 365.1 мянган тонны орд

-Хотгорын 1,213.7 мянган тонны нөөцтэй орд

-Цагаан чулуутын 274.55 тонны орд,

-Лугийн голын 14.5 мянган тонны орд

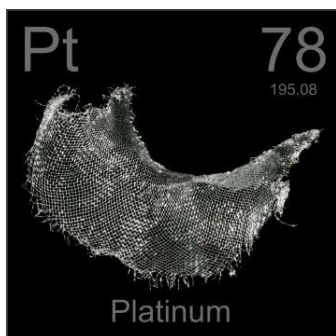
Платинум (Pt)

Платинум (Pt) нь байгалийн ховор металл бөгөөд алттай төстэй өнгө, шинж чанартай байдаг. Энэ металл нь өндөр зэврэлт тэсвэртэй, химийн идэвхгүй, цахилгаан дамжуулах чадвар сайтай. Платинум нь алт, мөнгөний зэрэгт байдаг ч илүү өндөр үнэ цэнтэй байдаг.

¹ Kaspersky, "Cyber Threat Landscape Report," Kaspersky Lab, 2021.

² Kaufman, L. (2021). "Cybersecurity in Border Control Technologies.

³ News.mn. (2023). Монголын алтны уурхайн үйлдвэрлэл өссөөр байна./Нийтлэл/



Зураг 2. Платинум элемент

Технологийн хэрэглээ: Платинум нь эрчим хүчний салбарт хамгийн өргөн хэрэглэгддэг металл юм. Ялангуяа авто машины катализаторууд, хими болон химийн бүтээгдэхүүн үйлдвэрлэл, эрчим хүчний салбар зэрэгт ашиглагддаг.

Гоёл чимэглэл: Платинум нь мөн гоёл чимэглэл, зүүлт, бөгж зэрэгт хэрэглэгддэг. Түүний зэврэлтээс хамгаалагдсан шинж чанар нь гоёл чимэглэлийн үйлдвэрлэлд үнэт металл болгодог¹.

Палладийум (Pd)

Палладийум (Pd) нь мөн платинум бүлгийн металл бөгөөд нь байгальд ихэнхдээ платинум болон родийм-тай хамт илрэх юм. Палладийум нь хөнгөн, зэврэлтэд тэсвэртэй, цахилгаан дамжуулах чадвар өндөртэй.



Зураг 3. Палладийум элемент

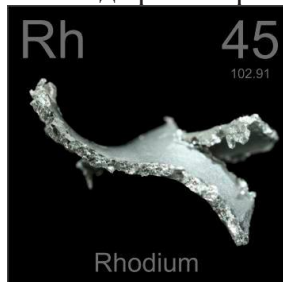
Технологийн хэрэглээ:

Палладийум нь катализатор болон электроник үйлдвэрлэлд ихээхэн ашиглагддаг. Энэ нь машины хаягдлыг цэвэршүүлэх болон цахим төхөөрөмжүүд дээр хэрэглэгддэг.

Эрчим хүчний хэрэглээ: Палладийум нь цахилгаан автомашинууд болон түлшний хаягдлыг цэвэрлэх шинэ технологид ашиглагддаг².

Родиум (Rh)

Родиум (Rh) нь ховор металл бөгөөд өндөр зэврэлтэд тэсвэртэй, бат бөх чанар сайтай, тус элемент нь зэвсэг үйлдвэрлэлд өргөнөөр ашиглагддаг. Родиум нь мөн катализатор болон электрон төхөөрөмжүүд дээр ашиглагддаг. Энэ нь автомашины хаягдлын хийн системд өргөн хэрэглэгддэг³.



¹ Britannica. (2022). Platinum. Encyclopedia Britannica.

² Britannica. (2022). Palladium. Encyclopedia Britannica.

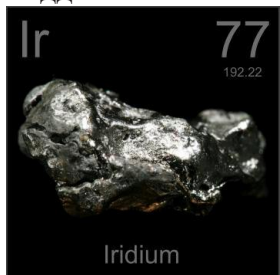
³ ScienceDirect. (2022). Rhodium. ScienceDirect Topics.

Зураг 4. Родийм элемент

Технологийн хэрэглээ:
Родийм нь автомашины катализаторуудаар хамгийн их хэрэглэгддэг. Энэ нь хорт хийнүүдийг (нүүрсхүчлийн хий, азотын оксид гэх мэт) цэвэршүүлдэг.

Иридиум (Ir)

Иридиум (Ir) нь платинум бүлгийн хамгийн хүнд металл бөгөөд өндөр халуунд тэсвэртэй, устай болон зэврэлттэй орчинд ч тогтвортой байдаг. Иридиум нь хамгийн хүнд металлуудын нэг бөгөөд хямд биш, ховор ашиглагддаг металл юм¹.



Зураг 5. Иридиум элемент

Технологийн хэрэглээ:
Иридиум нь өндөр температурт тэсвэртэй материал шаарддаг төхөөрөмжүүд, гэрэл гэрэлтүүлэг, цөмийн технологи зэрэгт хэрэглэгддэг.

Эрчим хүч: Иридиум нь цөмийн цахилгаан станцын бүтцэд ашиглагддаг бөгөөд аюулгүй ажиллагаа, өндөр температурт тэсвэрлэх чадвартай.

Осмиум (Os)

Осмиум (Os) нь платинум бүлгийн хамгийн хүнд металл бөгөөд өндөр зэврэлт тэсвэртэй, тунгалаг шинж чанартай байдаг. Осмиум нь химийн хувьд маш тогтвортой, удаан хугацаанд гэмтэхгүй байдаг².



Зураг 6. Осмиум элемент

Технологийн хэрэглээ:
Осмиум нь цөмийн энерги болон химийн үйлдвэрүүд зэрэгт хэрэглэгддэг. Мөн үүнийг электрон, механик төхөөрөмжүүдэд ашиглаж байна.

Нэг грамм цэвэр элемент дунджаар 10-20000 ам.долларт хүрдэг байна³. Байгалийн ховор элементийг олборлож худалдаалах нь маш их хэмжээний ашиг олох боломжтой тул улсын хилээр хууль бусаар нэвтрүүлэх эрсдэлийг дагуулж байна.

Гурав. Хилийн шалган нэвтрүүлэх рентген сканерын үйл ажиллагаа ба, системийн аюулгүй байдлыг хангах талаар

Олон улсын түвшинд хилийн рентгений төхөөрөмжүүд нь аюулгүй байдал, терроризм, хуурамч бараа бүтээгдэхүүн, мансууруулах бодис болон бусад

¹ ChemicalBook. (2022). Iridium. ChemicalBook.

² ChemicalBook. (2022). Osmium. ChemicalBook.

³ News.mn. (2023). Монголын алтны уурхайн үйлдвэрлэл өссөөр байна./Нийтлэл/

хууль бус зүйлсийг илрүүлэхэд хэрэглэгддэг. Энэ салбарт Smiths Detection, Leidos зэрэг олон улсын компаниуд рентген тоног төхөөрөмжийг үйлдвэрлэж, хилийн хяналтад өргөнөөр ашиглагдаж байна.

1. Smiths Detection - Smiths Detection компани нь HCV болон Hi-Scan 6040i зэрэг рентген төхөөрөмжүүдийг олон улсын хилийн хяналтын байгууллагуудад нийлүүлдэг. Эдгээр төхөөрөмжүүд нь ачаа болон зорчигчдын тээшинд дүн шинжилгээ хийхэд ашиглагддаг бөгөөд террористууд болон контрабандчдыг илрүүлэхэд тусалдаг¹.

2. Leidos - Leidos нь хилийн аюулгүй байдал болон ачаа тээврийн шалгалтын зориулалттай рентген төхөөрөмжүүдийг нийлүүлдэг бөгөөд эдгээр төхөөрөмжүүд нь хилийн аюулгүй байдалд чухал үүрэг гүйцэтгэдэг. Тус компани нь өндөр нарийвчлалтай рентген системийн шийдлийг санал болгодог².

Монгол Улс нь хилийн аюулгүй байдлыг хангах, хил дээрх ачаа болон зорчигчдыг шалгахдаа дараах төхөөрөмжийг ашигладаг байна.

Монгол Улсад хилийн шалгалт хийхэд **Smiths Detection** компанийн рентген

төхөөрөмжүүд болон **Nuctech** компанийн **X-ray scanners** ашигладаг. **Nuctech** компанийн рентген системүүд нь ачааны автомашинуудыг хянан шалгах, хууль бус зүйлсийг илрүүлэх, болон хилийн аюулгүй байдлыг сайжруулах зорилгоор хэрэглэгддэг. Тус төхөөрөмж нь өндөр чанарын зураглал, харьцангуй бага хугацаанд илрүүлэлт хийх боломжийг олгодог³.



Зураг 7. Smith detection компанийн Nuctech рентген

Хилийн Рентген Системүүдэд Хорт Программын Халдлагын Жишээ

Хилийн аюулгүй байдал, гаалийн хяналтын системүүд нь ихэвчлэн нууцлалтай бөгөөд тэдгээрийн үйл ажиллагаа болон халдлагын талаарх тоон мэдээлэл олон нийтэд ил болох нь ховор.

2017 оны WannaCry халдлага

Хорт программ нь дэлхий даяар олон улсын байгууллагуудын компьютерын сүлжээг халдлагад автуулсан бөгөөд рентген системүүд ч үүнд

¹ Smiths Detection. (2022). High security X-ray machines.

² Leidos. (2022). Advanced X-ray technologies for border security.

³ Nuctech. (2021). X-ray scanners for customs and border security.

өртөж байжээ. Энэ халдлагын үед олон улсын гаалийн байгууллагуудын хилийн рентген системүүд ажиллахаа больж, нэг хэсэг нь аюулгүй байдлын зэрэглэлд хүчтэй нөлөө үзүүлсэн. CISA (*Cybersecurity and Infrastructure Security Agency*) байгууллага тус хорт программын халдлагаар аюулгүй байдлын чиглэлд анхаарал хандуулж, урьдчилан сэргийлэх арга хэмжээг авч эхэлсэн байна¹.

NotPetya халдлага

Тус халдлага нь 2017 онд дэлхий даяар олон байгууллагын компьютер системд халдварласан бөгөөд энэ нь рентген болон аюулгүй байдлын системд саатал үүсгэж, хил дээрх аюулгүй байдлыг сулруулсан байна. Тус хорт программ нь мэдээлэл шифрлэх замаар олон улсын аюулгүй байдлын тогтолцооны системийг хохирол амсуулахад хүргэсэн².

Гаалийн хяналтын рентген төхөөрөмжүүдэд хорт программын халдлагаас сэргийлэх дараах хэдэн стратегиудыг багтааж үзэж болно:

Системийн аюулгүй байдлыг сайжруулах

Рентген хяналтын систем нь цахим хяналтын шилдэг технологийг ашигладаг ч хорт

программын халдлагаас хамгаалахын тулд чухал анхаарал шаарддаг. Эдгээр системүүдэд хорт программын халдлагын эрсдэлээс сэргийлэхийн тулд антивирус болон кибер аюулгүй байдлын программ хангамжийг ашигладаг хэдий ч шинэ төрлийн хорт программыг танихын тулд тогтмол сайжруулалт хийх шаардлагатай. Хорт программыг илрүүлэх, устгах, эсвэл халдлагын эх үүсвэрийг устгах нь мэдээллийн аюулгүй байдлыг хангах гол арга юм³. Түүнчлэн, гаалийн хяналтын төхөөрөмжийн хяналтын сүлжээнд хэрэглэх антивирус, firewall системүүдийг байнга шинэчилж байх шаардлагатай.

Мэдээллийг шифрлэх арга хэмжээ авах

Рентген хяналтын төхөөрөмжийн өгөгдлийг шифрлэх нь хорт программын халдлагаас сэргийлэх хамгийн чухал арга юм. Хорт программ нь системд нэвтэрч, мэдээллийг өөрчлөх, хуурамч мэдээлэл илгээх замаар гаалийн хяналтын ажиллагаанд нөлөөлж болно. Иймээс шифрлэлт хийх нь мэдээллийг зөвхөн зөвшөөрөгдсөн хэрэглэгчдэд хүргэх боломжийг олгодог⁴

¹ Smiths Detection. (2021). Cybersecurity in border security systems.

² Kaspersky. (2020). Cybersecurity in critical infrastructure systems.

³ Boulanger, M., & Li, X. (2020).

Cybersecurity in critical infrastructure: A

review of emerging threats and solutions. International Journal of Cybersecurity, 5(2), 45-63.

⁴ Miller, T. (2022). "Cyber Threats in Customs and Border Security Systems."

Олон улсын хамтын ажиллагаа

Кибер аюулгүй байдлын асуудал нь олон улсын хэмжээнд хамтран ажиллах шаардлагатай асуудал болж байна. Рентген хяналтын төхөөрөмжийн аюулгүй байдалд цахим халдлагын эрсдэлээс урьдчилан сэргийлэхийн тулд олон улсын аюулгүй байдлын байгууллагуудтай хамтран ажиллах нь чухал юм. Олон улсын хамтын ажиллагаа нь шинэ төрлийн халдлагыг илрүүлэх, устгах болон эдгээр халдлагуудын нөлөөг бууруулахад чухал үүрэг гүйцэтгэнэ¹.

Алба хаагч, ажилтны мэдлэгийг дээшлүүлэх

Гаалийн хяналтын байгууллагын ажилтнуудад кибер аюулгүй байдал, хорт программын халдлагаас сэргийлэх сургалтыг тогтмол зохион байгуулснаар мэргэжилтнүүдийн чадавх сайжирч, асуудал гарсан тохиолдолд шуурхай хариу арга хэмжээ авах боломжтой бүрдэнэ.

Дөрөв. Гэмт хэргийн зүйлчлэл

Байгалийн ховор элемент болон хилийн рентген системд халдах цахим гэмт хэрэг нь дан ганц төрлөөр зүйлчлэгдэх бус олон төрлийн гэмт хэргийн

шинжийг давхар агуулж байна. Үүнд.

Эрүүгийн хуулийн 26 дугаар бүлэг (Кибер аюулгүй байдлын эсрэг гэмт хэрэг)-ийн 26.1 (Кибер орчинд хууль бусаар халдах), 26.2 (Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах), 18.5 (Улсын хилээр барааг хууль бусаар нэвтрүүлэх), 18.3 (Татвар төлөхөөс зайлсхийх) зэрэг гэмт хэргийн төрөл ангилалд хамаарч байна.

Дүгнэлт

Хилийн рентген системүүд нь хориглосон ачаа тээш нэвтрэх эрсдэл, аюулгүй байдлыг хангахад чухал үүрэг гүйцэтгэдэг боловч технологийн хөгжлийн энэ үед эдгээр системүүд нь хорт программ болон кибер халдлагад өртөх эрсдэлтэй байдаг. Эдгээр халдлагууд нь тухайн улсын хил, гаалийн аюулгүй байдалд томоохон эрсдэл учруулж, ачаа болон зорчигчдын мэдээллийг алдах, системийн ажиллагааг саатуулах, бүр томоохон эрсдэл үүсгэх боломжтой.

Хорт программын халдлагын тохиолдлууд нь рентген системийн программ хангамжийн эмзэг байдал, системийн шинэчлэлтүүдийн дутагдал, сүлжээний хамгаалалтгүй байдал зэрэг хүчин

Journal of Cyber Risk Management, 14(1), 77-82.

¹ Chen, Y., Liu, J., & Wu, Z. (2021).

"International Cooperation on Customs

Border Control Cybersecurity." Global Border Security Review, 10(4), 134-142.

зүйлсийн нөлөөгөөр үүсдэг. Одоогийн байдлаар олон улсад хилийн рентген системийн аюулгүй байдлыг хамгаалахад чиглэсэн олон арга хэмжээ, бодлогын санаачилгуудыг хэрэгжүүлж байгаа ч, энэ асуудал нь бүрэн шийдэгдээгүй хэвээр байна. Тиймээс, хорт программын халдлагаас урьдчилан сэргийлэх, илрүүлэх нь рентген төхөөрөмжүүдийн аюулгүй байдлын хамгийн чухал хэсэг болох бөгөөд үүнийг сайжруулах шаардлагатай.

Рентген системийн хорт программын халдлагаас урьдчилан сэргийлэхийн тулд тавигдах шаардлага нь чухал бөгөөд технологийн шинэчлэл, тогтмол системийн шалгалт, мэргэжлийн сургалтууд хэрэгтэй. Гэхдээ эдгээр арга хэмжээнүүдийг зөв хэрэгжүүлэх нь зөвхөн технологийн асуудал биш, харин улс орнуудын аюулгүй байдлын байгууллагууд, кибер аюулгүй байдлын мэргэжилтнүүдийн хамтын ажиллагаа, төсвийн хуваарилалттай ч холбоотой юм.

Программ хангамжийн шинэчлэлт болон системийн хяналт нь зөвхөн хорт программын халдлагад өртөх эрсдэлийг бууруулахад биш, мөн ашигт ажиллагааны өндөр түвшнийг хадгалахад чухал ач холбогдолтой. Хилийн рентген системийн сүлжээний хамгаалалт болон хорт программ илрүүлэх системүүдийн аюулгүй байдлыг тасралтгүй сайжруулах нь

халдлагын эрсдэлийг бууруулах, мөн цаашдын технологийн хязгаарлалт, эмзэг байдлыг арилгах гол арга юм.

Урьдчилан сэргийлэх арга хэмжээг зөв хэрэгжүүлснээр, рентген системүүд нь хорт программын халдлагаас хамгаалагдаж, олон улсын аюулгүй байдалд хүлээсэн үүргээ үргэлжлүүлэн гүйцэтгэх боломжтой. Рентген тоног төхөөрөмжүүдийн хорт программын халдлагад өртөх нь зөвхөн тоног төхөөрөмжийн ажиллагааг зогсоох бус, улс орнуудын хил хамгаалалт, аюулгүй байдалд чухал нөлөө үзүүлэх учраас энэ асуудалд анхаарал хандуулах нь нэн чухал. Тиймээс, хилийн рентген системийн хамгаалалтын арга хэмжээг сайжруулах, хорт программын халдлагаас сэргийлэхийн тулд олон улсын хамтын ажиллагаа, технологийн шинэчлэлтүүд, мэдээллийн аюулгүй байдлын чадавхуудыг нэмэгдүүлэх шаардлагатай.

Эх сурвалж:

1. Монголын Хэл Соёлын Судалгааны Төв, "Монгол хэлний эх тайлбар толь," Улаанбаатар, 2024.
2. News.mn, "Монголын алтны уурхайн үйлдвэрлэл өссөөр байна," 2023. [Нийтлэл].
3. Kaspersky, "Cyber Threat Landscape Report," Kaspersky Lab, 2021.

4. Kaspersky, "Cybersecurity in critical infrastructure systems," 2020.
5. Kaufman, L. (2021). "Cybersecurity in Border Control Technologies."
6. F. Müller, "Machine Learning for Malware Detection," *International Journal of Cybersecurity*, vol. 14, no. 2, pp. 100-110, 2020.
7. M. Sikorski and A. Honig, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, No Starch Press, 2012.
8. Smiths Detection, "Cybersecurity in border security systems," 2021.
9. Smiths Detection, "High security X-ray machines," 2022.
10. Leidos, "Advanced X-ray technologies for border security," 2022.
11. Nuctech, "X-ray scanners for customs and border security," 2021.
12. Britannica, "Platinum," *Encyclopedia Britannica*, 2022.
13. Britannica, "Palladium," *Encyclopedia Britannica*, 2022.
14. ScienceDirect, "Rhodium," *ScienceDirect Topics*, 2022.
15. ChemicalBook, "Iridium," *ChemicalBook*, 2022.
16. ChemicalBook, "Osmium," *ChemicalBook*, 2022.
17. Boulanger, M., & Li, X. (2020). "Cybersecurity in critical infrastructure: A review of emerging threats and solutions," *International Journal of Cybersecurity*, 5(2), 45-63.
18. Miller, T. (2022). "Cyber Threats in Customs and Border Security Systems," *Journal of Cyber Risk Management*, 14(1), 77-82.
19. Chen, Y., Liu, J., & Wu, Z. (2021). "International Cooperation on Customs Border Control Cybersecurity," *Global Border Security Review*, 10(4), 134-142.