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.2026.01.023

Some Approaches to Mitigating Risks in Databases

Altangerel Bayannamsrai[1], Bayarsaikhan Lkhagvadorj[2]

[1] *Second lieutenant, Researcher, Innovation and technology transfer center, Defense Research Institute of Mongolia, E-mail address: baynnamsrai3@gmail.com, ORCID: 0009-0004-3968-1760*

[2]*Ph.D, Specialist, Research and innovation division, Mongolian National Defense University E-mail address: lkhagvadorj.mndu@gmail.com*

Received: 04 February 2026 *Revised: 15 March 2026*
Accepted: 24 March 2026 *Published online: 30 March 2026*

ABSTRACT

In the information age, data has become a strategic and valuable resource for individuals, organizations, and nations. The rapid development of digital technologies, cloud computing, artificial intelligence, and big data has expanded data utilization, while simultaneously increasing risks related to database security, including cyberattacks, data leakage, and ransomware incidents. In recent years, Mongolia has experienced a growing number of cyberattacks targeting databases of government institutions and critical sectors such as healthcare and energy, making database security a pressing issue.

The objective of this study is to identify common database risks based on theoretical research on data and database systems and to develop feasible approaches for risk mitigation. Scientific analysis, comparative analysis, and synthesis methods were applied, and database risks were assessed in accordance with international standards. In addition, a web-based system was developed to evaluate database risks using both quantitative and qualitative methods. Machine learning and artificial intelligence techniques were utilized to propose effective risk mitigation solutions. The results provide practical recommendations for reducing database security risks at policy, organizational, and technical levels.

Keywords: *Database risk, database security, security, risk management.*

Өгөгдлийн сан дахь эрсдэлийг бууруулах зарим арга зам

Алтангэрэл Баяннамсрай[1], Баярсайхан Лхагвадорж[2]

[1]*Батлан хамгаалахын эрдэм шинжилгээний хүрээлэнгийн Инновац, технологи дамжуулалтын төвийн эрдэм шинжилгээний ажилтан, baynnamsrai3@gmail.com, ORCID: 0009-0004-3968-1760*

[2]*Үндэсний батлан хамгаалахын их сургуулийн Эрдэм шинжилгээ, инновацын хэлтсийн мэргэжилтэн, доктор (Ph.D), lkhagvadorj.mndu@gmail.com*

ХУРААНГУЙ

Мэдээллийн эрин зуунд өгөгдөл нь хувь хүн, байгууллага, улс орны стратегийн ач холбогдол бүхий үнэт нөөц болж байна. Дижитал технологи, үүлэн тооцоолол, хиймэл оюун ухаан, их өгөгдлийн хурдацтай хөгжил нь өгөгдлийн хэрэглээг өргөжүүлж буй боловч өгөгдлийн санг

онилсон кибер халдлага, мэдээлэл алдагдал, ransomware халдлагын эрсдэлийг нэмэгдүүлж байна. Сүүлийн жилүүдэд Монгол Улсад төрийн байгууллага, эрүүл мэнд, эрчим хүч зэрэг стратегийн салбаруудад чиглэсэн цахим халдлага нэмэгдсэн нь өгөгдлийн сангийн аюулгүй байдлыг хангах асуудлыг нэн чухал болгож байна.

Энэхүү судалгааны зорилго нь онолын судалгаанд тулгуурлан өгөгдлийн сан дахь түгээмэл эрсдэлийг тодорхойлж, тэдгээрийг бууруулах арга, шийдлийн хувилбар боловсруулахад оршино. Судалгаанд задлан шинжлэх, харьцуулалт хийх, нэгтгэн дүгнэх аргуудыг ашиглаж, өгөгдлийн сангийн эрсдэлийг тоон болон чанарын аргаар үнэлэх систем боловсруулж, машин сургалт, хиймэл оюунд тулгуурлан эрсдэлийг бууруулах зөвлөмж боловсруулав.

Түлхүүр үг: *Өгөгдлийн сангийн эрсдэл, өгөгдлийн сангийн аюулгүй байдал, аюулгүй байдал, эрсдэлийн удирдлага.*

Оршил

Өнөө үеийн дижитал технологи, интернэт, үүлэн тооцоолол, хиймэл оюун ухаан, квант технологийн хурдацтай хөгжил нь асар их хэмжээний өгөгдлийг бий болгож, тэдгээрийг шийдвэр гаргалт, судалгаа, шинжилгээ, удирдлагын үндсэн эх сурвалж болгон ашиглах боломжийг нэмэгдүүлж байна. Энэ утгаар нь өгөгдлийг “шинэ үеийн баялаг” хэмээн тодорхойлох хандлага ч олон улсад түгээмэл болжээ.

Гэвч өгөгдлийн хэрэглээ тэлэхийн хэрээр мэдээллийн аюулгүй байдал, нууцлал, бүрэн бүтэн, хүртээмжтэй байдлыг хангах асуудал тулгамдсаар байна. Ялангуяа өгөгдлийн санг онилсон ransomware халдлага, зөвшөөрөлгүй хандалт, мэдээлэл алдагдал зэрэг кибер аюул заналхийлэл нь байгууллагын үйл ажиллагаанд ноцтой сөрөг нөлөө үзүүлж, эдийн засгийн ихээхэн хохирол учруулж буй бодит жишээнүүд олширч байна. Нэг удаагийн ransomware халдлагын дундаж хохирол жижиг, дунд байгууллагад хэдэн зуун мянган ам.доллар, томоохон байгууллагад хэдэн сая ам.долларт хүрдгийг судалгаагаар тогтоосон нь өгөгдлийн сангийн аюулгүй байдал чухал болохыг харуулж байна.

Монгол Улсын төр, эрүүл мэнд, эрчим хүч, дэд бүтэц зэрэг стратегийн ач холбогдол бүхий салбаруудыг хамарсан кибер халдлагууд сүүлийн жилүүдэд нэмэгдэж, 2024-2025 онд манай улсыг чиглэсэн зохион байгуулалттай халдлагууд эрчимжсэн талаар олон улсын кибер аюулгүй байдлын эх сурвалжууд мэдээлсэн байна. Тухайлбал, эрүүл мэндийн байгууллагын эмзэг мэдээлэл алдагдах, төрийн өгөгдлийн санд чиглэсэн халдлага зэрэг нь эрсдэл бодит байгааг нотолж, түүнийг шинжлэх ухааны үндэслэлтэйгээр судалж, бууруулах шаардлагыг нэмэгдүүлж байна.

Монгол Улсад өгөгдлийн сангийн эрсдэлийг системтэйгээр тодорхойлж, бодлогын, зохион байгуулалтын болон техникийн түвшинд бууруулах шийдлийг цогцоор нь авч үзсэн судалгаа харьцангуй хомс байна. Иймээс өгөгдлийн сан дахь түгээмэл эрсдэлийг тодорхойлж, олон улсын стандарт, дэвшилтэд технологид тулгуурлан эрсдэлийг бууруулах арга, шийдлийн хувилбар боловсруулах нь онолын төдийгүй практикийн ач холбогдолтой судалгааны асуудал болж байна.

Энэхүү судалгааны ажлаар өгөгдөл, өгөгдлийн сангийн онолын судалгаанд тулгуурлан өгөгдлийн сан дахь эрсдэлийг тодорхойлж, түүнийг бууруулах арга, шийдлийн боломжит хувилбар боловсруулах зорилго тавив.

Судалгааны арга зүй

Онолын судалгаанд задлан шинжлэх, харьцуулах, үнэлгээ хийх аргыг, практик судалгаанд туршилт, систем хөгжүүлэлт, симмуляц, машин сургалтын аргуудыг

хослуулан ашиглав. Судалгааг мэдээллийн технологи, өгөгдлийн сангийн аюулгүй байдлын чиглэлд түгээмэл хэрэглэгддэг онол-практикийн уялдаа бүхий аргачлалд тулгуурлан зохион байгуулсан болно.

Судалгааны үр дүн

1. Өгөгдлийн сангийн түүхэн хөгжил

Компьютерын технологи хөгжихийн хэрээр өгөгдлийн хэмжээ, төрөл, хэрэглээ эрчимтэй нэмэгдэж, үүнийг үр ашигтайгаар удирдах хэрэгцээ бий болсон. Өгөгдлийн сан нь 1960-аад оны эхэн үе бий болсон цагаасаа хойш асар их хувьсан өөрчлөгдөж ирсэн. Шаталсан өгөгдлийн сан (мод шиг загварт тулгуурласан бөгөөд зөвхөн нэгээс олон харилцааг зөвшөөрдөг), сүлжээний өгөгдлийн сан (олон харилцааг зөвшөөрдөг илүү уян хатан загвар) зэрэг навигацийн өгөгдлийн сан нь мэдээллийг хадгалахад ашигладаг анхны системүүд байсан. Хэдийгээр энгийн боловч эдгээр системүүд нь уян хатан биш байлаа. 1980-аад онд харилцааны өгөгдлийн сан түгээмэл болж, дараа нь 1990-ээд онд объект хандалтат өгөгдлийн сангууд гарч ирэв. Саяхан NoSQL өгөгдлийн сан нь интернэтийн өсөлт, илүү хурдацтай, бүтэцгүй өгөгдлийг боловсруулах хэрэгцээ шаардлагад хариу үйлдэл болгон бий болсон. Үүний үр дүнд өгөгдлийн сангийн технологи 1960-аад оноос эхлэн өнөөг хүртэл үе шаттайгаар хөгжиж иржээ.

Өгөгдлийн сангийн 1-р үе: Навигацийн өгөгдлийн сан (1960–1970-аад он)

Өгөгдлийн сангийн хөгжлийн эхний үеийг навигацийн өгөгдлийн сангийн үе гэж нэрлэдэг. Энэ үед өгөгдөлд хандахдаа тодорхой зам (path) зааж өгч, өгөгдлийг шат дараалсан байдлаар уншиж боловсруулах шаардлагатай байв. Шаталсан өгөгдлийн сан нь мод хэлбэрийн бүтэцтэй бөгөөд нэг эцэг–олон хүүхэд харилцааг зөвшөөрдөг. Өгөгдөл нь хатуу бүтэцтэй тул нэг объект нь зөвхөн нэг л эцэгтэй байх боломжтой. Энэ төрлийн өгөгдлийн сангийн түгээмэл жишээ нь IBM IMS юм *(Grolinger K. 2013)*.

Шаталсан өгөгдлийн сангийн давуу тал нь Энгийн бүтэцтэй, өгөгдөлд хандах хурд өндөр бол сул тал нь уян хатан бус, олон төрлийн харилцааг илэрхийлэх боломж муу байсан.

Харин сүлжээний өгөгдлийн сан нь шаталсан загварыг сайжруулсан хэлбэр бөгөөд нэг объект олон эцэгтэй байж болох боломжийг олгодог. CODASYL стандарт дээр суурилсан энэхүү загвар нь илүү уян хатан боловч системийн зохион байгуулалт, программчлалын хувьд төвөгтэй байв.

Эдгээр навигацийн өгөгдлийн сангууд нь тухайн үеийн техник, технологийн боломжид тохирсон боловч өгөгдлийн бүтцийг өөрчлөх, системийг өргөтгөхөд хүндрэлтэй байсан нь дараагийн үеийн хөгжилд нөлөөлсөн.

Өгөгдлийн сангийн 2-р үе: Харилцааны өгөгдлийн сан (1980–1990-ээд он)

1980-аад онд E.F.Codd-ийн дэвшүүлсэн харилцааны өгөгдлийн сангийн загвар нь өгөгдлийн сангийн хөгжлийн хоёрдугаар үеийг эхлүүлсэн. Энэхүү загвар нь өгөгдлийг хүснэгт хэлбэрээр зохион байгуулж, өгөгдөл хоорондын харилцааг математик онолд тулгуурлан илэрхийлдэг. Харилцааны өгөгдлийн сан нь SQL (Structured Query Language) хэл ашиглан өгөгдөлд хандах боломжийг олгосноор хэрэглэгч болон өгөгдлийн сангийн хоорондын харилцааг хялбарчилсан.

Давуу тал нь өгөгдлийн хараат бус байдал, бүрэн бүтэн байдал, асуулга

боловсруулахад хялбар, сул тал нь их хэмжээний өгөгдөлд ашиглахад хүндрэлтэй, бүтэцгүй өгөгдөлд тохиромжгүй зэрэг болно *(Grolinger K. 2013)*.

Энэ үеэс эхлэн Oracle, MySQL, PostgreSQL, SQL Server зэрэг өгөгдлийн сангууд өргөн хэрэглээнд нэвтэрсэн.

Өгөгдлийн сангийн 3-р үе: NoSQL ба Их өгөгдөл (2000 оноос хойш)

Интернэт, үүлэн технологи, сошиал сүлжээ, IoT системүүд хурдацтай хөгжсөнөөр өгөгдлийн хэмжээ, хурд, төрөл эрс нэмэгдсэн. Үүний үр дүнд уламжлалт харилцааны өгөгдлийн сангаас өөр шийдлүүд шаардлагатай болж, NoSQL өгөгдлийн сан болон их өгөгдлийн технологи бий болсон. NoSQL өгөгдлийн сан нь тогтсон схем шаардахгүй, хэвтээ тэлэх боломжоороо онцлогтой. Үүнд: Key-Value, Document, Column-based, Graph өгөгдлийн сангууд багтана. Эдгээр нь өндөр хурдтай өгөгдөл боловсруулах, их хэмжээний мэдээллийг хуваарилагдсан орчинд хадгалахад тохиромжтой. Эдгээр нь их өгөгдлийн суурь юм. Их өгөгдөл / Big data/ нь Volume, Velocity, Variety гэсэн гурван үндсэн шинж чанартай. Hadoop, Apache Spark зэрэг технологиуд нь их өгөгдлийг хадгалах, боловсруулахад өргөн ашиглагддаг. Их өгөгдлийн технологи нь хиймэл оюун ухаан, машин сургалт, бодит цагийн анализ, шийдвэр дэмжих системүүдийн суурь болж байна *(Grolinger K. 2013)*.

2. Өгөгдлийн сангийн бүтэц, зохион байгуулалт

Өгөгдлийн сан (Database) нь тодорхой зорилгоор цуглуулж, тодорхой зохион байгуулалттайгаар компьютерын тогтмол санах ойд хадгалсан цогц өгөгдлийн цуглуулга юм. Өгөгдлийн сан нь хандах, засварлах болон нэмэхэд хялбар байдлаар хийгдсэн байдаг. Өгөгдлийн сан нь талбар (fields), бичилтүүд (records) болон файлаас (files) бүрддэг. Талбар гэдэг нь багана бүхий мэдээлэл бөгөөд бичилт нь нэг мөрөнд байгаа нийт мэдээллийг хэлдэг. Нийт оруулсан мэдээллээ нэр өгч сануулан, файл болгодог *(Connolly T. M. 2005)*.

Өгөгдлийг ангилж, нэгдсэн удирдлагаар хангах боломжийг олгосноор түүнд хялбар хандах, боловсруулах, дүн шинжилгээ хийх боломжтой болдог. Өгөгдлийн санд өгөгдлийг ихэвчлэн мөр, баганаас бүрдэх хүснэгтээр зохион байгуулдаг. Мөр нь бичлэгийг илэрхийлдэг бол багана нь талбарыг илэрхийлдэг. Жишээлбэл, өгөгдлийн сан нь бүтээгдэхүүний хүснэгт бол дотроо захиалгын болон үйлчлүүлэгчдэд зориулсан хүснэгттэй байж болно. Энэ бүтэц нь илүүдэл өгөгдлийг багасгах, хадгалагдсан мэдээллийн үнэн зөв, бүрэн бүтэн байдлыг хангадаг. Өгөгдлийн сангийн зохион байгуулалт нь янз бүрийн хүснэгтүүдийн хоорондын хамаарлыг тодорхойлоход чухал үүрэгтэй. Тухайлбал, захиалгыг хэрэглэгчийн ID эсвэл бүтээгдэхүүний ID гэх мэт өвөрмөц танигчаар дамжуулан тодорхой хэрэглэгч, бүтээгдэхүүнтэй холбох гэх мэт.

Мөн өгөгдлийн сангийн зохион байгуулалт нь тухайн байгууллагын тодорхой хэрэгцээнд тулгуурлан тохирох мэдээллийн санг сонгоход нөлөөлдөг. Жишээлбэл, харилцааны өгөгдлийн сангууд бүтэцлэгдсэн өгөгдөлд тохиромжтой байдаг бол NoSQL өгөгдлийн сангууд нь ихэвчлэн бүтэцгүй их хэмжээний өгөгдөлтэй ажиллахад ашиглагддаг. Өгөгдлийн сангийн төрлийг сонгох нь өргөтгөх чадвар, ашиглахад хялбар байдал, хадгалагдаж буй өгөгдлийн шинж чанар зэрэг хүчин зүйлээс хамаарна.

Орчин үеийн байгууллагуудын үйл ажиллагаа өгөгдөлд тулгуурласан хэлбэрт бүрэн шилжсэнтэй холбоотойгоор өгөгдлийн сан нь кибер халдлагын гол бай болж байна. Өгөгдлийн сан нь их хэмжээний нууц, эмзэг, стратегийн ач холбогдолтой мэдээллийг хадгалдаг тул түүнд чиглэсэн аливаа халдлага нь байгууллагын санхүүгийн тогтвортой байдал, нэр хүнд, хууль эрх зүйн хариуцлага-д ноцтой сөрөг үр дагавар учруулах өндөр эрсдэлтэй. Иймээс өгөгдлийн сан дахь эрсдэлийг тодорхойлох, түгээмэл халдлагын хэлбэрүүдийг онолын түвшинд судлах нь мэдээллийн аюулгүй байдлын судалгааны чухал бүрэлдэхүүн хэсэг болдог.

Интернэтэд суурилсан халдлагууд нь өгөгдлийн сангийн аюулгүй байдалд тулгарч буй байнгын сорилтуудын нэг бөгөөд халдагч этгээдүүд өгөгдлийн санд нэвтрэх, мэдээлэл хулгайлах шинэ арга, тактик, техникүүдийг тасралтгүй боловсруулж байна. Эдгээр халдлагын зарим нь илрүүлэхэд хүндрэлтэй байдаг бөгөөд үүнд хэрэглэгчийн итгэмжлэлийг хууль бусаар олж авах фишинг халдлага, нууц үг задлах, эсвэл хууль ёсны хэрэглэгчийн нэрийн дор системд нэвтрэх үйлдлүүд багтдаг. Өгөгдөл нэгэнт алдагдвал хувь хүний эмзэг, нууц мэдээллээс эхлээд улс үндэстний тусгаар тогтнол, аюулгүй байдалтай холбоотой томоохон хэмжээний хохирол учруулах ч эрсдэлтэй.

<u>3. Өгөгдлийн санд үүсэж болох эрсдэлүүд</u>

1. Өгөгдлийн сангийн сул хамгаалалтаас шалтгаалж зөвшөөрөлгүй этгээд системд нэвтрэх боломж бүрдэж, байгууллагын нууц болон эмзэг мэдээлэлд хууль бус хандалт үүсэх эрсдэл бий болдог. Энэ нь ихэвчлэн сул нууц үг, буруу тохиргоо, шинэчлэгдээгүй системтэй холбоотой байдаг. Ийм нөхцөл байдал нь халдлага цаашид өргөжих үндсэн суурь болж өгдөг.

2. Өгөгдлийн санд зөвшөөрөлгүй нэвтрэлт үүссэнээр мэдээллийн нууцлал алдагдаж, хувь хүний эмзэг, нууц мэдээлэл задрах, байгууллагын дотоод баримт бичиг, стратегийн ач холбогдолтой өгөгдөл гуравдагч этгээдийн гарт орох эрсдэл нэмэгддэг. Энэ төрлийн эрсдэл нь харилцагч, хэрэглэгчдийн эрх ашгийг шууд хөндөж, итгэлцэлд сөргөөр нөлөөлдөг. Мөн нууц мэдээлэл задрах нь бусад төрлийн сөрөг үр дагаврын эх үүсвэр болдог.

3. Халдагч этгээд өгөгдлийг санаатайгаар өөрчлөх, устгах, эсвэл гуйвуулах замаар мэдээллийн бүрэн бүтэн байдал алдагдаж, улмаар буруу тооцоолол, буруу шийдвэр гаргах нөхцөл байдал үүсэх эрсдэл бий болдог.

4. Өгөгдлийн найдвартай байдал алдагдсанаар удирдлагын түвшинд гарч буй шийдвэрүүд бодит бус мэдээлэлд тулгуурлах аюултай. Энэ нь байгууллагын дотоод хяналтын тогтолцоог сулруулах сөрөг үр дагавартай.

5. Өгөгдөл устах, шифрлэгдэх, эсвэл систем доголдох зэргээс шалтгаалан өгөгдлийн хүртээмж алдагдаж, байгууллагын үндсэн үйл ажиллагаа тасалдах, үйлчилгээ үзүүлэх боломжгүй болох эрсдэл үүсдэг. Ялангуяа өгөгдөлд бүрэн тулгуурласан процессууд зогсоноор хэрэглэгчдэд үзүүлэх үйлчилгээ саатах нөхцөл бүрдэнэ. Энэ нь байгууллагын өдөр тутмын үйл ажиллагаанд шууд сөрөг нөлөө үзүүлдэг.

6. Өгөгдлийн сангийн халдлагаас үүдэн системийг сэргээх, өгөгдөл нөхөн бүрдүүлэх, аюулгүй байдлыг сайжруулахад их хэмжээний зардал шаардагдаж, байгууллагад шууд болон шууд бус санхүүгийн хохирол учрах эрсдэл нэмэгддэг.

Үүнээс гадна үйлчилгээ тасалдсанаас орлого буурах, нэмэлт нөөц зарцуулах шаардлага үүсдэг. Ийм санхүүгийн дарамт нь байгууллагын тогтвортой байдалд шууд нөлөөлдөг.

7. Өгөгдөл алдагдсанаар хувь хүний мэдээлэл хамгаалах болон холбогдох хууль, стандартууд зөрчигдөж, байгууллага торгууль, хяналт шалгалт, шүүхийн маргаанд өртөх хууль эрх зүйн эрсдэлтэй тулгардаг. Энэ нь зөвхөн санхүүгийн бус, удирдлагын болон зохион байгуулалтын хүндрэл дагуулдаг. Хууль эрх зүйн эрсдэл нь байгууллагын бодлого, хяналтын тогтолцооны сул талыг илчилдэг.

8. Өгөгдлийн сангийн аюулгүй байдал алдагдсан тухай мэдээлэл олон нийтэд ил болох үед байгууллагын нэр хүнд, харилцагчдын итгэл алдагдаж, урт хугацаанд зах зээл дэх байр суурь сулрах эрсдэл бий болдог. Итгэл алдагдах нь шинэ хэрэглэгч татах боломжийг багасгаж, одоогийн харилцагчдыг алдах нөхцөл бүрдүүлдэг. Энэ төрлийн эрсдэл нь богино хугацаанд нөхөгдөхөд хүндрэлтэй байдаг.

9. Стратегийн ач холбогдолтой өгөгдөл алдагдсанаар байгууллагын өрсөлдөх чадвар буурч, хөгжлийн төлөвлөгөө, бизнесийн стратеги алдагдах замаар урт хугацааны тогтвортой байдалд сөрөг нөлөө үзүүлэх эрсдэл үүсдэг. Судалгаа, шинжилгээ, зах зээлийн мэдээлэл алдагдах нь өрсөлдөгчдөд давуу байдал олгох боломжийг бүрдүүлдэг.

Иймээс өгөгдлийн сангийн аюулгүй байдал нь байгууллагын стратегийн түвшний асуудал гэж үздэг *(Laudon 2018)*.

4. Өгөгдлийн сан дахь эрсдэлийг бууруулах арга зам

Эрсдэлийг үнэлсний эцэст дараагийн зайлшгүй хэрэгжүүлэх үе шат нь илэрсэн эрсдэлүүдэд тохирсон бууруулах арга хэмжээг тодорхойлох, төлөвлөх, хэрэгжүүлэх, хянах явдал юм. Өгөгдлийн сан нь байгууллагын үндсэн мэдээллийн санг бүрдүүлдэг тул түүнд учрах аливаа халдлага, доголдол нь санхүүгийн алдагдал, нэр хүндийн уналт, хууль эрх зүйн хариуцлага үүсгэх өндөр эрсдэлтэй байдаг. Иймээс өгөгдлийн сангийн эрсдэлийг бууруулах үйл ажиллагаа нь техник-технологийн шийдэл төдийгүй удирдлага, бодлого, стандартын шаардлагыг хамарсан цогц хандлагад суурилах шаардлагатай.

Өгөгдлийн сан дахь эрсдэлийг бууруулахад түгээмэл хэрэглэдэг аргачлалууд нь эрсдэлийг багасгах (mitigation), зайлсхийх (avoidance), шилжүүлэх (transfer) болон хүлээн зөвшөөрөх (acceptance) гэсэн үндсэн хэлбэрүүдэд хуваагддаг. Жишээлбэл, SQL Injection болон Privilege Escalation зэрэг өндөр магадлал, өндөр нөлөөлөлтэй халдлагын хувьд тэдгээрийг хүлээн зөвшөөрөх бус, техникийн болон зохион байгуулалтын хүчтэй хамгаалалтын арга хэмжээгээр багасгах нь зүйтэй байдаг. Харин бага магадлалтай, хязгаарлагдмал нөлөөлөлтэй эрсдэлийг тодорхой нөхцөлд хүлээн зөвшөөрөх боломжтой *(Whitman 2017)*.

Өгөгдлийн сангийн аюулгүй байдлын хүрээнд эрсдэлийг бууруулах техникийн арга хэмжээнд өгөгдлийг шифрлэх, хэрэглэгчийн хандалтыг үүрэгт суурилсан хяналтаар (Role-Based Access Control) зохицуулах, аудитын бүртгэл (logging), халдлага илрүүлэх систем (IDS/IPS), нөөцлөлт болон сэргээн босголтын механизмыг нэвтрүүлэх зэрэг орно. Эдгээр арга хэмжээ нь Data Leakage, Insider Threat, Ransomware зэрэг халдлагын магадлал болон үр дагаврыг мэдэгдэхүйц бууруулахад чиглэгддэг *(Kendrick 2015)*.

Үүнээс гадна бодлого, зохион байгуулалтын арга хэмжээ нь өгөгдлийн сангийн эрсдэлийг бууруулахад чухал үүрэгтэй. Үүнд мэдээллийн аюулгүй байдлын бодлого боловсруулах, нэвтрэх эрхийн зохицуулалтыг журамлах, ажилтнуудад зориулсан сургалт, мэдлэг олгох хөтөлбөр хэрэгжүүлэх, дотоод аудит явуулах зэрэг орно. Судалгаагаар өгөгдлийн сангийн аюулгүй байдлын зөрчлийн ихээхэн хувь нь техникийн бус, хүний хүчин зүйлтэй холбоотой байдаг нь эдгээр арга хэмжээний ач холбогдлыг тодотгодог.

Мөн өгөгдлийн сан дахь эрсдэлийг бууруулах үйл ажиллагааг олон улсын стандарттай уялдуулах нь хамгаалалтын арга хэмжээг системтэй, дахин давтагдахуйц байдлаар хэрэгжүүлэх боломжийг олгодог. ISO/IEC 27005 стандарт нь эрсдэлийг тодорхойлох, шинжлэх, үнэлэх, бууруулах, хянах гэсэн үе шатуудыг нэгтгэсэн хүрээг санал болгодог бөгөөд уг стандартыг өгөгдлийн сангийн аюулгүй байдалд ашигласнаар судалгааны үр дүн онолын болон практикийн хувьд баталгаатай болдог.

Нэг. Бодлого, зохион байгуулалтын арга:

Өгөгдлийн сан дахь эрсдэлийг бууруулахад бодлого, зохион байгуулалтын арга хэмжээ нь техникийн хамгаалалтаас дутахааргүй чухал үүрэгтэй. Учир нь өгөгдлийн сангийн аюулгүй байдлын зөрчил, мэдээллийн алдагдлын ихэнх нь хүний хүчин зүйл, дотоод процессын сул зохион байгуулалттай холбоотой байдаг. Иймээс байгууллага мэдээллийн аюулгүй байдлыг зөвхөн техник хэрэгслээр бус, зохион байгуулалтын түвшинд системтэйгээр удирдах шаардлагатай.

Энэхүү аргачлалын үндсэн суурь нь мэдээллийн аюулгүй байдлын бодлого боловсруулах явдал юм. Өгөгдлийн сангийн аюулгүй байдлын бодлого нь өгөгдөлд хандах эрх, ашиглалт, хадгалалт, дамжуулалт, устгалттай холбоотой нийтлэг шаардлага, хариуцлагыг тодорхойлж өгдөг. Бодлого нь байгууллагын бүх түвшний ажилтнуудад ойлгомжтой, хэрэгжих боломжтой байдлаар боловсруулагдсан байх ёстой бөгөөд бодлогын хэрэгжилтийг дотоод хяналтын механизмаар баталгаажуулна.

Мөн ажилтнуудын мэдлэг, хандлагыг дээшлүүлэх сургалт, дадлага нь бодлого, зохион байгуулалтын арга хэмжээний салшгүй хэсэг юм. Фишинг, нууц үгийн аюулгүй байдал, өгөгдлийн ангилал зэрэг сэдвээр тогтмол сургалт явуулах нь хүний алдаанаас үүдэх эрсдэлийг мэдэгдэхүйц бууруулдаг. Иймээс мэдээллийн аюулгүй байдлын соёлыг төлөвшүүлэх нь өгөгдлийн сангийн эрсдэлийг бууруулах стратегийн чухал бүрэлдэхүүн хэсэг болдог. Бодлого, зохион байгуулалтын арга хэмжээг оновчтой хэрэгжүүлэх нь техникийн хамгаалалтын аргын үр дүнг шууд нэмэгдүүлнэ.

Хоёр. Техникийн хамгаалалтын арга:

Техникийн хамгаалалтын арга нь өгөгдлийн сан дахь эрсдэлийг бууруулах хамгийн шууд бөгөөд бодит нөлөө үзүүлдэг хэрэгслүүдийн нэг юм. Эдгээр арга хэмжээ нь өгөгдөлд зөвшөөрөлгүй хандах, өөрчлөх, устгах, алдагдахаас сэргийлэхэд чиглэдэг бөгөөд SQL Injection, Data Leakage, Ransomware зэрэг түгээмэл халдлагын эсрэг хамгаалалтын үндсэн шугам болдог.

Юуны өмнө өгөгдлийг шифрлэх арга нь өгөгдлийн сангийн аюулгүй байдлын үндсэн техник шийдэлд тооцогддог. Өгөгдлийг хадгалах болон дамжуулах явцад

шифрлэснээр өгөгдөл алдагдсан тохиолдолд ч агуулга нь гуравдагч этгээдэд ашиглагдах боломжгүй болдог. Энэ нь ялангуяа санхүүгийн, хувийн болон стратегийн ач холбогдолтой өгөгдөлд илүү тохиромжтой *(Elmasri 2016)*.

Хандалтын хяналтын техникийн механизмд хэрэглэгчийн баталгаажуулалт (authentication), эрх олголт (authorization), аудит лог (audit logging) зэрэг орно. Эдгээр механизмууд нь өгөгдлийн санд хэн, хэзээ, ямар өгөгдөлд хандсан болохыг бүртгэж, сэжигтэй үйлдлийг илрүүлэх боломжийг олгодог. Ингэснээр Insider Threat болон Privilege Escalation-ийн эрсдэлийг илрүүлэх, хянах нөхцөл бүрддэг.

Гурав. Стандартын арга:

Стандартын арга нь өгөгдлийн сан дахь эрсдэлийг бууруулах үйл ажиллагааг системтэй, баталгаатай, дахин давтагдахуйц байдлаар хэрэгжүүлэхэд чиглэсэн аргачлал юм. Олон улсын стандартууд нь байгууллагын мэдээллийн аюулгүй байдлын менежментийн тогтолцоог тодорхойлж, эрсдэлийг удирдах нэгдсэн хүрээг санал болгодог *(27005:2018 2013)*.

ISO/IEC 27001 болон ISO/IEC 27005 стандартууд нь өгөгдлийн сангийн аюулгүй байдлын бодлого, эрсдэлийн үнэлгээ, бууруулах арга хэмжээг уялдуулахад өргөн хэрэглэгддэг. Тухайлбал, ISO/IEC 27005 стандарт нь эрсдэлийг тодорхойлох, шинжлэх, үнэлэх, бууруулах, хянах гэсэн үе шатуудыг системтэйгээр хэрэгжүүлэхийг зөвлөдөг. Энэ нь өгөгдлийн сангийн эрсдэлийн удирдлагыг байгууллагын нийт мэдээллийн аюулгүй байдлын стратегитай уялдуулах боломжийг олгодог *(27005:2013 2013)*.

Стандартын арга хэрэглэхийн давуу тал нь хамгаалалтын арга хэмжээг субьектив байдлаар бус, олон улсын хэмжээнд хүлээн зөвшөөрөгдсөн шалгуур, үзүүлэлтэд тулгуурлан хэрэгжүүлэхэд оршдог. Мөн аудит, үнэлгээ хийхэд хялбар болж, байгууллагын мэдээллийн аюулгүй байдлын төлөвшлийг илүү бодитой үнэлэх нөхцөл бүрддэг.

Иймээс өгөгдлийн сангийн эрсдэлийг бууруулахад стандартын арга нь бодлого, техникийн хамгаалалтын арга хэмжээг нэгтгэх, урт хугацаанд тогтвортой хэрэгжүүлэх стратегийн суурь болдог.

5. Машин сургалт ба хиймэл оюунд суурилсан эрсдэлийг бууруулах шийдэл:

Сүүлийн жилүүдэд мэдээллийн хэмжээ огцом өсөж, өгөгдлийн сангийн бүтэц улам нарийсахын хэрээр уламжлалт дүрэмд суурилсан аюулгүй байдлын аргачлалууд нь бүх төрлийн халдлага, эрсдэлийг бүрэн илрүүлэхэд хангалтгүй болж байна. Үүнтэй уялдан машин сургалт (Machine Learning, ML) болон хиймэл оюун ухаан (Artificial Intelligence, AI)-д суурилсан шийдлүүдийг өгөгдлийн сангийн аюулгүй байдалд ашиглах хандлага эрчимтэй нэмэгдэж, эрсдэлийг бууруулах дэвшилтэт арга хэлбэр болон хөгжиж байна.

Машин сургалт, хиймэл оюунд суурилсан системүүдийн гол давуу тал нь их хэмжээний өгөгдөлд суурилан хэвийн болон хэвийн бус зан төлөвийг ялган таних чадварт оршдог. Өгөгдлийн сангийн орчинд энэ нь хэрэглэгчийн хандалтын давтамж, асуулгын бүтэц, өгөгдөл татах хэмжээ, цаг хугацааны хэв маяг зэрэг үзүүлэлтүүдийг тасралтгүй шинжилж, урьд өмнө илрээгүй сэжигтэй үйлдлийг автоматаар илрүүлэх боломжийг бүрдүүлдэг. Ийм байдлаар машин сургалтын аргууд нь SQL Injection, Data Leakage зэрэг халдлагыг бодит цаг хугацаанд таних

үр ашигтай хэрэгсэл болдог.

Мөн insider threat буюу дотоод аюулыг илрүүлэхэд зан төлөвийн шинжилгээнд суурилсан AI шийдлүүд онцгой ач холбогдолтой. Уламжлалт хамгаалалтын системүүд нь эрх бүхий хэрэглэгчийн хууль ёсны хандалтыг аюул гэж ялгаж танихад хүндрэлтэй байдаг бол машин сургалтын алгоритмууд нь тухайн хэрэглэгчийн хэвийн зан төлөвийн суурь загварыг бий болгож, түүнээс гажсан аливаа үйлдлийг сэжигтэй гэж тодорхойлох боломжтой. Ингэснээр өгөгдлийг зориудаар эсвэл санамсаргүйгээр гадагшлуулах эрсдэлийг эрт үед нь илрүүлэх нөхцөл бүрдэнэ.

Цаашлаад хиймэл оюунд суурилсан шийдлүүд нь халдлагын хэв шинжийг урьдчилан таамаглах (predictive analysis) боломжийг олгодог. Өмнөх халдлагын өгөгдөл, эмзэг байдлын мэдээлэл, системийн лог бүртгэлд дүн шинжилгээ хийснээр AI загварууд ирээдүйд ямар төрлийн халдлага, ямар өгөгдлийн сангийн хэсэгт илүү өндөр магадлалтай үүсэхийг урьдчилан тодорхойлох чадвартай. Энэ нь эрсдэлийг зөвхөн илрүүлэх бус, урьдчилан сэргийлэх түвшинд удирдах боломжийг бий болгодог.

Гэсэн хэдий ч машин сургалт, хиймэл оюунд суурилсан шийдлүүд нь уламжлалт хамгаалалтын аргуудыг бүрэн орлох бус, харин тэдгээрийг нөхөх, сайжруулах үүрэгтэй гэж үздэг. Эдгээр технологи нь чанартай сургалтын өгөгдөл, зөв тохируулсан загвар, тасралтгүй шинэчлэл шаарддаг тул бодлого, зохион байгуулалтын болон техникийн хамгаалалтын арга хэмжээнүүдтэй уялдуулан хэрэгжүүлэх нь зүйтэй. Ийм байдлаар ML, AI-д суурилсан шийдлүүдийг өгөгдлийн сангийн эрсдэлийн удирдлагын цогц тогтолцоонд нэгтгэснээр кибер халдлагын эрсдэлийг илүү үр дүнтэй бууруулах боломж бүрдэнэ.

6. Туршилт явуулах үе шат

Хүснэгт 1. *Туршилт явуулах үе шат*

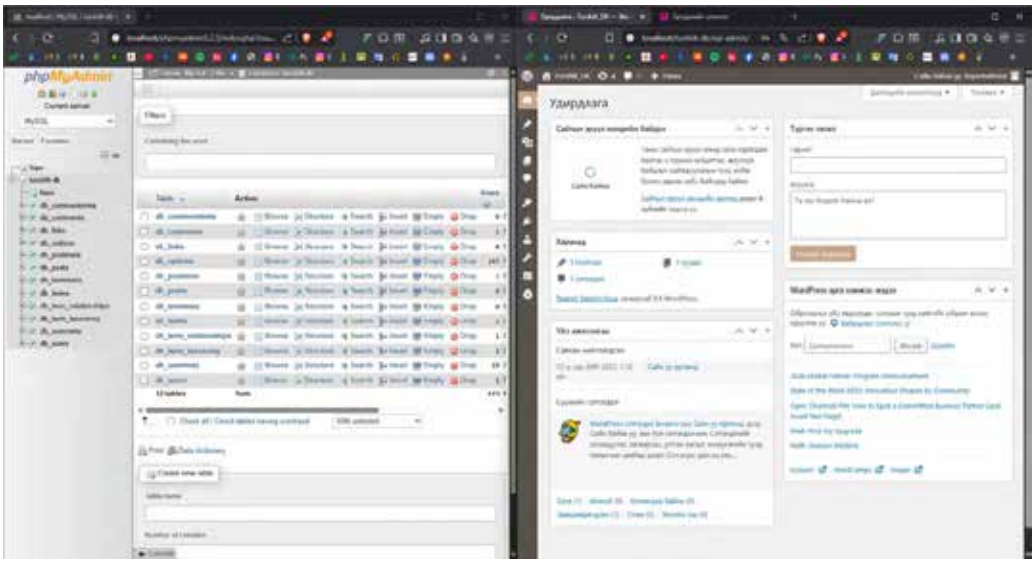
№	**Туршилтын үе шат**	**Хийх үйлдэл**	**Туршилтаас гарах үр дүн**
1	Туршилтын орчин бүрдүүлэх	WAMP сервер суулгаж Apache, MySQL серверийг ажиллуулах	Веб туршилтын орчин амжилттай бүрдэнэ
2	Өгөгдлийн сан үүсгэх	phpMyAdmin ашиглан зохиомол өгөгдлийн сан, хүснэгтүүд үүсгэх	Туршилтад ашиглах өгөгдлийн сан бэлэн болно
3	Веб интерфейс боловсруулах	PHP, HTML ашиглан эрсдэлийн үнэлгээ оруулах веб хуудас боловсруулах	Эрсдэлийн өгөгдөл оруулах боломжтой веб систем бий болно
4	Эрсдэлийн шалгуур тогтоох	Эрсдэлийн төрөл, магадлал, нөлөөллийн шалгуур тодорхойлох	Эрсдэлийг үнэлэх нэгдсэн шалгуур тогтоогдоно

5	Эрсдэлийн үнэлгээ хийх	Магадлал × Нөлөөлөл томьёогоор эрсдэлийн оноо тооцоолох	Эрсдэлийн тоон үнэлгээ автоматаар гарна
6	Эрсдэлийн түвшин ангилах	Эрсдэлийн матриц ашиглан Low, Medium, High, Critical түвшинд хуваах	Эрсдэлийн ач холбогдол тодорхой болно
7	Үр дүн шинжлэх	Өндөр эрсдэлтэй эрсдэлүүдийг харьцуулан шинжлэх	SQL Injection, Data Leakage зэрэг эрсдэлүүд өндөр түвшинд илэрнэ
8	Дүгнэлт гаргах	Туршилтын үр дүнд тулгуурлан аналитик дүгнэлт хийх	Туршилтын өгөгдлийн санд ямар хамгаалалт шаардлагатай нь нотлогдоно
9	Зөвлөмж боловсруулах	Техникийн болон зохион байгуулалтын зөвлөмж боловсруулах	Эрсдэлийг бууруулах практик шийдлүүд гарна

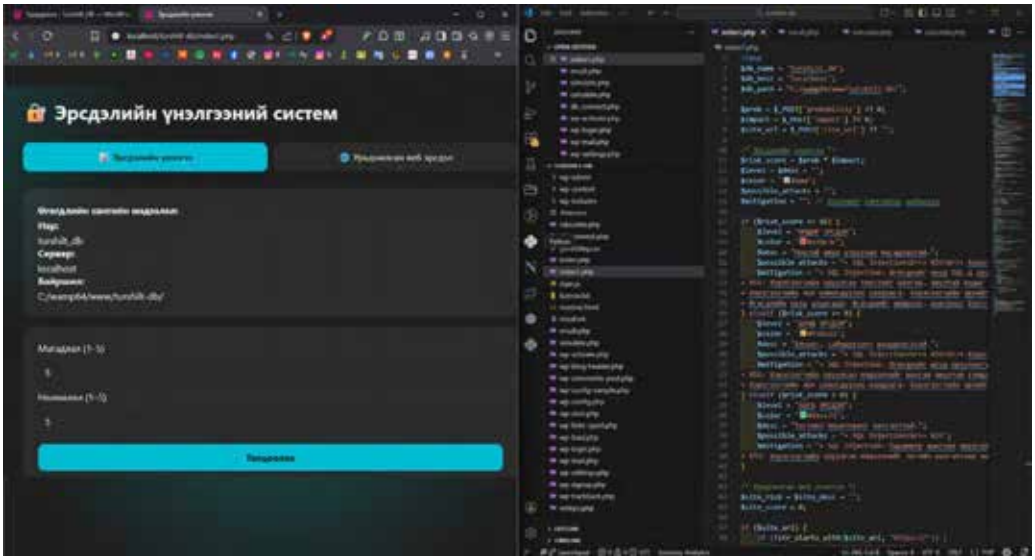
Туршилтыг үе шаттайгаар гүйцэтгэж, өгөгдлийн сан дахь эрсдэлийг бодит орчинд үнэлсэн. Туршилтаас гарсан үр дүн нь өгөгдлийн сангийн аюулгүй байдлыг сайжруулах шаардлагатайг нотолж, эрсдэлийг бууруулах оновчтой арга замуудыг тодорхойлох боломж олгоно.

Туршилтын үйл явц:

Эрсдэлийн үнэлгээний систем дээр компьютерт үүссэн сервер, байршил, өгөгдлийн сангийн нэр зэрэг мэдээллүүдийг шууд харуулна. Магадлал, нөлөөллийн үнэлгээг стандартуудад нийцүүлэн гараар оруулж өгснөөр эрсдэлийн үнэлгээ хийгдэнэ.



Зураг 1. *WAMP server үүсгэж, туршилтын өгөгдлийн санг ажиллуулж веб сайттай холбосон*



Зураг 2. *Тооцоолол хийх сайтыг бэлэн болгосон.*

Зураг 3. *Үнэлгээ хийгдсэн байдал*

Тооцоолол хийхэд тухайн өгөгдлийн санд халдаж болох боломжит халдлагуудыг нэрлэж, халдлагаас хамгаалах боломжит шийдлүүдийг боловсруулж өгнө.

Хөгжүүлэлт, туршилтын үр дүн:

Энэхүү туршилтыг үе шаттайгаар хэрэгжүүлж, туршилтын орчинд үүсгэсэн веб сайт болон өгөгдлийн санд эрсдэлийн үнэлгээ хийлээ. Туршилтын явцад WAMP сервер дээр суурилсан PHP ба MySQL технологийг ашиглан эрсдэлийн үнэлгээний веб системийг амжилттай хөгжүүлж, өгөгдлийн сангийн түгээмэл эрсдэлүүдийг магадлал–нөлөөллийн (Likelihood–Impact) аргачлалаар үнэлэв.

Туршилтын үр дүнгээс дараах үндсэн дүгнэлтүүд гарч байна. Үүнд:

- Өгөгдлийн сангийн аюулгүй байдалд чиглэсэн эрсдэлийг веб орчинд бодитойгоор үнэлэх боломжтой системийг туршилтын түвшинд амжилттай хэрэгжүүлж чадсан. Энэхүү систем нь зохиомол өгөгдөл ашигласан ч бодит орчинд тулгардаг эрсдэлийн нөхцөл байдлыг загварчлан харуулах боломжийг бүрдүүлсэн бөгөөд практик хэрэглээнд шилжүүлэх суурь шийдэл болох боломжтойг харуулж байна.
- Магадлал–нөлөөллийн (Likelihood–Impact) аргачлалыг ашиглан эрсдэлийг үнэлэх нь өгөгдлийн сангийн олон төрлийн эрсдэлийг нэг ижил шалгуурын хүрээнд, ойлгомжтой бөгөөд харьцуулах боломжтой байдлаар үнэлэхэд үр дүнтэй болох нь туршилтаар батлагдсан. Энэ нь эрсдэлийн үнэлгээг субьектив байдлаас тодорхой хэмжээгээр ангид болгож, тоон болон чанарын үнэлгээг уялдуулан ашиглах боломжийг олгож байгаагаараа онцлог юм.
- Эрсдэлийн матриц ашигласнаар эрсдэлийн түвшнийг системтэйгээр ангилж, хамгаалалтын арга хэмжээг эрэмбэлэн төлөвлөх, улмаар шийдвэр гаргалтыг дэмжих бодитой үндэс бүрдсэн. Өндөр болон маш өндөр түвшний эрсдэлүүдийг тодорхойлсноор хамгаалалтын нөөцийг оновчтой хуваарилах, аюулгүй байдлын стратегийг үе шаттайгаар хэрэгжүүлэх боломж нэмэгдэж, байгууллагын мэдээллийн аюулгүй байдлын удирдлагад бодит үр өгөөж өгөхүйц шийдэл болох нь нотлогдлоо.

7. Эрсдэлээс урьдчилан сэргийлэх зөвлөмж

Туршилтын үр дүнд үндэслэн дараах хамгаалалтын зөвлөмжийг дэвшүүлж байна. Үүнд:

1. SQL Injection буюу өгөгдлийн сангийн асуулгад хорт код шургуулах халдлагааас урьдчилан сэргийлэхийн тулд хэрэглэгчийн оруулж буй мэдээллийг оролтын шалгалтаар нягтлах, мөн өгөгдлийн сантай харилцах асуулгуудыг урьдчилан бэлтгэсэн асуулга ашиглан гүйцэтгэх шаардлагатай. Энэ нь хэрэглэгчийн оруулсан мэдээлэл өгөгдлийн сангийн командын бүтцийг өөрчлөх эрсдэлийг бууруулна.

2. Өгөгдлийн нууцлал болон хандалтын аюулгүй байдлыг хангах үүднээс хэрэглэгчийн эрхийн зохицуулалтыг оновчтой хэрэгжүүлэх, түүнчлэн эмзэг мэдээллийг хадгалах болон дамжуулах явцад мэдээллийг нууцлан хувиргах (шифрлэх) аргыг ашиглах нь зүйтэй. Ингэснээр мэдээлэл алдагдах, зөвшөөрөлгүй этгээдэд ил болох эрсдэл буурна.

3. Дотоод хэрэглэгчийн буруутай болон санамсаргүй үйлдлээс үүдэх эрсдэлийг бууруулах зорилгоор системийн үйл ажиллагааны бүртгэл (лог) болон хяналт, шалгалтын (аудитын) механизмыг сайжруулах шаардлагатай. Энэ нь хэрэглэгчийн үйлдлийг мөрдөх, сэжигтэй өөрчлөлтийг илрүүлэх, улмаар эрсдэлийг эрт үед таньж хариу арга хэмжээ авах боломжийг бүрдүүлнэ.

4. Эрсдэлийн үнэлгээг нэг удаагийн арга хэмжээ гэж үзэх бус, тогтмол хугацаанд дахин гүйцэтгэх замаар хамгаалалтын түвшнийг тасралтгүй сайжруулах нь чухал. Ингэж аюул заналын орчин, системийн өөрчлөлттэй уялдуулан эрсдэлийг үе шаттайгаар үнэлснээр өгөгдлийн сангийн аюулгүй байдлыг урт хугацаанд тогтвортой хангах боломж бүрдэнэ.

Дүгнэлт

Өгөгдөл, түүний онцлог шинж чанар, ангилал, өгөгдлийн сангийн бүтэц, удирдлага болон аюулгүй байдлын асуудлыг онолын болон туршилтын түвшинд судаллаа.

Судалгааны үр дүнгээс харахад өгөгдөл нь зөвхөн техникийн объект бус, харин хүний сэтгэлгээ, шийдвэр гаргалт, боловсруулалтын үйл явцтай нягт уялдсан стратегийн үнэ цэнтэй нөөц болохыг тогтоов. Өгөгдлийг зөв ангилж, боловсруулан мэдээлэл болгон хувиргах процесс нь ч өгөгдлийн аюулгүй байдалтай шууд холбоотой ажээ. Судалгааны ажлын гол үр дүнг дараах байдлаар дүгнэж байна. Үүнд:

1. Өгөгдлийн сангийн бүтэц, загварчлал, SQL хэл дээр суурилсан өгөгдлийн сангийн удирдлага, түүний аюулгүй байдлын талаарх судалгаа, туршилт, түүний үр дүнгээр бий болсон шинэ мэдлэгүүд нь өгөгдөлтэй ажиллах, хадгалах, боловсруулах, үнэлэх болон хамгаалах суурь ойлголтыг бүрдүүлж байна.

2. Судалгаагаар өгөгдлийн үнэлэмж /үнэ цэн/ нэмэгдэхийн хэрээр халдлагад өртөх магадлал өсдөг нь ажиглагдсан бөгөөд энэхүү эрсдэлийг зөвхөн техникийн түвшинд бус, хүний хүчин зүйл, зохион байгуулалтын орчин, бодлого, журам зэрэг олон түвшинд цогцоор нь удирдах шаардлагатайг тодорхойлов. SQL Injection, Privilege Escalation, Data Leakage, Insider Threat, Ransomware зэрэг түгээмэл эрсдэлүүд нь өгөгдлийн сангийн аюулгүй байдалд ноцтой нөлөө үзүүлдэг тул олон түвшний хамгаалалтын бодлогоор удирдах нь зайлшгүй болохыг судалгаа харуулж байна.

3. Мөн өгөгдлийн сангийн эрсдэлийн үнэлгээг хэрэгжүүлэхэд чанарын болон тоон үнэлгээний аргуудыг хослуулан ашиглах нь оновчтой болохыг өөрийн хөгжүүлсэн вебийн орчинд хийсэн туршилтын үр дүн баталлаа.

4. Чанарын үнэлгээ нь эрсдэлийг хурдан ангилан эрэмбэлэх, өндөр эрсдэлтэй заналхийллийг тодорхойлоход үр дүнтэй бол тоон үнэлгээ нь эрсдэл бүрийн бодит болон санхүүгийн үр дагаврыг нарийвчлан тооцоолох замаар удирдлагын шийдвэрийг эдийн засгийн үндэслэлтэй болгох боломжийг бүрдүүлж байна.

5. Эрсдэлийн матрицыг ашигласнаар магадлал ба нөлөөллийн хослолыг үнэлж, аль эрсдэлийг нэн тэргүүнд бууруулах, аль нь хянах түвшинд үлдээх шийдвэрийг илүү оновчтой гаргах нөхцөл бүрдсэн.

6. Судалгаагаар өгөгдлийн сангийн аюулгүй байдлыг хангахад техникийн, зохион байгуулалтын болон стандартын арга хэмжээг уялдуулан хэрэгжүүлэх нь чухал болохыг тогтоов. Тухайлбал, шифрлэлтийн хэрэгсэл, хандалтын хяналтын механизм, халдлага илрүүлэх систем, ажилтны сургалт, дотоод бодлого, олон улсын стандартын хэрэгжилт зэрэг арга хэмжээг цогцоор нь хэрэгжүүлэх нь эрсдэлийг бууруулах, хянахад бодитой үр нөлөөтэй байна.

7. Ийнхүү өгөгдлийн сангийн менежмент, эрсдэлийн үнэлгээ болон

хамгаалалтын арга хэмжээг иж бүрнээр, нэгтгэн хэрэгжүүлэх нь байгууллагын стратегийн нөөц болсон мэдээлэл болон өгөгдлийн сангийн аюулгүй байдлыг хангах, эрсдэлийг бодитой үнэлж удирдах хамгийн оновчтой шийдэл болох нь энэхүү судалгааны онолын дүгнэлт, туршилтын үр дүнгээр батлагдлаа.

Эшлэл авсан сурвалж, судалгааны бүтээл:

1. 27005:2013, ISO/IEC. 2013. *Information technology — Security techniques — Information security management systems — Requirements. Geneva: ISO.*
2. 27005:2018, ISO/IEC. 2013. *Information technology — Security techniques — Information security risk management. Geneva: ISO.* ISO/IEC.
3. Connolly T. M., Begg C. E. 2005. *Database Systems: A Practical Approach to Design, Implementation, and Management. 4th ed. – Edinburgh: Pearson Education Limited.*
4. Elmasri, R. Navathe, S. 2016. *Fundamentals of Database Systems, 7th ed.* Boston: MA: Pearson.
5. Grolinger K., Hayes M., Higashino W. A., L’Heureux A., Allison D., Capretz M. A. M. 2013. “Data Management in Cloud Environments: NoSQL and NewSQL Data Stores.” *Journal of Cloud Computing.*
6. Kendrick, T. 2015. *Identifying and Managing Project Risk: Essential Tools for Failure-Proofing Your Project, 3rd ed.* New York: AMACOM.
7. Laudon, K. C., Laudon, J. P. 2018. *Management Information Systems: Managing the Digital Firm. 15th ed.* Edinburgh: UK: Pearson Education Limited .
8. NIST. 2012. . *Guide for Conducting Risk Assessments, Special Publication 800-30 Revision 1. Gaithersburg, MD: National Institute of Standards and Technology.*
9. Paar, C., Pelzl, J., Güneysu, T. 2024. *Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms. – Berlin, Germany : Springer-Verlag GmbH, 2nd edition .*
10. Whitman, M. E., Mattord, H. J. 2017. *Principles of Information Security, 6th ed.* Boston: MA: Cengage Learning .