ЦАХИМ ОРЧИНД /КИБЕР/ ҮЙЛДЭГДСЭН ГЭМТ ХЭРГИЙГ МЭРГЭЖЛИЙН УДИРДЛАГААР ХАНГАХ НЬ

О.Эрхэмзаяа
Дотоод хэргийн их сургуулийн Удирдлагын академийн 8021 дүгээр дамжааны суралцагч, цагдаагийн хошууч

Товч агуулга: Энэхүү илтгэлийн зорилго нь Кибер гэмт хэрэгтэй тэмцэх, мөрдөн шалгах ажиллагааг мэргэжлийн удирдлага, арга зүйгээр хангах, мэргэшсэн хүний нөөцийг бэлдэх, өндөр ур чадвартай мэргэшсэн алба хаагчийг тогтвор суурьшилтай ажиллуулах эрх зүйн орчинг бүрдүүлэх хэрэгцээ шаардлага үүссэн байна. Иймд энэхүү сэдвээр магистрын түвшинд судлан үр дүнтэй судалгаанд суурилсан санал зөвлөмж хэрэгцээ шаардлага байгаа нь энэхүү сэдвийг судлах зорилго оршино.

Түлхүүр үгс: Кибер аюулгүй байдал, Кибер орон зай, Кибер орчин, Кибер халдлага,

Key words: Cyber security, Cyberspace, environment, Cyber attack.

Оршил

Монгол Улсын Их Хурлын 2020 оны 05 дугаар сарын 13-ны өдрийн 52 дугаар тогтоолоор “Алсын хараа 2050” урт хугацааны хөгжлийн бодлогын баримт бичгийг баталсан. Түүнд:

- Кибер аюулгүй байдлыг хангах хууль, эрх зүйн орчныг бүрдүүлж, технологид суурилсан инновац, интеграцыг хөгжүүлж, эрсдэлийн менежментийн үндэсний чадавхыг бэхжүүлнэ.
- Кибер аюулгүй байдлыг хангах тогтолцоог бэхжүүлнэ.
- Мэдээлэл, технологи, харилцаа холбооны систем, техник хэрэгсэл, программ хангамжийн үндэсний үйлдвэрлэлийг дэмжсэн тогтолцоо бүрдэж, технологийн хараат байдал буурч, кибер гэмт хэрэг, кибер халдлагатай тэмцэх чадавхийг бэхжүүлэх талаар тодорхой үе шаттай хэрэгжүүлэх зорилтыг тус тус дэвшүүлсэн байна[1].

Өнөөдөр Монгол Улсад facebook, instagram, twitter, tiktok зэрэг шууд зохицуулалт хийх боломжгүй, гадаад улсад сервертэй олон нийтийн сүлжээг иргэд өргөнөөр идэвхтэй ашиглаж байна.

Ялангуяа фэйсбүүк орчинд бага болон өсвөр насны хүүхдүүдийн дунд нээлттэй, хаалттай групп идэвхтэй үйл ажиллагаа явуулж байгаагаас хаалттай группүүд их байдаг. Эдгээр хаалттай групп, чатуудад гэмт этгээдүүд хуурамч хаяг ашиглан хохирогч нартай харилцаа тогтоох, садар самуун агуулгатай зураг, дүрс бичлэг солилцох, биеэ үнэлэлт зохион байгуулах зэрэг хүүхдийн эсрэг гэмт хэрэг олноор үйлдэгдэх боллоо.

Фэйсбүүк компаний хувьд хэрэглэгчийн мэдээллийг зөвхөн

[1] Монгол Улсын Их Хурлын 2020 оны 52 дугаар тогтоол. “Алсын хараа 2050” урт хугацааны бодлогын баримт бичиг.

терроризм, хүний амь нас хохирох нөхцөл байдал бий болсон, хүүхэдтэй холбоотой садар самуун, секс сүрдүүлэг болон үндэстэн дамнасан зохион байгуулалттай гэмт хэрэгт мэдээлэл гаргаж өгөхөөр хамтын ажиллагаатай боловч хүсэлтийн хариу хэт удаан ирдэг, зарим тохиолдолд ирдэггүй, шууд мэдээлэл авах боломжгүй, цаг хугацаа алдаж тоон ул мөр, нотлох баримт устах эрсдэл бий болгож байна.

Мөн гадаад улсад сервертэй бусад сошиал медиа, мэйл үйлчилгээ үзүүлэгч зэрэг компаниудаас мэдээлэл авах боломж, бололцоогүй байдал нь гэмт этгээдийг илрүүлэх, нотлох баримт цуглуулахад хүндрэл бэрхшээлийг учруулж мөрдөн шалгах ажиллагаа зогсож байна. Тиймээс манай улстай эрх зүйн харилцан туслалцаа үзүүлэх гэрээгүй улс орнуудтай эрх зүйн харилцан туслалцаа үзүүлэх гэрээ, санамж бичиг байгуулж идэвхтэй хамтран ажиллах, хилийн чанадад сервертэй, шууд зохицуулалт хийх боломжгүй системүүдээс (фэйсбүүк, твиттер гэх мэт) мэдээлэл шуурхай гаргуулан авах нөхцөл бололцоог бүрдүүлэх хэрэгцээ шаардлагатай бий болж байна.

Нэг. Кибер гэмт хэргийн тухай ойлголт

Монгол улсад өдөр ирэх тусам өсөн нэмэгдэж буй компьютерын хэрэглээг дагаад компьютер, компьютерын сүлжээг ашиглан үйлдэгдэх гэмт хэргийн гаралт ихэссээр байгаа билээ. Олон нийт, иргэдийн дунд Кибер гэмт хэргийн тухай ойлголт байхгүй нь уг төрлийн гэмт хэргийн гаралт ихсэх нэг том шалтгаан болж байгаа юм. Эрүүгийн хуулийн хорин зургаадугаар бүлэгт Кибер аюулгүй байдлын эсрэг гэмт хэргийн талаар зүйлчлэн заасан бөгөөд эдгээр зүйл заалтад:

- Кибер орчинд хууль бусаар халдах 26.1
- Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах 26.2

Кибер гэмт хэргийн гол обьект нь төр, байгууллага, хувь хүний мэдээ мэдээлэл, компьютерийн мэдээллийн дэд бүтэц, програм хангамж байдаг бөгөөд уг төрлийн гэмт хэргийг олон төрлийн арга технологи ашиглан үйлдэгддэг ба эдгээр арга технологиуд өдөр ирэх тусам өөрчлөгдөн шинэчлэгдэж байдаг.

- “Identity theft”- Хувь хүн, хуулийн этгээдийн мэдээллийг ашиглан залилан мэхлэх, хуурах.
  - Сэргийлэх арга зам: Шаардлагагүй тохиолдолд өөрийнхөө мэдээллийг бусдад өгөхгүй байх, олон нийтийн сүлжээнд байршуулахгүй байх. /Зураг, регистрийн дугаар, өвчтөний түүх гэх мэт/
- “Phishing”- Цахим хуудасны хандалтыг өөрчилж, хэрэглэгчийг тусгайлан бэлтгэсэн хуурамч цахим хуудас руу хандуулах замаар мэдээлэл хулгайлах.
  - Сэргийлэх арга зам: Цахим хуудасны хандах нэрийг сайтар нягталж шалгасны дараа цахим хуудас руу хандах.
- “Кибер хүчирхийлэл”- Олон нийтийн сүлжээ, цахим шуудан бусад цахим зам сувгийг ашиглан хувь хүнийг гүтгэх, доромжлох, айлган сүрдүүлэх.
  - Сэргийлэх арга зам: Олон нийтийн сүлжээнд болон бусад цахим сүлжээнд үл таних этгээдтэй харилцаа тогтоохтой сэрэмжтэй байх, хэт хувийн чанартай мэдээллээ бусдад задлахгүй байх, кибер хүчирхийлэл гэж

үзэж буй үедээ хуулийн байгууллагад хандахаас эмээхгүй байх.

- “Man in the Middle”–Хуурамч АР /Access Point/ үүсгэн, түүнд холбогдсон хэрэглэгчийн мэдээллийг замаас хулгайлах.
  - Сэргийлэх арга зам: Нийтийн болон найдваргүй утасгүй интернетийг ашиглахгүй байх, ашигласан тохиолдолд хувийн мэдээлэл, хандах эрхээ нууцлах.

ХОЁР. КИБЕР ГЭМТ ХЭРГИЙН НӨХЦӨЛ БАЙДАЛ

Хэрэг бүртгэлт, мөрдөн байцаалт явуулсан нийт 7599 хэргийн 6901 буюу 90.8 хувийг нийгмийн сүлжээ, хэрэглэгчийн нэвтрэх нэр, нууц үгийг хууль бусаар олж авах, 524 буюу 6.9 хувийг хэрэглэгчийн дансны болон зээлийн картын мэдээллийг хууль бусаар олж авах, 168 буюу 2.2 хувийг хувь хүнд сэдэл өгч, итгэл төрүүлэх замаар мэдээллийг олж авах, 6 буюу 0.1 хувийг компьютерын сүлжээнд вирус, хортой код тараах, спам халдлага үйлдэх аргаар үйлдэгдсэн байна.

Эдгээр хэргүүдийг зүйлчлэлээр нь авч үзвэл:

Нийгмийн сүлжээ, хэрэглэгчийн нэвтрэх нэр, нууц үгийг хууль бусаар олж авах аргаар үйлдэгдсэн 6901 хэргийн 586 буюу 8.5 хувийг Эрүүгийн хуулийн 26.1 дүгээр зүйлд заасан “Цахим мэдээлэлд хууль бусаар халдах”, 28 буюу 0.4 хувийг 13.10 дугаар зүйлийн 2 дахь хэсгийн 2.1-д заасан “Цахим хэрэгсэл ашиглаж хувь хүний нууцад халдах”, 14 буюу 0.2 хувийг 16.9 дүгээр зүйлийн 2 дахь хэсгийн 2.1-д заасан “Цахим сүлжээ ашиглаж хүүхэд оролцуулж садар самууныг сурталчлах”, 6273 буюу 90.9 хувийг 17.3 дугаар зүйлийн 1 дэх хэсэгт заасан “Цахим хэрэгсэл ашиглаж Залилах” гэмт хэрэг тус тус эзэлж байна.

Хэрэглэгчийн данс болон зээлийн картын мэдээллийг хууль бусаар олж авах аргаар үйлдэгдсэн 524 хэргийн 54 буюу 10.3 хувийг “Цахим мэдээлэлд хууль бусаар халдах”, 4 буюу 0.7 хувийг “Цахим хэрэгсэл ашиглаж хувь хүний нууцад халдах”, 466 буюу 89.0 хувийг “Цахим хэрэгсэл ашиглаж залилах” гэмт хэрэг тус тус эзэлж байна.

Хувь хүнд сэдэл өгч, итгэл төрүүлэх замаар мэдээллийг олж авах аргаар үйлдэгдсэн 168 хэргийн 4 буюу буюу 2.3 хувийг “Цахим мэдээлэлд хууль бусаар халдах”, 163 буюу 97.0 хувийг “Цахим хэрэгсэл ашиглаж залилах” гэмт хэрэг тус тус эзэлж байгаа бол “Цахим хэрэгсэл ашиглаж хувь хүний нууцад халдах”, “Цахим сүлжээ ашиглаж хүүхэд оролцуулж садар самууныг сурталчлах” гэмт хэрэг тус бүр 1 шалгагджээ.

Компьютерын сүлжээнд вирус, хортой код тараах, спам халдлага үйлдэх аргаар үйлдэгдсэн 6 хэргийн 5 буюу 83.3 хувийг “Цахим мэдээлэлд хууль бусаар халдах”, 1 буюу 16.7 хувийг “Цахим хэрэгсэл ашиглаж залилах” гэмт хэрэг эзэлж байна.

Судалгаагаар тогтоогдсон нөхцөл байдлаас дүгнэхэд, Эрүүгийн хуулийн 26 дугаар бүлэгт заасан “Цахим мэдээллийн аюулгүй байдлын эсрэг” болон Эрүүгийн хуулийн 17.3 дугаар зүйлийн 1 дэх хэсэгт заасан “Цахим хэрэгсэл ашиглаж залилах” гэмт хэрэг өссөн байна. Тухайлбал:

Нийгмийн сүлжээ хэрэглэгчийн нэвтрэх нэр, нууц үгийг хууль бусаар олж авч системд нэвтэрч, тухайн хэрэглэгчийн найз нөхөд, хамаатан садан, хамт ажилладаг зэрэг ойр дотны хүмүүс рүү нь “Би ийм хүнд байдалд орлоо. Яаралтай мөнгөний хэрэг гарлаа, бараа авахад мөнгө дутлаа, түр хугацаагаар зээлье” гэх зэрэг зурвас

илгээн төөрөгдөлд оруулж, өөр хүний дансны дугаараар мөнгийг шилжүүлэн авч залилсан гэмт 2022 онд 1114 гарсан бол 2023 онд 1185 болж 29-р буюу 25.4 хувиар өссөн, харин 2024 оны II улирлын байдлаар 1231 болж 146-р буюу 1.7 дахин өсчээ.

Мөн хэрэглэгчийн данс болон зээлийн картын мэдээлэлд хууль бусаар халдаж, иргэдийн данснаас мөнгө гуйвуулан авсан хэрэг 2022 онд 1193 гарсан бол 2023 онд 1299 болж 6-р буюу 6.5 хувиар 89-р буюу 89.9 хувиар тус тус өссөн байна.

Гэмт этгээдүүд тодорхой нэг мэдээллийн сайт, хүмүүсийн сонирхол татсан мэдээллийн зургийг ашиглан мэдээллийг дэлгэрүүлэн үзэх холбоосыг байршуулдаг байх ба иргэд мэдээллийг нарийвчлан авахын тулд тухайн холбоосоор нэвтэрч, дараагийн сайт руу дамжин ордог. Гэтэл уг сайт нь гэмт этгээдүүдийн зохиомол буюу хуурамч сайтууд байдаг ба холбоосоор нэвтэрснээр хэрэглэгчээс фэйсбуукын нэр, нууц үгийг шаарддаг. Хэрэглэгч нь нэр, нууц үгээ хийгээд нэвтэрсэн тохиолдолд хуурамч сайт нь мэдээллийг автоматаар хадгалж авч, улмаар гэмт этгээд тухайн фэйсбуукын нэр, нууц үгийг ашиглан нэвтэрч, хэрэглэгчийн найз нөхөд, хамаатан садан руу мөнгө шилжүүлэхийг хүссэн зурвас илгээж залилдаг. Гэмт этгээдүүд ихэнх тохиолдолд 50.000-500.000 төгрөг хүссэн мессэж илгээдэг байна.

Хувь хүнд сэдэл өгч, итгэл төрүүлэх замаар мэдээллийг олж авах аргаар үйлдэгдсэн залилах гэмт хэрэг 2022 онд 197 гарсан бол 2023 онд 236 болж 39-р буюу 19.8 хувиар, 2023 оны III улирлын байдлаар 389 болж 153-р буюу 64.8 хувиар тус тус өсчээ.

Дээрх аргаар үйлдэгдсэн гэмт хэргийн тухайд, гэмт хэрэг үйлдэж буй этгээдүүд нь иргэдийн хэрэгцээт шаардлагад тулгуурлан, нийгмийн сүлжээнд өөрийгөө нуун далдалсан хуурамч хаягнаас “бага хүүтэй, удаан хугацааны зээл олгоно, онлайн захиалга авч, хямд үнээр бараа зарна” гэх зэргээр зар, бичлэг байршуулж, зарын дагуу холбогдсон иргэний хэрэгцээ шаардлага, сэтгэл зүйн онцлогийг харгалзан сэдэл өгч, харилцдаг.

Мөн өөрийгөө “олон улсын байгууллагын ажилтан” хэмээн танилцуулж, “танай улсад их хэмжээний тусламжийн хөрөнгө нийлүүлнэ, илгээмж явуулна”, “гэрээний зардал, зээлийн татвар, хураамж, урьдчилгаа төлбөр хэрэгтэй“ гэх зэргээр иргэдийн итгэлийг олж, тодорхой хэмжээний төлбөрийг урьдчилж төлөх шаардлагатай мэтээр төөрөгдөлд оруулж, мөнгийг нь шилжүүлэн авсан тохиолдол нийтлэг байна.

Мөрдөн шалгах ажиллагааны явцад мөнгө хүлээн авагчийг шалгахад, мөнгийг хүлээн авсан данс эзэмшигч нь мөн төөрөгдөлд орох замаар бусдад дансаа ашиглуулсан нөхцөл байдлууд тогтоогдсон байна. Тухайлбал:

Такси үйлчилгээ үзүүлсэн жолооч, АТМ /Автомат тооцооны машин/-аас бэлэн мөнгө авахаар дугаарлан зогсож байгаа хүн, худалдаа, үйлчилгээний ажилтан зэрэг хүмүүст “картаа мартсан, гээгдүүлсэн, блоклуулсан” гэх зэргээр худал хэлж, дансыг нь ашиглаж, урамшуулалд нь бага хэмжээний мөнгө өгөх зэргээр иргэний дансыг ашиглаж мөнгө шилжүүлэн авсан, эсхүл “ажилд оруулж өгнө, анкет судалгаа авна” гэх зэргээр хуурч дансны мэдээллийг нь олж авч ашигладаг, карго үйлчилгээ эрхэлдэг хүнтэй хуурамч бүртгэлтэй хаягаар харьцаж, тухайн хүнээр

дамжуулан гадаад улс руу мөнгийг шилжүүлдэг, спорт бооцооны сайтад бооцоо тавих, компьютер тоглоомын аккаунтыг цэнэглэдэг байна.

“i-mail” цахим сүлжээ үйлдэгдэн гарч байгаа хэргүүдийн тухайд хувь хүн болон Монгол улсад үйл ажиллагаа явуулж байгаа бизнесийн байгууллагууд гадаад улсын харилцагч байгууллагынх нь тогтмол харилцдаг цахим шуудангийн хаягийн нэг үсэг, тоо, цэг, таслалыг нэмэх, хасах зэрэг байдлаар өөрчлөн өөр хаяг үүсгэн харилцаж, улмаар өөр банк, дансны дугаар илгээсэн байхад, иргэд түүнийг нь нягтлахгүйгээр их хэмжээний гадаад валютыг гадаад улс уруу шилжүүлж залилуулсан хэргүүд мөн байна.

ГУРАВ: ЦАХИМ ОРЧИНД ҮЙЛДЭГДЭЖ БАЙГАА ГЭМТ ХЭРГИЙГ МӨРДӨХ АЖИЛЛАГААНЫ ОНЦЛОГ

Цахим орчинд үйлдэгдсэн гэмт хэрэгт мөрдөн шалгах ажиллагааг зайлшгүй мэдээллийн технологи, харилцаа холбооны талаар өндөр мэдлэг, мэргэшилтэй алба хаагч хийж гүйцэтгэх шаардлагатай байдаг. Учир нь цахим орчинд үйлдэгдэж байгаа гэмт хэрэг тул алс хол байрлах газар ч хэрэг учралын газар байх тохиолдол байдаг. Өөрөөр хэлбэл, цахим халдлагын улмаас нэг төхөөрөмжөөс өөр төхөөрөмж рүү хууль бус халдлага явуулдаг нь энгийн мөрдөгч мөрдөн шалгах ажиллагаа явуулахад хүндрэлтэй байхаас гадна олон талын мэдлэгтэй байхыг шаарддаг. Мөн цахим мэдээллийн сүлжээнд хууль бусаар халдах программ, техник хэрэгсэл бэлтгэх, борлуулах, хор хөнөөлт программ хангамж бүтээх, ашиглах, тараах гэмт хэргийг энгийн мөрдөгч мөрдөн шалгах ажиллагаа явуулахад хүндрэл учрах юм.

Дээрх төрлийн гэмт хэргийг мөрдөгч, прокурор, шүүгч шалгаж, нотлон, эцэслэн шийдвэрлэхэд цахим технологийн мэдлэг шаардлагатай тул мөрдөн шалгах ажиллагаанд хүндрэл учруулдаг. Гэвч өдөр ирэх тусам өсөн нэмэгдэж байгаа компьютерийн хэрэглээг дагаад бүхий л төрлийн харилцаа, цахим хэлбэрт шилжиж байгаа тул хууль сахиулах байгууллагын алба хаагчид цахим, технологийн мэдлэг чадвар эзэмших шаардлагатай болж байна.

Хэрэв энэ төрлийн гэмт хэрэгтэй тэмцэх зохих мэдлэг, чадвар байхгүй бол цахим гэмт хэргийг таслах зогсоох, илрүүлэх, шийдвэрлэх боломжгүй болно.

Энгийн үгээр хэлбэл цахим орчинг бодит орчинд 12 давхар байшин гэж төсөөлж үзээд тэр байшинд гэмт хэрэгтнүүд амьдарч, ажиллаж гэмт үйлдлээ хийж байгаа бол тэр байшинд хууль сахиулах байгууллагын алба хаагчид орж ажиллах л шаардлагатай болж байгаа юм.

Кибер гэмт хэргийн ул мөрийг 2 хэсэгт хувааж үзэх ба криминалистикийн болон цахим ул мөр үлдээдэг.

Криминалистикийн ул мөр гэдэг нь материаллаг үлдэж байгаа ул мөр буюу тодорхой тэмдэглэл, гар бичмэл, хэвлэмэл баримт мэдээлэл, компьютерын төхөөрөмж, CD, DVD, Flash, Hard дискүүд дээр үлдээсэн гар хурууны хээ, тухайн объектийн хяналтын камерын бичлэг зэрэг байж болно.

Мэдээллийн ул мөр нь компьютер дээрх мэдээллийг устгасан, өөрчилсөн, хаалт хийсэн эсвэл хуулбарласан талаарх ул мөр юм. Мөн мэдээллийн ул мөрд антивирусийн программуудын Windows/avp* Program болон Files/Anti Virtal Toolkit Pro/-д

үлдсэн Log файлд хадгалагдсан байж болно. Энэ төрлийн ул мөрийг илрүүлэх, бэхжүүлэхэд мэргэжилтэн зайлшгүй оролцуулах шаардлагатай.

Дээрх төрлийн гэмт хэргийг мөрдөн шалгах ажиллагаа явуулж байгаа алба хаагч доорх зүйлсийг зайлшгүй мэдэх шаардлагатай.

Цахим ул мөр нь шууд компьютер /тодорхой техник хэрэгсэл дээр/ болон шууд бус төхөөрөмж[1]-үүд дээр хадгалагдсан байж болдог. Халдлагын үед тоон ул мөр "Windows 10" үйлдлийн системийн хувьд интернет холболтыг ямар компанийн хаяг, IP хаяг ашиглан холбогдсон, уг хаягаар тухайн хэрэглэгчийн сүлжээнд тухайн Log файл /интернет сүлжээнд нэвтэрсэн үйлдлийг автоматаар хадгалдаг/-аар нэвтэрсэн цаг хугацаа, хэдий хугацаанд байрласан зэргийг тодруулж болдог ба тухайн компьютероос халдсан төхөөрөмж, сүлжээ, системийг тогтоох нотлох баримт болдог. Жишээ дурдахад тоон ул мөрүүд энэ энэ хавтасанд байж болзошгүй:

- /Windows/Temporary Internet Files/ хэсэгт - Интернетэд байрласан мэдээлэл,
- Windows/History хэсэгт - тухайн үйлдлийн системд ажилласан программуудын үр дүн буюу файлуудын түүхийг хадгалдаг. Үйлдлийн системүүдээс шалтгаалан уг мэдээллүүд нь өөр өөр газар хадгалагдах боломжтой байдаг.
- Windows/Cookies хэсэгт - Интернетэд орох үед мэдээлэл солилцсон талаарх түүх хадгалагддаг.
- /Windows/Downloaded Programm Files хэсэгт - тухайн үйлдлийн системд гаднаас ачаалагдсан файлуудын талаарх түүхийг харуулдаг. Нэг үгээр хэлэх юм бол вирус болон бусад байдлаар тухайн үйлдлийн системд нөлөөлөх програмууд ачаалагдсан байдлыг харуулдаг.
- /Windows/Aplication Data/ хэсэгт - цахим шуудангаар явуулсан, хүлээн авсан талаарх мэдээллийг харуулдаг.
- /Windows/Aplication Data/ Identities/Microsoft/Outlook хэсэгт - цахим шуудангаар явуулсан, хүлээн авсан талаарх мэдээллийг харуулдаг.
- /Windows/Aplication Data/Microsoft/Adress book хэсэгт - тухайн эзэмшигчийн хаягуудыг харуулдаг.
- /Windows/SchedLog.txt/ хэсэгт - тухайн үйлдлийн системийн төлөвлөлтийг харуулдаг.

Windows үйлдлийн системийн дээр үеийн хувилбарууд болох /2000, XP, 2003 гэх мэт/ дээр мөрдөгчид хэрэгцээ шаардлагатай мэдээллүүд нь хатуу диск дээр хадгалагдаж байж болдог. Жишээлбэл, C:/Documents and Settings/ хэсэгт мессеж, шуудангуудын архив, мөн интернет холболтын үед ямар ямар хаягт хандсан талаарх мэдээллүүд болон өөр чухал мэдээллийг хадгалагдсан байдаг.

Кибер гэмт хэргийн талаар гомдол мэдээллийг хүлээн авснаас хойш дээрх хүснэгтэд тусгагдсан мэдээллийг шалгах шаардлагатай юм.

ДӨРӨВ: КИБЕР ГЭМТ ХЭРГИЙГ МӨРДӨН ШАЛГАХ АЖИЛЛАГААНЫ ТАКТИК АРГА ЗҮЙ

Кибер гэмт хэргийг мөрдөн шалгах анхан шатны ажиллагаанд

[1] Шууд бус төхөөрөмж гэдгийг модем болон утасны холболт, хэт ягаан туяаны холболт болон бусад интернетийн холболт гэж ойлгоно.

мөрдөгч дараах ажиллагааг ЭХХШТХ-д заасан үндэслэл журмын дагуу зайлшгүй хийх шаардлагатай. Үүнд:

1. Хэрэг учралын газрын үзлэг,

2. Гэрч, хохирогчоос мэдүүлэг авах,

3. Хэрэгт ач холбогдолтой эд зүйлсийг хураан авах, шаардлагатай үед нэгжлэг хийх,

4. Шинжээч томилох ажиллагааг зайлшгүй явуулах шаардлагатай байдаг.

Хэрэг учралын газрын үзлэг. Тухайн гэмт хэргийн "Хэрэг, учралын газар" нь тодорхой газар орон, өрөө тасалгаа гэх зүйл байдаггүй.

Компьютерын техник хэрэгсэл нь тодорхой өгөгдлийг боловсруулах нэг үйлдлийн систем, эсвэл тодорхой систем, сүлжээний хэсэг болох компьютер байдаг. Хэрэв дээрх компьютерыг систем, сүлжээний хэсэгт хамааруулалгүй гэмт хэргийн зорилгоор ашиглаж байгаа бол хэргийн газар нь тодорхой өрөө тасалгаанд байгаа компьютер байх боломжтой, харин уг компьютерын систем, сүлжээг ашиглан гэмт хэрэг үйлдэж байвал тухайн гэмт хэрэг үйлдсэн газар нь алс хол байрлаж байдаг.

Үзлэг хийж болох объектууд нь:

1. Гэмт халдлага болсон мэдээллийн технологийг хадгалж, боловсруулж байгаа газар, компьютер, үйлдлийн систем;

2. Хөнөөлт программ вирус бүтээж байгаа, ашиглаж байгаа газар, компьютер, үйлдлийн систем;

3. Гэмт хэргийн замаар олж авсан мэдээллийг хадгалж байгаа газар, компьютер, үйлдлийн систем;

4. Гэмт халдлагад өртөж байгаа компьютер, үйлдлийн систем гэж Оросын холбооны улсын судлаачид [1] ангилсан байдаг.

Үзлэг эхлэхийн өмнө бэлтгэл ажлыг сайтар хангасан байх шаардлагатай. Тухайн ажиллагаанд оролцох мэргэжилтэн, техник хэрэгсэл, үзлэг хийх объектийн талаарх мэдээлэл болон үзлэг хийх хэмжээ хязгаарыг нарийвчлан тогтооно. Мэдээллийн технологийн мэргэжилтэнг үзлэгийн анхан шатнаас оролцуулах нь тухайн үзлэг хийж байгаа компьютер, мэдээллийг хадгалж байгаа төхөөрөмжийн онцлогийг тодорхойлж, ямар эд зүйлсийг хураан авах, хэрхэн бэхжүүлэн авах талаар үнэтэй зөвлөгөө өгдөг. Мөн үзлэгийн ажиллагаанд эрүүгийн төлөөлөгч, шинжээч криминалист, дүрс бичлэг хийх алба хаагчийг зайлшгүй бэлтгэн үзлэгийн онцлогийг тайлбарлан өгнө.

Хэргийн газрын үзлэгийн зорилго нь гэмт хэрэг үйлдэх хэрэгсэл болгон ашигласан мэдээлэл, программ зэргийг тогтоох зайлшгүй шаардлагатай тул доорх төхөөрөмжийг бэлтгэнэ. Үүнд:

1. DVD, CD унших төхөөрөмж, принтер, зөөврийн хард диск, зургийн аппарат, видео камер холбож болох ороллтой зөөврийн компьютер, эсвэл лабораторийн шинжилгээ хийх зориулалттай, тусгай программ суулгасан зөөврийн компьютер;

2. Бага хэмжээний принтер. Уг принтерээр үзлэгийн явцад илэрсэн файлуудын жагсаалт, үйлдлийн системийн шаардлагатай мэдээллүүдийг хэвлэх шаардлага гардаг;

[1] Тактика следсвенних дейсвий.Дворкин А.И и др. 2011 года, Москва 502 тал

3. Зөөврийн хатуу диск. Хэрэв тухайн үзлэг хийх гэж байгаа компьютерыг асаах боломжгүй, эсвэл тодорхой мэдээллүүдийг устгах эрсдэл байгаа бол уг дискэнд шаардлагатай мэдээллийг хуулбарлан авч үзлэг хийдэг.

4. Цахим ул мөр илрүүлэх зориулалт бүхий тусгай програм хангамж, тоног төхөөрөмж

Үзлэгийг эхлэхийн өмнө дараах зүйлийг анхаарах шаардлагатай. Үүнд:

1. Гэмт хэргийг илрүүлэх ач холбогдол бүхий мэдээллийг устгах эрсдэл байгаа эсэх;

2. Тухайн үзлэг хийх компьютер, мэдээллийг хадгалж байгаа төхөөрөмжид шаардлагатай нууц үгийг хийхгүй байх, эсвэл тодорхой хугацааны дотор нууц коноп дарах, эвсэл тусгайлан бэлтгэсэн үйлдэл хийгээгүй тохиолдолд хадгалж байгаа бүх мэдээллээ устгах программ, төхөөрөмж суурилуулсан эсэх;

3. Тухайн компьютер, мэдээллийг хадгалж байгаа төхөөрөмжийн эзэмшигчээс өөр хүн ашиглахаас хамгаалах зорилгоор хамгаалалтын программ, хэрэгсэл

Үзлэгээр тогтоох шаардлагатай нөхцөл байдал:

- Компьютерыг нүүрэн ба ар талаас нь, ялангуяа бусад төхөөрөмжтэй холбогдсон холболтын зургийг авах. Интернет холболтын модем, кабель шугам, эсвэл утасны шугамд холбогдсон эсэхийг шалгах, ул мөр, биологийн гаралтай болон бусад эд мөрийн баримт, бичиг баримт байгаа эсэхийг сайтар нягтлан шалгана;
- Компьютерыг унтраасан байвал асааж болохгүй;
- Компьютер асаалттай суурилуулсан эсэхийг эхлээд нарийвчлан шалгах шаардлагатай.

Дээрх эрсдэл үүсвэл зөвхөн мэргэжилтний зөвлөгөөний дагуу ажиллах тухайн төхөөрөмжид холбосон бүх холболтуудыг салгах, боломжтой бол тухайн хамгаалалтын системийг зогсоох арга хэмжээ авч, үүссэн нөхцөл байдлаас шалтгаалан цаашдын арга хэмжээг авна. Мөн тухайн үзлэг хийж буй тоног төхөөрөмж рүү “remote control” ашиглан хандах тохиргоог хийсэн эсэх, энэ төрлийн “team viewer” зэрэг бусад төрлийн програм хангамжийг суулгасан эсэхийг шалгаж, суулгасан тохиодолд тухайн төхөөрөмжийг сүлжээнээс салгаж, тоон ул мөрийг хамгаалах арга хэмжээг тухайн нөхцөл байдалдаа уялдуулан зайлшгүй авах хэрэгтэй. Нөгөөтэйгүүр гэмт этгээдэд дээрх төрлийн програм хангамжийг ашиглах нөхцөл боломжийг зориудаар хэвээр үлдээн мөрдлөгийн ажиллагааг үргэжлүүлэх нь зарим тохиолдолд илүү үр дүнтэй байхыг үгүйсгэх учир тухайн нөхцөл байдалдаа үнэлэлт дүгнэлт өгч зөв шийдвэр гаргах шаардлагатай.

бол унтраахгүй, товчлуур дээр дарах зэргээр ямар нэгэн нэмэлт үйлдэл хийж болохгүй;

- Дэлгэцэн дээрх дүрсийг гэрэл зургаар бэхжүүлж, боломжтой бол тухайн үед ажиллуулж байсан программ эсвэл windows-ыг тэмдэглэн авна;
- Цахилгааны утсыг компьютероос салгах эсвэл зөөврийн компьютер байвал цахилгааны утсыг салгаж батарейг байрнаас салгана[1];

[1] Болор-Эрдэнэ

- Тухайн компьютер болон бусад орчинд байгаа цахим төхөөрөмжүүдийн байршил;

- Тухайн компьютерын өнгө, загвар, хэлбэр, хэмжээ, серийн дугаар болон онцлог шинж;

- Тухайн компьютерт холбосон төхөөрөмжүүдийг ямар байдлаар холбосон болох, тэдний холболтын онцлог, сүлжээнд холбосон эсэх, хэрэв холбосон бол ямар хэлбэрээр холбосон болох, тухайн холболтуудын нэр, өнгө, загвар;

- Тухайн компьютер төхөөрөмжийн унтраалганы байдал;

- Тухайн компьютер төхөөрөмжийн ажиллагаатай эсвэл холболт байгаа эсэхийг илэрхийлсэн гэрлүүдийн байдал;

- Дэлгэц дээр байгаа файлуудын мэдээлэл, мөн тухайн компьютерын талаарх мэдээлэл өгч байгаа Taskbar хэсгийн мэдээлэл;

- Кабелаар холбосон эсэх, хэрэв холбосон бол өөр тусгай зориулалтын төхөөрөмж залгаатай байгаа эсэх, хэрэв байгаа бол тухайн төхөөрөмжийн онцлог;

- Тухайн компьютер төхөөрөмжид байгаа тусгай тэмдэглэгээ, тэмдэгтүүд, гадна талд байгаа лац, наалт, түүний онцлог;

- Механик гэмтэл байгаа зэргийг тодорхойлон бичиж, шаардлагатай бол гадна үзлэгийг хийн гарын мөрийг бэхжүүлэн авна.

- Компьютер асах үеийн “Boot” тохиргоог шалган “USB” оролтыг “Boot” дээр тохируулсан эсэхийг шалгана. Хэрэв тохиргоог шалгасанаас тухайн этгээд “USB” төхөөрөмж ашиглан давхар үйлдлийн систем ашиглаж байгаа эсэхэд үнэлэлт дүгнэлт хийх боломжтой. Түүнчлэн /live boot/ тухайн төхөөрөмж дээр давхар виарутал компьютер суулгасан эсэхийг нягтлах шаардлагатай. /VMWARE/

Компьютер, түүний тоног, хэрэгслийг хураан авахад “ЦБҮАЖ КОД-226”-д заасан дараах ажиллагааг зайлшгүй хийнэ:

- Эд зүйл бүрт хэргийн дугаар, эд мөрийн баримтын хуудасны дугаар, эд зүйлийн дугаар олгож бичих;

- Компьютер болон мэдээлэл, файл хадгалах төхөөрөмж /диск, мемори карт, флаш бусад драйвер/ тээвэрлэх, зөөвөрлөх явцад алдагдаж үрэгдэхээс сэргийлэх арга хэмжээ авна;

- Цахим хэрэгслийг бүрдэл хэсгийн хамт эд мөрийн баримт хадгалах өрөөнд хадгална. Хэт хүйтэн, чийгшил ихтэй, тоос шороотой орчинд компьютерын төхөөрөмжийг хадгалж болохгүй.

Шаардлагатай бол эд мөрийн баримтыг хураан авахдаа мэргэжилтний зөвлөгөөг даган битүүмжлэх.

Эд мөрийн баримтыг тээвэрлэхэд анхаарах асуудал:

1. Тухайн эд мөрийн баримтад механик хүчин зүйл нөлөөлөхгүй байх;
2. Цас, бороо, өндөр чийгшил зэрэг байгалийн хүчин зүйлс нөлөөлөхөөс сэргийлэх;
3. Цахилгаан соронзон орон үүсэхээс сэргийлэх;
4. Хэт халах, хэт хөрөхөөс сэргийлэх. Мэдээллийн технологитой холбоотой мэдээллийг хадгалах зориулалт бүхий төхөөрөмжүүд нь 0 градусаас +50 температурт хадгалагдах зориулалттай гэдгийг анхаарах.

Шаардлагатай эд зүйлсийг хураан авахад анхаарах асуудал:

1. Цахим төхөөрөмжтэй ажиллах журмыг зөрчиж, аливаа холболтыг хүчээр салгах, бэхжүүлэн авсан эд зүйлс, төхөөрөмжийг

бэхжүүлэн авах, битүүмжлэх, тээвэрлэхдээ гэмтээх;

2. Хурдан устах зориулалттай мэдээллийг хуулбарлан авах зориулалттай цэвэр дискгүй үзлэг хийх. Шаардлагатай тохиолдолд зарим мэдээллийг шууд хуулбарлан авах шинэ дискүүдийг үзлэгт бэлэн байлгах шаардлагатай;

3. Үзлэгийн тэмдэглэл техникийн үг хэллэгийг ямар нэгэн тайлбаргүйгээр шууд бичиж тэмдэглэх;

4. Хэрэгт ач холбогдолгүй техник хэрэгслийг хураан авах. Жишээлбэл компоютерийн дэлгэцийг хураан авах явдал байдаг. Дэлгэц нь мэдээллийг харуулах зориулалттай төхөөрөмж, харин хадгалах зориулалтгүй гэдгийг анхаарч шаардлагатай эд зүйлсийг хураан авах;

5. Хатуу диск дээр мэдээллийг хуулбарлахаас өмнө компьютерыг асаасны улмаас шаардлагатай мэдээллийг устгах эрсдэл байгаа эсэхийг шалгах.

Гарын мөрийг бэхжүүлэн авсны дараа мэргэжилтнээр үзлэг хийлгэн, шаардлагатай бол зөөврийн хатуу дискээр шаардлагатай мэдээллүүдийг хуулбарлуулан авч тухайн хэргийн онцлогт тохирсон үзлэгийг явуулна. Боломжтой бол тухайн үзлэгийг дүрс бичлэгийн аппаратаар бэхжүүлэх нь нотлох баримтын өндөр ач холбогдолтой байдаг.

Мэдээллийн технологитой холбоотой эд мөрийн баримтыг хураан авах:

1. Тухайн эд зүйлсийг тусгай зориулалтын үйлдвэрлэгчээс ирүүлсэн уут сав нь байвал уг уутанд хийн, савлах.

2. Мэдээлэл хадгалах зориулалт бүхий төхөөрөмж бүрийг тус тусад нь гялгар уут, цаасан дугтуй, хуванцар саванд хийх. Хэрэв дээрх уут байхгүй бол цаасаар нямбай ороож, цахилгаан соронзон орон үүсгэхгүйн тулд ахуйн хэрэглээний хөнгөн цагааны хольцтой туузаар орох.

3. Компьютерын процессор зэргийг үйлдвэрлэгчийн уут, сав байхгүй бол модон хайрцагт хийн, хөдөлгөөнийг байхгүй болгох зорилгоор картон хайрцаг, хатуу цаасаар зай завсрыг дүүргэх.

4. Тухайн баглаа боодол бүрийг битүүмжлэн, хэргийн товч утгыг бичэн, ямар төхөөрөмж байгааг тодорхой заан хаяглан, лацдах, уг тэмдэглэгээг үзлэгийн тэмдэглэл тусгах.

Гэрч, хохирогчоос мэдүүлэг авах. Мэдүүлэг авах ажиллагааны явцад гэмт хэрэг гарахаас өмнө 3-4 хоногт компьютер дээрээ хийсэн ажиллагаануудын талаар хохирогч, гэрчээс дэлгэрэнгүй тодруулан, ямар интернет сайтуудаар орсон, ямар шинэ программ татаж суулгасан, ямар сүлжээ ашигладаг болох [1], өөр хүн тухайн компьютер дээр ажилласан эсэх, ямар нэгэн төхөөрөмж холбосон эсэх, тухайн компьютер дээрх ач холбогдол бүхий мэдээллийг ямар хүн мэддэг болох, мөн тухайн компьютерын нууц үгийг хэн мэддэг болох, тухайн офисс, албан байгууллагын хамгаалалт зэргийг тодруулан дэлгэрэнгүй мэдүүлэг авна.

Мөн тухайн гэрч, хохирогчийн хувийн байдлыг, ялангуяа техникийн мэдлэгийн талаарх мэдээллийг дэлгэрэнгүй судлан үзэж, гэмт хэрэг

[1] О.А. Егерева “Некоторые вопросы методики расследования киберпреступлений” журнал «Государство и право. Юридические науки»

гарсан мэт байдлыг үүсгэсэн байх боломжийг шалгах шаардлагатай.

Хэрэгт ач холбогдолтой эд зүйлсийг хураан авах, шаардлагатай үед нэгжлэг хийх. Хураан авах, нэгжлэг хийх ажиллагааны үр дүн нь бэлтгэл ажиллагаатай салшгүй холбоотой. Үүнд:

- Хураан авах цахим мэдээлэл нь ямар байдлаар, ямар төхөөрөмжид хадгалагдаж байгаа болох;

- Хураан авах, нэгжлэг хийх ажиллагаа явагдах объектийн талаарх дэлгэрэнгүй мэдээлэл, уг газар телефон болон интернет сүлжээ байдаг эсэх, хураан авах гэж байгаа техник хэрэгсэл, компьютер нь уг төхөөрөмжтэй холбоотой эсэх;

- Уг объектын цахилгааны самбар, сүлжээний холболтын ерөнхий самбар нь хаана байрладаг болох, хураан авах гэж байгаа төхөөрөмжийг ямар нэгэн байдлаар хамгаалсан эсэх;

- Тухайн эд зүйлсийг хураан авах гэж байгаа этгээдийн талаар судлан, хураан авах, нэгжлэг хийх объектод өөр хүн амьдардаг эсэх, хэрэв байдаг бол тухайн хүний өдөр тутмын дадал, зуршил, техникийн мэдлэг зэргийг тогтоох;

- Хураан авах, нэгжлэг хийх ажиллагаанд оролцуулах мэргэжилтэн, хөндлөнгийн гэрч /техникийн мэдлэгтэй байхыг анхаарах/;

- тусгай зориулалтын техник хэрэгсэл, хураан авсан эд зүйлсийг хадгалах, зөөвөрлөх хайрцаг, савыг бэлтгэх.

Хураан авах, нэгжлэг хийх ажиллагааг явуулахдаа тоймчилсон болон нарийвчилсан байдлаар үзлэг хийдэг. Тоймчилсон үзлэг хийхдээ цахим мэдээллийн хэргийн ердийн үзлэг хийх, журам, дэс дарааллын дагуу явуулан эд зүйлсийг хураан авна. Харин нарийвчилсан үзлэгийг ажлын байран дээрээ явуулах нь үр дүнтэй байдаг[1].

Шинжээч томилох. Тоон технологийн шинжилгээ гэдэг нь ихэвчлэн кибер гэмт хэрэг мөрдөх явцтай холбоотойгоор, тоон технологи дээр суурилсан төхөөрөмжийн санах ойд агуулагдаж байгаа мэдээллийг сэргээх, шинжлэх асуудлыг дагнан судалдаг шүүх шинжилгээний нэг салбарыг хэлнэ.

Одоо олон улсын хэмжээнд, тоон мэдээлэл хадгалах чадвартай бүх төхөөрөмжийг шинжлэх гэдэг ухагдахуунд хамруулж ойлгож, дараах төрлүүдээр шүүх шинжилгээ хийж байна:

- Компьютерт хийх шүүх шинжилгээ (Computer forensics)– зөөврийн ба суурин компьютерын хатуу диск болон бусад хатуу диск, флаш диск... мэт төхөөрөмжийн санах ойд хийх шүүх шинжилгээ.

- Сүлжээнд хийх шүүх шинжилгээ (Network forensics)- Сүлжээ, сервер зэрэгт хийх шүүх шинжилгээ.

- Гар утсанд хийх шүүх шинжилгээ (Mobile device forensics) - бүх төрлийн гар утас, GPS гэх мэт төхөөрөмжид хийх шүүх шинжилгээ.

- IoT forensics - internet of things, drones … хийх шүүх шинжилгээ.

- Мултимедиад хийх шүүх шинжилгээ (Multimedia forensics) - дүрс бичлэг, дуу авиа, дүр зураг зэрэг мультимедиад хийх шүүх шинжилгээ.

- Үүлэн орчинд хийх шүүх шинжилгээ (Cloud forensics)- үүлэн

[1] Будилов А.М “Киберпреступления: криминалистическая характеристика и особенности расследования” Вологда – 2016

орчинд хийх шинжилгээ, онлайн хост үйлчилгээн хийх шүүх шинжилгээ.ххх

- Дүрс өгөгдөлд хийх шүүх шинжилгээ (Digital image forensic) - гэрэл зураг болон бусад дүрсэд хийх шүүх шинжилгээ.

- Санах ойд хийх шүүх шинжилгээ (Memory forensic)- ажиллаж байгаа компьютерын RAM (Шуурхай санах ой)-д хийх шинжилгээ.

Шүүх шинжилгээний эсрэг (Antiforensic) -тоон мэдээлэлд оруулсан аливаа өөрчлөлтөд хийх шүүх шинжилгээний үйл ажиллагаанд саад учруулах, хүндрүүлэх зорилгоор оруулсан өөрчлөлтийг тогтоож, эх хувьд байсныг тогтоохоор хийх шүүх шинжилгээг тус тус хийдэг.

Одоогийн байдлаар Монгол Улсын хэмжээнд Шүүхийн шинжилгээний үндэсний хүрээлэнгийн Криминалистикийн шинжилгээний газрын Гэрэл зураг-дүр зураг, дүрс бичлэгийн лабораторид дараах шинжилгээг хийж байна. Үүнд:

- Компьютер техник - зөөврийн компьютер, суурин компьютер, дата мэдээлэл хадгалдаг төхөөрөмжүүд (хатуу диск, мемори картууд)...хийх шүүх шинжилгээ.

- Гар утас болон бусад - бүх төрлийн гар утас, SIM карт, PDA, GPS төхөөрөмж, таблет... хийх шүүх шинжилгээ.

- Дүрс бичлэг - Дүрс бичлэгийн төхөөрөмж, дүрс бичлэгүүдэд хийх шүүх шинжилгээ.

- Дуу авиа - Дуу авианы бичлэг, дуу авиатай дүрс бичлэг, дуу авиа, дүрс бичлэг бичигдсэн төхөөрөмжид хийх шүүх шинжилгээ.

- Дүр зураг - Аман зураг, дүр төрхийн адилтгалхийх шүүх шинжилгээ[1].

Шинжилгээ хийлгэх бол шинжээч томилсон тогтоолын хамт тухайн эд мөрийн баримтаас гадна дор дурдсан зүйлсийг хүргүүлэх талаар ЦБҮАЖ КОД-226-д заасан. Үүнд:

- Хураан авсан тэмдэглэлийн хуулбар;

- Шинжилгээгээр олж тогтоох зүйлийн жагсаалт /фото зураг, санхүүгийн бүртгэл, емэйл, бичиг баримт гэх мэт/ бөгөөд эдгээрийг тогтоолд зааж өгнө. Цахим мэдээлэл агуулсан хард диск, флоппи диск, CD, DVD, хуурцаг, мемори карт, флаш зэрэг төхөөрөмжийг хураан авахдаа дижитал мэдээлэл устаж гэмтэхээс урьдчилан сэргийлэх арга хэмжээ авна гэж заагаад дараах журмыг тодорхойлж өгсөн байдаг.

- Тухайн хэрэгсэл нь хуулбарлан авахаас сэргийлсэн унтраагуурtай бол түүнийг идэвхжүүлнэ;

- Шинжилгээнд хүргэж өгөхөөс өмнө дижитал файлыг нээх, үзэхийг хориглоно;

- Мэдээлэл шаардлагатай болсон үед тухайн хураан авсан цахим хэрэгсэлд байгаа мэдээллийг зохих хэрэгсэлд хуулбарлан авах хүсэлт тавина;

- Дижитал мэдээлэл агуулсан хэрэгслүүд цахилгаан соронзон орны орчинд устгагдах, гэмтэх аюултай байдаг. Иймээс эдгээр төхөөрөмжүүдийг соронзон хэрэгслүүд, тухайлбал цахилгаан мотор, радио дамжуулагч болон бусад соронзон эх үүсвэр бүхий төхөөрөмжүүдээс тусад нь хол

[1] Ц.Болор-Эрдэнэ “Тоон технологийн шинжилгээ” 2019

хадгална;

- Ердийн дулаанаас хэт өндөр температуртай газар жишээлбэл халуун өдөр автомашин дотор тавьж орхих зэрэг байдлаар цахим мэдээлэл хадгалсан хэрэгслийг хадгалж болохгүй;

- Эвдэрч, гэмтэхээс урьдчилан сэргийлсэн зориулалтын битүүмжлэл бүхий хайрцаг, саванд хадгалах ёстой[1].

Мөн цахим төхөөрөмжид хадгалагдаж байгаа бүх төрлийн мэдээллийг арилгах, устгах, гэмтэхээс сэргийлэх зорилгоор дор дурдсан журмыг баримтална гэжээ. Үүнд:

- Шинжилгээнд оруулахаас өмнө тухайн төхөөрөмжид байгаа мэдээллийг үзэх, агуулгыг хайх зэргээр оролдож болохгүй. Ингэж оролдсоноор илгээгээгүй, гаднаас хүлээн авсан мессеж устгагдах, хадгалагдсан мессежнүүд давхардах зэрэг ноцтой үр дагавар гарч болзошгүй байдаг;

- Тухайн төхөөрөмжийг асаах, эсвэл унтрааж болохгүй. Төхөөрөмжийг металл хайрцаг эсхүл зориулалтын сав, хайрцагт хийж сүлжээний холболтыг нь таслахгүй байх нөхцөлийг хангана;

- Төхөөрөмжийг хураан авахад цэнэглэгч нь байвал шинжилгээ хийх хүртэл түүнийг салгахгүй байлгана. Цэнэг нь дуусвал төхөөрөмжид байгаа мэдээлэл алдагдах, устаж болзошгүй.

Цагдаагийн албан хаагч цахим /биет бус/ мэдээллийг бэхжүүлэхдээ “Дүрс, дуу бичлэг хийх зориулалтын төхөөрөмжөөс нотлох баримтыг цахим хэлбэрээр хуулбарлан авах шаардлагатай бол алба хаагч тухайн нотлох баримтыг устаж үрэгдэхгүй байх нөхцөлийг бүрэн хангаж мэргэжилтэнг байлцуулан гүйцэтгэнэ” гэж заасан.

Мөн дүрс, дуу бичлэг хийх зориулалттай бусад төхөөрөмжийг хураан авахад дор дурдсан журмыг баримтална:

- Дижитал хэрэгсэл /смарт карт, компакт карт, бусад картууд/-ийг нотлох баримтаар хураан авсан тохиолдолд нэн даруй эд мөрийн баримт хадгалах өрөөнд хүргүүлнэ;

- Мемори болон бусад картыг шалгах болон хуулбарлаж болохгүй. Зөвхөн компьютерын мэргэжилтний тусламжтайгаар картад байгаа мэдээллийг боломжтой хэлбэрээр бэхжүүлнэ;

- Нотлох баримтаар хураан авсны дараа камераас мемори картыг салгаж тусад нь гялгар уутанд хийх ёстой. Дараа нь гялгар уутанд хийсэн мемори картыг тусгай уутанд хийж амсрыг нь битүүмжлэн уутны гадна талд хураан авсан ажилтны нэр, хэргийн дугаар, огноог бичнэ;

- Мэргэжилтний тусламжтайгаар хадгалах төхөөрөмж ашиглан мемори болон бусад карт дээрх мэдээллийг хуулбарлан авна;

- Камераар зураг авсан тохиолдолд компьютерын мэргэжилтэн зургийг камераас зохих төхөөрөмжөөс хуулбарлан авсны дараа камерын мемори картад байгаа мэдээллийг устгаж дахин ашиглахад бэлэн болгоно.

Дижитал нотлох баримтыг хадгалахдаа цахим мэдээлэл бүхий нотлох баримтад ямар нэгэн өөрчлөлт хийж болохгүй гэж заасан ба мэдээллийн нууцыг задруулахыг хориглосон байна.

Мөн Цахим эд мөрийн баримт нь шинжилгээний явцад устах, гэмтэх эрсдэлтэй тул эх хувийг лацдан хадгалж, хуулбарласан хувийг шинжилгээний байгууллагад

[1] ЦБҮАЖ КОД-226

битүүмжилж хүргүүлнэ[1].

Компьютер техникийн шинжилгээгээр:

1.Шинжилгээнд хүргүүлсэн компьютер нь ямар марк загварын, техникийн үзүүлэлттэй болох?

2.Мэдээллийг боловсруулах төхөөрөмжийн хүчин чадал нь ямар үзүүлэлттэй болох?

3. Тухайн компьютер нь үйлдвэрлэгчээс гаргасан загвараар, эсвэл гар аргаар угсарсан эсэх? Тухайн компьютерт нэмэлт ямар нэгэн төхөөрөмж суурилуулсан эсэх?

4. Тухайн компьютерыг ашиглах боломжтой эсэх? Хэрэв боломжгүй бол ямар учраас?

5. Тухайн компьютерын хүчин чадал нь өөрт нь суулгасан программ хангамжуудыг ачааллан ажиллах боломжтой эсэх?

6. Тухайн компьютерын мэдээлэл хадгалах зориулалттай төхөөрөмжүүд бүрэн ажиллагаатай эсэх?

Өгөгдөлд шинжилгээ хийлгэхэд шинжээчид тавих жишиг асуулт:

1. Энэхүү файл нь хэзээ, хаана, ямар тоон технологи дээр суурилсан төхөөрөмжид үүсгэгдсэн болох?

2. Энэхүү программ нь ямар зориулалтын, ямар үйлдэл гүйцэтгэдэг болох?

3. Энэхүү программыг бүтээсэн этгээдийн мэдээлэл байгаа эсэх?

4. Энэхүү программ нь хандалтын бүртгэл явуулдаг эсэх? Хэрэв хандалтын бүртгэл явуулдаг бол хандалтын бүртгэлийг өөрчлөх, устгах боломжтой эсэх, устгасан тохиолдолд сэргээх боломжтой эсэх?

5. Энэхүү программ нь хууль бус хандалтаас хамгаалсан хамгаалалтын функц байгаа эсэх?

6. Энэхүү программд /файл, өгөгдөл/ хортой код байгаа эсэх, хэрэв байгаа тохиолдолд ямар үйлдэл гүйцэтгэдэг болох?

7. Шинжилгээнд хүргүүлсэн серверт байх ХХХ нэртэй мэдээлэл бүхий өгөгдөл /мэдээлэл/ ямар багтаамжтай болох?

8. Уг өгөгдөлд /файл/ байх мэдээллийг хамгийн сүүлд хэзээ шинэчилсэн, нэмсэн, ашигласан болох?

9. Уг өгөгдөлд /файл/ байх мэдээллийг ямар /IP хаягтай/ сериал дугаартай компьютероос ямар хэмжээтэй мэдээллийг хэзээ хуулсан, арилгасан өөрчилсөн

Шинжээчид тавих асуултыг тухайн хэргийн онцлогоос шалтгаалан сонгож тавих нь хурдан шуурхай шинжилгээ явуулах ач холбогдолтой байдаг.

ТАВ: КИБЕР ГЭМТ ХЭРГИЙГ МӨРДӨН ШАЛГАХ АЖИЛЛАГААНД АШИГЛАЖ БАЙГАА ОРЧИН ҮЕИЙН ТЕХНИК ТЕХНОЛОГИ

Дэлхий дахинд гэмт хэрэг илрүүлэх нотлох үйл ажиллагаанд хэрэг учралын болон цахим сүлжээнээс тоон нотлох баримтыг илрүүлэх, хураан авах, баталгаажуулах, шинжлэх, шүүхийн шатанд нотлох үйл ажиллагаанд хэш “Hash” функцийн утгыг ашиглан нотлох баримтын эх, бүрэн бүтэн байдлыг баталгаажуулахад ашиглаж байна.

Монгол Улсын Ерөнхий

[1] Монгол Улсын Ерөнхий прокурорын 2017.07.16-ны өдрийн А/80 дугаартай тушаал

прокурорын 2017 оны 07 дугаар сарын 16-ны өдрийн А/80 дугаартай тушаалаар баталсан “Эрүүгийн хэрэгт хөрөнгө, орлого, барьцааны мөнгө, эд мөрийн баримт, эд зүйлийг хураан авах, бэхжүүлэх, хүлээн авах, хадгалах, хамгаалах, шилжүүлэх, шийдвэрлэх журам”-д “...Цахим баримтыг мэргэжилтний тусламжтайгаар тусгай техник хэрэгсэл, программ ашиглан хуулбарлан авч, засварлаж өөрчлөх боломжгүйгээр код үүсгэн “hash” /хэшлэх-тусгай программ ашиглах/, хөндлөнгийн 2-оос доошгүй гэрчийг байлцуулан, энэ тухай тэмдэглэл үйлдэж, үйл явцыг гэрэл зураг, дуу-дүрсний бичлэгээр бэхжүүлэн, байлцсан хүмүүсээр гарын үсэг зуруулах...” талаар тусгасан байна.

Хэш функц /hash function-таташ хийх[1]/ гэдэг нь мэдээллийн агуулгыг нуух, өөрчлөлт хийх, бусад этгээдүүд зөвшөөрөлгүй хандалт хийхээс сэргийлэх зорилгоор үндсэн өгөгдлийг хувиргах аргыг ашиглан “Мэдээллийн системийн өгөгдлийн аюулгүй байдлыг хангах” нэг төрлийн арга юм.

Судлаач Ц.Болор-Эрдэнэ өөрийн судалгааны ажилдаа доорх байдлаар тайлбарласан байна. Хэш утга нь санхүүгийн эсвэл хувийн гэх мэт нууцлал шаардсан өгөгдлийг хадгалах болон дамжуулах үед өгөгдлийн нууцлалыг хамгаалах, өгөгдөлд өөрчлөлт орсон эсэхийг, мөн файлыг өөрчилсөн хүн эсвэл төхөөрөмжийг илрүүлэх зэргээр өгөгдлийн бүрэн бүтэн байдлыг шалгахад ашигладаг.

Энэхүү функцийн ажиллагаа нь тоон өгөгдлийг уншиж шинжлээд түүнээс бичил мэдээлэл үүсгэдэг. Энгийн үгээр хэлбэл энэхүү функцийн үйлдэл нь ямар нэгэн юмнаас сорьц, дээж авч орц, найрлагыг нь тогтоох үйлдэл буюу ДНК-ын шинжилгээ авч, хариуг нь гаргахтай төстэй зүйл юм.

Файлын хэмжээ, өргөтгөлөөсөө хамаарахгүй “найрлага” буюу хэш-ийн хэмжээ нь ижил байдаг. Ялгаатай 2 файл ижил найрлага үүсгэх боломжгүй. Нэг тэмдэгт өөрчилсний дараа хэш функцээр шинжлэхэд “найрлага” нь дахин өөрчлөгдсөн байдаг. Харин өөрчилсөн тэмдэгтээ буцааж хэвэнд нь оруулаад хэш функцээр шинжлэхэд “найрлага” анхны байдалдаа орно.

Энэ функцийн гол онцлог нь үндсэн өгөгдлийг өөрчилсөн “найрлага”-аас эх мэдээллийг нь гарган авах боломж байдаггүй бөгөөд ямар нэгэн нууцлагч, нууц тайлагч түлхүүр ашигладаггүй. Тоон нотлох баримтын хэш утгыг гаргах үйл явц нь математик тооцоолол дээр үндэслэдэг бөгөөд тодорхойлогдсон тооцооллоор өгөгдлийн нэг мөрөнд тогтмол хэмжээтэйгээр үргэлжилсэн үсэг тоон тэмдэгтийн алгоритм үүсгэдэг.

Практикт MD (Message Digest) болон SHA (Secure Hash Algotithm) алгоритмын төрлүүдийг хэш функцэд түгээмэл ашигладаг. Дэлхий нийтэд тоон технологийн шинжилгээнд MD5 болон SHA1 алгоритмуудыг хослуулан түлхүү ашигладаг.

Түлхүүр, элемент гэсэн хосуудаас бүрдсэн өгөгдөлд хандахдаа түлхүүр дээр тодорхой боловсруулалт (хэш функц) хийж гаргаж авсан индексээр хэш гэж нэрлэгдсэн хүснэгтэд хандаж өгөгдлийн элементэд хандаж болдог бүтэц юм.

Олон төрлийн Хэш функц шинжлэн гарган авдаг програм байдаг боловч “**HashMyFiles**” нь тоон технологийн шинжилгээнд /digital

[1] ru.wikipedia.org

forensic/ зориулагдсан хэрэглэхэд хялбар программ юм.

HashMyFiles нь Аливаа өгөгдлөөс MD5 болон SHA1 алгоритмыг шинжилдэг жижиг хэмжээний /Tools/ программ бөгөөд 2007 онд *NirSoft веб сайтын* Windows үйлдлийн системд зориулсан.

Шинжилж авсан MD5 болон SHA1 алгоритмыг хялбар аргаар хуулбарлах, Text, HTML,XML өргөтгөлөөр хадгалж авах боломжтой. Hashmyfiles программ нь Windows Explorer-ийн context цэснээс ачааллаж болох ба мөн сонгогдсон файл, хавтсын MD5 болон SHA1 алгоритмыг харуулна.

WindowsXP, 2000, 2003,Vista, Windows 7, Windows 8, Windows 10 үйлдлийн системүүд дээр ажилладаг. HashMyFiles программыг суулгахад ямар ч суулгах процесс эсвэл нэмэлт DLL файл шаарддаггүй бөгөөд зөөврийн флаш диск, CD-с хүртэл ачааллах боломжтой. Мөн HashMyFiles нь Windows Explorer–с ачааллах боломжтой. Энэ программ нь үнэгүй ямар нэгэн лиценз шаардлагагүй ба Англи, Герман, Унгар, Итали, Япон, Бразил, Орос, Хятад, Спайн, Тайланд, Венесуэл гэх мэт хэл дээр ашиглах боломжтой юм[1].

Мөн уг программыг ШШҮХ-ийн Дүр зураг, дүрс бичлэгийн лабораториос хуулбарлан авах боломжтой талаар дурджээ.

ЗУРГАА: КИБЕР ГЭМТ ХЭРГИЙГ МӨРДӨН ШАЛГАХ АЖИЛЛАГААНД ТУЛГАМДАЖ БУЙ АСУУДАЛ

Монгол Улсад кибер гэмт хэрэг мөрдөн шалгах ажиллагаа явуулахад тулгамдаж байгаа асуудлыг дараах байдлаар тодорхойлдог. Үүнд:

1. Дээрх төрлийн хэргийг мөрдөн шалгах ажиллагаа явуулах, хяналт тавих, шүүхээр эцэслэн шийдвэрлэх туршлага байхгүй,
2. Дээрх төрлийн хэрэгт мөрдөн шалгах ажиллагаа явуулах цахим мэдээллийн чиглэлээр өндөр мэргэшсэн эрүүгийн процессын мэдлэгтэй мөрдөгчид дутмаг,
3. Цахим мэдээллийн хэрэгт хийх шинжилгээг бүрэн дүүрэн явуулах боломжгүй байдал,
4. Цахим мэдээллийн хэрэгт мөрдөн шалгах ажиллагаа явуулах нэгдсэн стандарт байхгүй [2]
5. Олон улсын хамтын ажиллагаа

Кибер гэмт хэрэг нь Монгол улсад харьцангуй шинэ төрлийн гэмт хэрэгт тооцогдож байгаа тул мөрдөн шалгах эрх бүхий байгууллага, прокурор, шүүхийн байгууллага тухайн хэргийг шийдвэрлэх нэгдсэн арга барил, туршлага хомс байгаа нь хэргийг нэгдсэн нэг ойлголтгүй байх, нотлох баримтыг үнэлэхэд хүндрэл учирч байна. Зөвхөн цахим орчинг ашиглан үйлдсэн залилах, далайлган сүрдүүлэх гэмт хэргийг л шийдвэрлэж байна.

Монгол Улсад үйлдэгдэж байгаа цахим гэмт хэргийн анхан шатны ажиллагааг явуулж буй мөрдөгчид тухайн гэмт хэргийн талаарх ойлголт дутмаг, цахим мэдээллийн мэргэшилгүй тул анхан шатны нотлох баримтыг устгах, хэргийг нотлох баримтыг бүрэн дүүрэн цуглуулах ажиллагааг гүйцэд явуулж чадахгүй байх тохиолдол нь практикт байна. Өөрөөр хэлбэл, тухайн төрлийн гэмт

[1] Ц.Болор-Эрдэнэ “Тоон технологийн шинжилгээ” 2019

[2] Нестерович С.А. “Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов”. Вестник науки и образования № 8(44) 2018. Москва

хэрэгтэй тэмцэхээр Эрүүгийн цагдаагийн албанд Кибер гэмт хэрэгтэй тэмцэх хэлтэс ажиллаж байгаа нь хангалтгүй байна. Учир бусад нутаг дэвсгэр хариуцсан алба хаагчид, прокурор, шүүгчдийг давхар мэргэшүүлэх шаардлагатай юм.

Тухайн төрлийн гэмт хэргийн талаарх гомдол мэдээллийг хүлээн аваад хийгдэх ажиллагаа, эд мөрийн баримт хураан авах, хадгалах, хамгаалах, шинжилгээнд хүргүүлэх талаар нэгдсэн стандарт хэлбэрийн төдий байгаа нь тухайн төрлийн гэмт хэргийг илрүүлэх, нотлох, эцэслэн шийдвэрлэхэд практикт хүндрэл учирч байна.

Мөн тухайн гэмт хэрэгт хийгддэг 9 төрлийн шинжилгээг Монгол Улсад бүрэн дүүрэн хийх боломжгүй, мэргэшсэн лаборатори, мэргэжилтэн дутмаг байна. Компьютер техникийн шинжилгээг Шинжилгээний байгууллагаас гадуур хийлгэх боломжийг судлан, бусад байгууллагатай хамтран ажиллах бололцоог бүрдүүлэх шаардлагатай. Оросын Холбооны Улсад дээрх төрлийн шинжилгээний 58 хувийг төрийн байгууллагаас гадна байх шинжилгээний байгууллагаар хийлгэж[1] байсан нь үр дүнгээ өгсөн талаар тухай орны судлаачид дурджээ.

Олон улсын хамтын ажиллагаа дутмаг байгаа нь тухайн гэмт хэргийг мөрдөн шалгахад зайлшгүй шаардлагатайг харуулж байна. Жишээ нь гэмт этгээдүүд сошиал сайтуудаар хохирогчдын судалгааг нарийвчлан хийж тэтгэврийн насны, ганц бие эмэгтэйчүүдийг онцлон харилцаа тогтоож, ихэнх тохиолдолд өөрийгөө АНУ-ын армид удирдах албан тушаалтай хэмээн танилцуулан удаан хугацааны туршид харилцаж итгэлийг олж авч, улмаар Монгол Улсад очно, хамт амьдарна гэж худал төрүүлдэг. Мөн аль нэг гадаад улсын дансанд гацсан их хэмжээний мөнгөө Монгол Улс руу гуйвуулахад гарах зардал, шимтгэл гэх нэрийдлээр их хэмжээний мөнгө гадаад улсын данс руу шилжүүлэн авдаг [2] . Тухайн гэмт хэргийг гадаад улсаас үйлдсэн тул “Эрх зүйн харилцан туслалцаа үзүүлэх” эрх зүйн орчинг бүрдүүлэх, тухайн улстай байгуулаагүй байгаа нь мөрдөн шалгах ажиллагааг явуулах боломжгүй болгодог.

ДҮГНЭЛТ

Монгол улсын хэмжээнд 2023 онд бүртгэгдсэн нийт гэмт хэргийн 0.7 хувийг Кибер аюулгүй байдлын эсрэг гэмт хэрэг эзэлж байгаа нь бага харагдаж байгаа боловч өмнөх жилийн мөн үеэс 71.5 хувиар, сүүлийн 5 жилд бүртгэгдсэн гэмт хэрэг нь өмнөх 5 жилийн мөн үеэс 8.5 дахин өссөн байгаа нь уг гэмт хэргийн гаралт цаашид тасралтгүй өсөх хандлагатай байна. Иргэд өөрийн мэдээллийн аюулгүй байдлыг хангадаггүй, хайнга ханддаг, ач холбогдол өгдөггүй, аж ахуй нэгжүүд өөрийн цахим хуудас, байгууллагын мэдээллийн аюулгүй байдлыг хангах нэгж байдаггүй зэрэгтэй холбоотой байна.

Бүртгэгдсэн нийт хэргийн 66.7 хувь нь фэйсбүүк орчинтой холбоотой, хохирогч нарын ихэнх нь өөрийн буруутай үйлдлээс шалтгаалсан байгаа нь иргэдийн мэдээллийн аюулгүй байдлын талаар мэдлэг тааруу, кибер орчин дахь аюул, халдлагаас хамгаалах аргад суралцаагүй зэрэг байдлаас гадна бусдад итгэх итгэл, аливаа мэдээллийг

[1] https://ceur.ru – “Центр экспертиз при институте судебных экспертиз и криминалистики” албан ёсны сайт

[2] “Зууны мэдээ” сонин №165 /5872/

нягтлалгүй ханддаг байдлаас шалтгаалж байна.

Хохирогч нарын боловсрол, нийгмийн байдал, нас зэрэг нь тухайн төрлийн гэмт хэргийн хохирогч болоход ямар нэгэн нөлөө байхгүй харагдаж байна. Харин дээд боловсролтой, компьютер техникийн чиглэлийн өндөр мэдлэгтэй хүн гэмт хэрэг үйлдэх нь бага байна. Компьютерын сүлжээний орчны талаар сонирхдог, мэдээлэл хайдаг, олсон мэдээллээ туршиж үзсэн гэх мэтчилэн өгүүлэмжтэй гэмт хэргийн холбогдогч нар олширсон байна. Энэ төрлийн гэмт хэргийг үйлдэхдээ нэг аргаар, олон хохирогч нарыг хамруулан богино хугацаанд олон гэмт хэрэг үйлдэх боломжийг ашиглаж байна.

Мөн урьд ажиллаж байсан ажил, албан тушаалаа ашиглан гэмт хэрэг үйлдэх явдал ихсэх хандлагатай байна. Иймд цахим орчинд /кибер/ үйлдэгдэх гэмт хэргээс урьдчилан сэргийлэх, мөрдөн шалгах үйл ажиллагааг зохион байгуулах мэргэжлийн удирдлагаар хангах нь чухал.

САНАЛ

Иймд Кибер аюулгүй байдлын эсрэг гэмт хэрэгт хийсэн шинжилгээний үндсэнд дараах саналыг гаргаж байна.

1. Уг төрлийн гэмт хэрэгт өртсөн иргэд хохирол бага, аливаа мэдээллээ алдаагүй, би өөрийгөө хамгаалж чадсан, энэ талаар мэдээлэл олон нийтэд тарвал байгууллагын нэр хүндэд муугаар нөлөөлнө гэх ойлголтоос болж холбогдох байгууллагад хандахгүй байх тохиолдол их байна. Энэ нь Монгол улсад бүртгэгдэж буй гэмт хэргийн статистик мэдээ, цаашлаад Кибер аюулгүй байдлын талаар авч хэрэгжүүлэх бодлого, түүнээс гарах шийдвэрт сөргөөр нөлөөж байх тул аливаа гэмт хэргийн талаар холбогдох байгууллагад шуурхай мэдээлж байх,

2. Иргэдэд аливаа цахим хэрэгсэл, программ хангамж нь аюулгүй байдлаа бүрэн хангасан байх, мэдээллийн аюулгүй байдал, кибер халдлагын талаар тогтмол мэдээлэл өгөх, энэ төрлийн гэмт хэргийн хохирогч нар хэрхэн гэмт халдлагад өртсөн талаар кейс дээр урьдчилан сэргийлэх, танин мэдүүлэх үйл ажиллагааг байнга зохион байгуулах,

3. Цахим орчинд байршиж буй аливаа гэмт хэргийн шинжтэй үйлдэл, зарлал, фишинг зэргийн шүүдэг нэгж байгуулах, шинэ төрлийн гэмт хэргийн арга гарсан талаар иргэдэд урьдчилан сануулдаг байх,

4. Уг төрлийн гэмт хэргийг илрүүлэх, мөрдөх, шүүхээр шийдвэрлэх ажиллагаанд техникийн болон цагдаа, прокурор, шүүгч нарын Кибер орчин, гэмт хэрэг, халдлага зэрэгт өөр өөр ойлголттой байна. Тоон нотлох баримт, шифрлэгдсэн, криптографын хамгаалалтаар хамгаалсан өгөгдлийг илрүүлэх, шифрлэлтийг тайлах чадвараа хөгжүүлэх, шүүхийн тоон шинжээчид болон цагдаагийн тоон криминалистикч, мэргэжилтнүүдийг энэ чиглэлээр гүнзгийрүүлэн сургах, энэ төрлийн ойлголтуудыг хуулийн бүх салбарт нэгэн ухагдахуунаар ойлгодог болгох чиглэлээр арга хэмжээ зайлшгүй авах шаардлагатай байна.

Эх сурвалжийн жагсаалт

Хууль тогтоомж.

1. Эрүүгийн хууль /шинэчилсэн найруулга/ Төрийн мэдээлэл. №7. Уб., 2016.

2. Эрүүгийн хэрэг хянан шийдвэрлэх тухай хууль /шинэчилсэн найруулга/ Төрийн мэдээлэл. №23. Уб., 2017.

3. ЦБҮАЖ КОД-226 Уб.,2012

Засгийн газрын тогтоол.

1. Монгол улсын засгийн газрын тогтоол. Үндэсний хөтөлбөр батлах тухай. №141. Уб., 2010.

2.Монгол Улсын Их Хурлын 2020 оны 52 дугаар тогтоол. “Алсын хараа 2050” урт хугацааны бодлогын баримт бичиг.

Цахим эх сурвалж

1. Цагдаагийн байгууллагын мэдээллийн нэгдсэн сан. http://system.police.gov

2. Цагдаагийн байгууллагын дүн шинжилгээний сан. http://research.police.gov/