ДОТООД ХЭРГИЙН ИХ СУРГУУЛЬ

КИБЕР ГЭМТ ХЭРГИЙН ШАЛТГААН НӨХЦӨЛ, УРЬДЧИЛАН СЭРГИЙЛЭХ АРГА ЗАМ

Судалгааны ажлын тайлан

Улаанбаатар хот

2023 он

УДИРТГАЛ

Судалгааны ажлын үндэслэл, шаардлага:

XXI зууны хүн төрөлхтний хамгийн том дэвшлийн нэг нь цахим хэрэглээ бөгөөд нийгмийн бүхий л харилцаа цахим хэлбэрт шилжиж байгаагийн хэрээр гэмт хэрэг үйлдэгдэх хэлбэр ч мөн адил цахим хэлбэрт шилжиж байна[1]. Цахим гэмт хэрэг нь олон улс, гүрэн хамран, өргөн цар хүрээтэй үйлдэгддэг бөгөөд энэ төрлийн гэмт хэргийг мөрдөн шалгах ажиллагаанд улс, орнуудын хамтын ажиллагаа нэн түрүүнд чухал ач холбогдолтой юм. Монгол Улсад төдийгүй дэлхий нийтийн хэмжээнд мэдээлэл, харилцаа холбооны технологийн хурдацтай хөгжил нь нийгэм - улс төр, эдийн засаг, боловсрол, ажил, амралт, чөлөөт цагийн зохион байгуулалт зэрэг хүний амьдралын харилцааны бүхий л салбарт багагүй өөрчлөлтийг авчирсаар байна.

Сүүлийн жилүүдэд манай улсын иргэд санаатай эсхүл болгоомжгүйгээр энэ төрлийн гэмт хэрэгт холбогдох, хохирогч болох асуудал цөөнгүй гарч байна.

Эрх зүйн шинэтгэл, олон улсын харилцаа, хамтын ажиллагааны төлөв байдал, техник-технологи болон эрх зүйн хөгжлийн өнөөгийн бодит байдал нь урьд өмнө байгаагүйгээр эрс өөрчлөгдөж, улмаар хүний эрх, эрх чөлөөний үнэлэмжээр тодорхойлогддог болсон билээ. Үүний гол хүчин зүйлийн нэг нь хүний эрхийн асуудлыг улс орон бүхэн гадаад, дотоод харилцааны чухал хэмжүүр болгон үнэлэмж тогтоох болсонтой холбоотой.

Энэ нь хүний туйлын эрх буюу бодит үнэнийг мэдэх, мэдээлэл харилцааны эрхтэй шууд холбоотой. Үнэнийг мэдэх эрхийг хангах, хамгаалах, мэдээлэл харилцаа холбооны хөгжлийн гол тулгуур нь компьютер, өндөр хүчин чадалтай техник, ухаалаг технологи бөгөөд даяаршсан мэдээллийн хөдөлгөгч хүч нь кибер орчин юм.

Кибер орчин нь өнөөгийн нийтийн харилцааны чухал хэрэгцээний нэг төдийгүй, нийгмийн хөгжлийг тодорхойлогч болсон компьютер, ухаалаг технологитой салшгүй холбоотой.

Мөн даяаршсан нийгмийн гол мөн чанар, дэлхийн хүн төрөлхтний хоорондын харилцаа, холбоо, мэдээллийн үйл ажиллагааны автоматжуулалтын хамгийн гол гүүр нь Кибер орчин учир иргэн, аж ахуйн нэгж, байгууллагын мэдээллийн аюулгүй байдлыг хангуулах талаар эрх зүйн орчныг боловсронгуй болгох, мэдээллийн аюулын эрсдэлээс урьдчилан сэргийлэх арга хэмжээг боловсронгуй болгох зайлшгүй шаардлага байгааг өнөөгийн хөгжил, дэвшлийн үйл явц илтгэж байна.

Иймд аливаа улс орон, байгууллага, тодорхой бүлэг хамт олон, хувь хүний мэдээлэл, түүний аюулгүй байдлыг баталгаатай хангах, хамгаалах явдал нь нэн ач холбогдолтой бөгөөд тулгамдсан бодит асуудлын нэг болсон мэдээллийн аюулгүй байдал ба кибер орчны өнөөгийн байдал энэ салбарт хэрэглэгдэж байгаа нэр томьёо, кибер орчинд үйлдэгдэж байгаа гэмт хэрэгтэй тэмцэх эрх зүйн тогтолцоо, олон улсын чиг хандлага, тулгамдаж байгаа асуудал, шийдвэрлэх арга замын талаар энэхүү судалгааны ажилд авч үзсэн болно.

[1] Өнөрмаа, Б. Цахим хэрэгсэл ашиглан үйлдэгдэж буй гэмт хэргийн шалтгаан нөхцөл, эрх зүйн орчинг боловсронгуй болгох шаардлага өгүүлэл. –Уб., https://www.mglbar.mn/news/4065

Судлагдсан байдал:

Кибер аюулгүй байдлын эсрэг гэмт хэргийн шалтгаан нөхцөлийг судлах, урьдчилан сэргийлэх арга боловсруулах чиглэлээр доктор, профессор Т.Халтар, Т.Баасанжав, Х.Ану “Цахим мэдээллийн аюулгүй байдлын эсрэг (кибер) гэмт хэргийн гүнзгийрүүлсэн судалгаа” нэрт захиалгат судалгааны ажил, Хууль сахиулахын их сургуулийн эрдэм шинжилгээ, хөгжлийн хүрээлэн “Монгол Улсад үйлдэгдэж байгаа кибер гэмт хэргийн шалтгаан, нөхцөл, түүнтэй тэмцэх арга зам, үндсэн чиглэл” сэдэвт суурь судалгааны ажил хийж гүйцэтгэжээ.

Судалгааны зорилго:

Судалгааны ажлын зорилго нь Монгол Улсын кибер аюулгүй байдлын эсрэг гэмт хэргийн өнөөгийн нөхцөл байдал, чиг хандлагыг тодорхойлж, түүний шалтгаан, нөхцөлийг судлан, энэ төрлийн гэмт хэрэгтэй тэмцэх эрх зүйн орчныг боловсронгуй болгох, урьдчилан сэргийлэх чиглэлээр санал, зөвлөмж боловсруулахад оршино.

Судалгааны зорилт:

Судалгааны ажлын зорилгыг хангах үүднээс дараах зорилтуудыг дэвшүүлсэн болно. Үүнд:

1. Гэмт явдал болон кибер гэмт хэргийн үндсэн шинж, ангиллыг тодорхойлох;

2. Кибер орчинд үйлдэгдсэн гэмт хэргийн статистик мэдээлэлд дүн шинжилгээ хийх;

3. Кибер орчинд үйлдэгдсэн гэмт хэрэгт мөрдөх ажиллагаа явуулах асуудлыг тодорхойлох;

4. Кибер орчинд үйлдэгддэг гэмт хэргийн шалтгаан нөхцөл, тулгамдаж буй асуудлыг тодорхойлох;

5. Энэ төрлийн гэмт хэрэгтэй тэмцэх, урьдчилан сэргийлэх санал, зөвлөмж боловсруулах зэрэг болно.

Судалгааны ажлын зохион байгуулалт:

Судалгааны ажлыг удирдамжийн хүрээнд календарчилсан төлөвлөгөө боловсруулан, Эрдэм шинжилгээний нэгдсэн хүрээлэнгийн захирлаар батлуулан хэрэгжүүлнэ. Судалгааны ажлын тайланг Эрдэм шинжилгээний нэгдсэн хүрээлэнгийн Гэмт явдал, цагдаа судлалын хүрээлэнд нэгтгэн боловсруулж, холбогдох төрийн байгууллагуудад хүргүүлэн, олон нийтийн хүртээл болгоно.

Судалгааны ажлыг гүйцэтгэх арга зүй:

Судалгааны ажилд эрх зүйн шинжлэх ухааны түгээмэл аргууд болох түүхчлэн судлах, баримт бичигт судалгаа хийх, статистик мэдээлэлд дүн шинжилгээ хийх, задлан шинжлэх, нэгтгэн дүгнэх зэрэг аргуудыг ашиглана.

Хамрах хүрээ:

Монгол Улсад бүртгэсэн кибер орчинд үйлдэгдсэн гэмт хэргийн сүүлийн 5 жилийн хугацааны статистик тоон мэдээллээр судалгааны хамрах хүрээ, хязгаарлалтыг тогтоосон болно.

Судалгааны үр дүнгийн ашиглалт:

Судалгааны ажлын тайланг Их сургуулийн удирдлагуудад танилцуулж, Цагдаагийн ерөнхий газар хүргүүлж, эрдэм шинжилгээ, практик хэрэглээний эргэлтэд оруулна.

НЭГДҮГЭЭР БҮЛЭГ. КИБЕР АЮУЛГҮЙ БАЙДЛЫН ЭСРЭГ ГЭМТ ХЭРГИЙН ҮНДСЭН ШИНЖ

§1.1. Гэмт явдал судлалын үндэс, кибер гэмт хэргийн сэтгэл зүй

Криминологийн шинжлэх ухааны үндсэн судлагдахуун нь гэмт явдлын шалтгаан нөхцөлийг судлан, тодорхой оношь, шинж тэмдгийг тогтоосны үндсэн дээр түүнтэй тэмцэх, үр өгөөж бий болгох нь хамгийн чухал зорилготой байдаг. Сүүлийн хэдэн зуун жил судлагдсан 200 гаруй онолууд энэ л зорилгыг агуулан гэмт явдлын шалтгааныг тайлбарлан, зөв механизмыг тогтоохын тулд тоологдошгүй олон модель, загварыг хэрэгжүүлсэн. Үүнээс дүгнэж үзвэл хуулийн хүрээнд тодорхойлсон "гэмт хэрэг" хэмээх харилцаатай зэрэгцэн нийгмийн хэм хэмжээ, нормыг зөрчсөн "зөрчил" гэх ойлголт ч хамаардаг ба криминологи нь дээрх харилцааны шалтгаан, хэрхэн тэмцэхтэй холбоотой өөр өөр талаас дүгнэн маш олон урьдчилан сэргийлэх, тэмцэх стратегийн үр нөлөөг бий болгодог. Манай оронд сүүлийн жилүүдэд гэмт хэргийн түвшин харьцангуй буурсан үзүүлэлттэй байх боловч зөрчлийн түвшин нэмэгдсээр байгаа юм. Иймээс дээрх хоёр ойлголтын хамаарлыг тодорхойлж, тэдгээрээс урьдчилан сэргийлэх зарим арга замыг дэвшүүлэх боломжтой.

Товч утгаараа гэмт явдлын шинжлэх ухаан хэмээн тодорхойлж болох криминологи нь гэмт хэрэгт нөлөөлөх биологийн, сэтгэл зүйн, нийгмийн, экологийн болон бусад хүчин зүйл, шалтгааныг судалж, гэмт явдлыг хэрхэн үйлдэгддэг талаар таамаг дэвшүүлж, урьдчилан сэргийлэх арга зүйг бий болгодог шинжлэх ухааны төрөл салбар юм. Э.Садерланд криминологи нь хууль зөрчих үйлдэл, түүнд авч буй арга хэмжээг судалдаг ухаан гэж үзжээ.[2] Эдгээр шинж чанартай зэрэгцэн криминологи нь гэмт явдлын шалтгааныг шинжлэх ухааны өнцгөөс судлах, гэмт хэрэг, зөрчлөөс урьдчилан сэргийлэхэд чиглэсэн стратегийн болон төрийн бодлогыг чиглүүлэх салбар юм.

Криминологийн судалгаа нь үндсэндээ гэмт явдлын шалтгаан нөхцөл, гэмт үйлдэлд оногдуулах хариуцлага гэсэн хоёр бүлэгт хуваагдаж байдаг[3]. Энэ хүрээнд криминологи нь шүүгч, прокурор, цагдаа зэрэг хэрэг бүртгэлт, мөрдөн байцаалтын ойлголт, өмгөөлөгч, хууль ёсны төлөөлөгч, яллах болон цагаатгах системийн бүхий л байгууллага, хэрэгжүүлэгчид, гэмт хэрэг, холбогдогч, хохирогч, иргэдийн нөлөө зэргийг судалдаг нийгмийн ухааныг хамааруулдаг өргөн судлагдахуун юм.

Гэмт хэрэг, зөрчил үйлдэгддэг шалтгаан нөхцөлийг судалдаг онолуудаас бүрддэг моделиудаар гэмт явдлын нөхцөл байдал болон ирээдүйд гэмт хэрэг үйлдэх эрсдэлтэй этгээдийн шинж, гэмт хэргийн түвшнийг таамаглах боломжтой болдог. Өөрөөр хэлбэл гэмт явдлын онолуудаар гэмт хэрэг, зөрчил үйлдэх магадлал өндөр хүмүүсийн онцлогийг тогтоох, гэмт хэрэг, зөрчлийн хүрэх түвшнийг урьдчилан тооцоолох боломжтой.

Гэмт хэргийг ихэнхдээ хуульд нээлттэйгээр хориглосон, ял шийтгэл оногдуулахаар заасан үйлдэл, эс үйлдэл хэмээн тодорхойлдог бол зөрчлийг нийгмийн норм, хэм хэмжээний хүрээнд хүлээн зөвшөөрөгдөхөөс гаднах бүх төрлийн үйлдэл, хандлага гэж

[2] Sutherland, Edwin H. Cressey, Donald R. 1978. Criminology. 10th edition. Philadelphia, New York, San Jose, Toronto; J. B. Lippincott Company. pp. 128

[3] Adler, Freda, Mueller, Gerhard O. W. Laufer, Williams S. 2004. Criminology. 5th edition. Boston. pp. 169

ойлгож болох юм[4]. Гэмт хэрэг үйлдсэн тохиолдолд ял шийтгэл хүлээлгэх нь гарцаагүй байдаг бол зөрчлийн шинжтэй үйлдэл, эс үйлдэл гаргасан тохиолдолд нийгмийн зүгээс жигших болон сөрөг хандлага үзүүлдэг байна.

Зураг 1. Гэмт хэрэг болон зөрчлийн харилцан хамаарал

Товчхондоо хэм хэмжээг зөрчсөн үйлдэл, хандлага гэж тодорхойлж болох зөрчлийг олон эрдэмтэн судлаачид өөр өөрөөр тайлбарладаг. И.Юүжел зөрчлийг “аль нэг нийгмийн тодорхой цаг хугацаан дахь хэм хэмжээний бус харилцаа” гэж тодорхойлсон бол Ф.Ичли “Нийгэм дэх соёлын үр дүнд бий болсон зан заншил, ёс, уламжлал, эрх зүйн дүрэм журамд нийцэхгүй үйлдэл” хэмээн тодорхойлжээ. Сокуллу Акынжи харин зөрчлийг “олон нийтийн хүлээлтээс өөр эсвэл нийгмийн зохимжтой төрлөөс өөр үйлдэл, хандлага” гэж үзжээ.

Гэмт хэргийг хуулийн үүднээс тодорхойлдог бол зөрчилд нийгмийн норм, хэм хэмжээний эсрэг үйлдэл, эс үйлдэл хамаардаг[5]. Дээрх хоёр ойлголт нь өөр өөр хэм хэмжээ, үнэт зүйлээс үйлчлэлцдэг ба эдгээр нь нэг нэгэнтэйгээ огтолцох зохицуулалттай байдаг. Үүнээс үзвэл гэмт хэргийг төрийн зүгээс хориглосон, зөрчлийг бол ард иргэдийн зүгээс хориглосон нийгмийн сөрөг харилцаа гэж тодорхойлж болох юм. Эндээс үзэхэд нийгмийн хэм хэмжээ болон үнэт зүйл нь нийгмийн өөрчлөлттэй шууд хамааралтай байна. Хуулиуд ихэвчлэн нийгмийн өөрчлөлтөөс хоцорч үлддэг ба тодорхой хугацаанд шинэчлэх шаардлагатай болдог.

Гэмт хэрэг зөрчлийн дунд огтолцох хэсгийн хэмжээ нь тухайн улс оронд төр болон ард иргэдийн үзэл санаа бие биетэйгээ хэрхэн зохицож байгааг харуулж буй хэмжээс болж өгдөг. Гэмт хэрэг зөрчлийг тодорхойлж байгаа ойлголтын давхардал бага байгаа бол төр болон ард иргэдийн дунд үл зохицол, зөрчилдөөн их байгааг илтгэдэг ба хоёр ойлголт бие биеэсээ салангид хол байна гэсэн үг юм. Ард иргэдийн зүгээс тааламжгүй гэж үздэг нийгмийн харилцаа хуульд тусгагдах чадвар нь төр ард иргэдийн үзэл нийлэх түвшнийг, тухайн улс орны хууль эрх зүйн зохицуулалт өндөр түвшинд чанартай байгааг илтгэдэг. Энэ хоёр хэм хэмжээний системүүдийн хооронд гарах хийдэл, давхардал нь нийгэмд үл ойлголцол бий болгож болзошгүй. Үүнээс үзэхэд хууль хэрхэн тогтоох, ямар үйлдэл эс үйлдлүүд гэмт хэрэгт тооцогдохыг шийдвэрлэх механизмыг тодорхойлох хоёр үзэл баримтлалыг тайлбарлах боломжтой: 1.Зөвшилцөл /consensus/ ба 2. Зөрчилдөөн /conflict/

Зөвшилцлийн үзэл баримтлалаар хууль бол нийтийн хэв журам, хүмүүсийн нийтлэг эрх ашигт үйлчлэх тохиролцооны шинжтэй байна. Энэхүү үзэл санаа нь нийгэм нэг бүхэллэг бүтэцтэй байх ба дүрэм журмуудын талаар зөрчилдөхгүй, нэг үзэл санаатай,

[4] Нарантуяа, Ш., Ганбадрал, Н., Буянхишиг, Г. Захиргааны зөрчил.-Уб., 1999 он. 22 дахь тал
[5] Долгорсүрэн, Ж.Захиргааны хариуцлага. -Уб., 1998 он. 17 дахь тал

түүнийгээ бүгд дагаж мөрддөг байх явдал юм. Ёс суртахууны үүднээс зохимжгүй байдал, хуулийн зүгээс зохимжгүй байдал хоёрын хооронд ялгаа үүсэх магадлалтай[6]. Энэ ялгаа нь хэдий чинээ бага байна хуулиуд төдий чинээ зөвшилцлийн шинжтэй байна гэж ойлгож болох юм.

Зөрчилдөөний үзэл баримтлалд бол зөвшилцөл гэх ойлголт үгүй. Учир нь хууль болон төрийн эрх мэдэл нийгмийн бүх гишүүдэд адил, эрх тэгш үйлчилдэггүй. Хуулийг шинээр боловсруулах явцыг үзвэл улс төрийн тооцоо, дарангуйлагч бүлэглэлийн эрх ашиг ихээхэн нөлөө үзүүлдэг. Хуулиуд хүн бүрийн нийтлэг эрх ашгийг хамгаалдаггүй бөгөөд нийгэмд үе үе ундууцал төрүүлдэг.

Эндээс үзэхэд зөвшилцлийн үзэл баримтлалд гэмт хэрэг, зөрчил үйлдэгддэг шалтгаан нь нийтээрээ хүлээн зөвшөөрсөн дүрэм журмыг дагаж мөрдөөгүй, хэрэгжүүлээгүй этгээдүүдийн үйлдэл, эс үйлдэл гэж үзэж болох атал зөрчилдөөний үзлээр гэмт хэрэг гэж тооцсон эсвэл тооцоогүй үйлдэл эс үйлдэхүй нь нийгмийн тодорхой бүлэг тухайн нийгмийн амьдралын хэв маягт үзүүлэх сөрөг үйлдэл гэж үздэг байна[7].

Гэмт хэрэг болон зөрчлийн харилцан хамаарлыг энэ хүрээнд дүгнэн тайлбарлах боломжтой юм. Зарим судлаачид “Бүх гэмт хэрэг бол зөрчил, харин бүх зөрчил гэмт хэрэг биш” гэх байдлаар гэмт хэргийг зөрчлийн нэгэн категори гэж үздэг[8]. Харин зөрчилдөөний үзлээр хуулиуд үргэлж заяагдмал эрх зүй, нийгмийн хэм хэмжээ, ард иргэдийн сонголтыг түшиглэдэггүй гэж үздэг. Үүнээс үзвэл бүх гэмт хэрэг нь зөрчил биш ч байж болох юм.

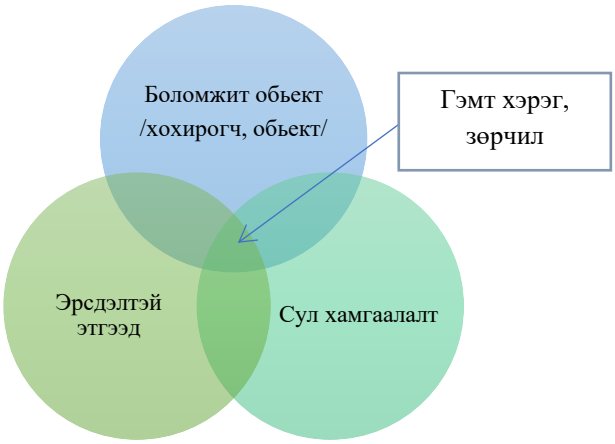
Байнгын үйл ажиллагааны онол /Routine activity theory/ буюу Кохен ба Фелсон нарын дэвшүүлсэн энэ ойлголт нь бусад онолоос ялгаатай нь гэмт этгээдтэй холбоотой онцлог шинжийг судлахын оронд цаг хугацаа, орон зайнаас шалтгаалах нөхцөл байдлын хүчин зүйлд анхаарлаа хандуулах нь зүйтэй гэж үзсэн.

Өмнө хийгдэж байсан орон зайнаас хамааралтай гэмт явдлын анализууд нь түүнийг ойлгоход үнэтэй хувь нэмрээ оруулсан болов ч хүнийг болон хүний экологи гэж хэлж болохуйц хүний орчин тойрны зүйлс, хүний амьдралын динамик бүтцийг тооцоолоогүй. Кохен ба Фелсон нар эдгээр дутуу зүйлсэд анализ хийж, гэмт явдлын механизмыг 1. Эрсдэл бүхий этгээд, 2. Боломжит объект, 3. Сул хамгаалалт гэсэн гурван хэсгээс бүрдэнэ гэсэн санааг дэвшүүлжээ.[9]

Үүнээс дүгнэхэд байнгын үйл ажиллагааны онолоор гэмт хэрэг, зөрчил үйлдэгдэхэд тухайн үйлдлийг үйлдэхэд цааргалахгүй этгээд, гэмт этгээдийн анхаарлыг татахуйц объект, түүнийг хамгаалах хэн нэгэн байхгүй байх гэсэн тохиолдлуудын давхцал бий болох шаардлага гарч байна. Энэ гурван шинж бол нэгэн бүхэллэг ойлголт болох бөгөөд гэмт хэрэг, зөрчил үйлдэгдэхэд бүгд байх шаардлагатай. Хэрэв аль нэг нь үгүй бол гэмт хэрэг, зөрчил үйлдэгдэхгүй гэсэн үг юм.

Зураг 2. Байнгын үйл ажиллагааны онол

[6] Jenkins, Philip. 1984. Crime and Justice. Issues and Ideas. Belmont, CA; Brooks/Cole Publishing Company, a division of Wadsworth, Inc. pp. 31-35
[7] Cloward, Richard A. Lloyd E. Ohlin. 1966. Delinquency and Opportunity; A theory of delinquent gangs. New York. Free Press. pp. 588-601
[8] Beccaria, Cesare. 1963. On Crimes and Punishment, trans. H. Paolucci. Indianapolis, IN; Bobbs-Merill
[9] Cohen, Lawrence E. and Felson, Marcus. 1979. ‘Social Change and Crime Rate Trends; A Routine Activity Approach.’ American Sociological Review. Vol. 44, No.4



Метрополис хотуудын гэмт хэрэг, зөрчлүүдийн түвшнийг авч үзвэл 10 сая хүн амтай Истанбулд жилд 91.693, 3 сая хүнтэй Берлинд 573.000, 1.6 сая хүн амтай Вианад жилд 154.000, 2,8 сая хүн амтай Мадридад 230.000 гэмт хэрэг үйлдэгддэг байна. Эдгээрийг хүн амын тоонд нь харьцуулан авч үзвэл Мадрид 8%, Виана 10%, Берлин 17% байгаа бол Истанбулд 1% гэсэн түвшин гарч байна. Эдгээр нь Европын хамгийн тайван, аюулгүй хотуудын жишээ юм[10].

Гэхдээ энэ тоон үзүүлэлт үнэн бодитой эсэх нь эргэлзээтэй юм. Учир нь криминологичид “далд нөхцөл байдал”, “хар тоо” зэрэг ойлголтыг байдаг гэдгийг нотолсоор ирсэн. Гэмт хэрэг, зөрчлийн албан ёсны бүртгэлээс авсан тоо мэдээлэл нь гэмт хэрэг зөрчлийн жинхэнэ тооноос хол зөрөх магадлалтай юм.

Гэмт хэрэг зөрчлөөс урьдчилан сэргийлэх стратегийн түвшинд “Хагархай цонхны онол”, “байнгын үйл ажиллагааны онол” зэргийн үзэл баримтлалыг үндсэн суурь болгон авч үзэж болох юм.

Гэмт хэргээс урьдчилан сэргийлэх ажил ихэвчлэн нийгмийн анхаарлыг татсан, хүнд гэмт хэргүүд рүү төвлөрдөг. Дараа нь гэмт хэрэгтнээс урьдчилан сэргийлэх буюу гэмт хэрэг, зөрчил үйлдэж болзошгүй эрсдэлтэй этгээдүүдийг хянах, сургалтын үйл ажиллагаа явуулах зэрэг байдаг. Тухайлбал манай улсын хэмжээнд 2019 оны эхний 11 сарын байдлаар гэмт хэрэг 30.011 байгаа бол өмнөх оны мөн үед нийт 33.880 гэмт хэрэг бүртгэгдсэн нь 12 хувиар буурсан сайн үзүүлэлттэй байна. Үүнээс хөнгөн хэрэг 9 хувиар, хүнд гэмт хэрэг 21 хувиар буурсан байна. Харин улсын хэмжээнд 2019 оны эхний 11 сарын байдлаар нийт 1.963.882 зөрчил бүртгэгдэж шалгагдсан бол өмнөх оны мөн үед 1.530.349 зөрчил бүртгэгдэж байсан нь 22 хувиар өссөн үзүүлэлттэй байна.[11] Бүртгэгдсэн гэмт хэргийн түвшин хэдийгээр буурсан үзүүлэлттэй байгаа ч зөрчлийн түвшин багагүй хэмжээгээр өссөн байна. Ийм тохиолдолд зөвхөн гэмт хэрэг бус зөрчлөөс урьдчилан сэргийлэх ажлыг ч зохион байгуулж, үр дүнг гэмт хэргийн түвшинтэй харьцуулах шаардлагатай юм. АНУ-ын Чикаго, Бостон зэрэг муж, тэдний тодорхой дүүргүүдэд дээрх онолуудад тулгуурлан 2000 оноос өмнө болон дараа хэд хэдэн үечлэлээр үр дүнг тооцсон туршлага байдаг байна.

[10] International Centre for the Prevention of Crime, U.S. Department of Justice Office of Justice Programs. 2016
[11] ЦЕГ-ын Мэдээлэл, судалгааны төв. “Улсын хэмжээнд 2019 онд бүртгэгдсэн гэмт хэрэг, зөрчлийн статистик мэдээ”. 2019 оны 12-р сарын 03

Гэмт хэрэг, зөрчлөөс урьдчилан сэргийлэх зорилго нь тодорхой гэмт хэрэг зөрчил үйлдэгдэх боломж, нөхцөлийг үгүй болгох, хамгийн бага түвшинд аваачих явдал юм. Мөн орчин тойрны урьдчилан сэргийлэх арга хэмжээ нь гэмт этгээд баригдах магадлалыг ихэсгэснээр тохиолдлоор гэмт хэрэг үйлдэх явдлыг багасгах ач холбогдолтой. Энэ нь "хагархай цонх"-ны үзэл буюу орчин тойрны эмх замбараагүй байдал, нийтийн хэв журмыг сахиулснаар гэмт хэрэг үйлдэгдэх магадлалыг багасгах боломжтой гэсэн үг юм. Гэмт хэргийн бодит үйлдэгдэж байгаа түвшнийг багасгахын тулд зөрчлөөс урьдчилан сэргийлэх ажлыг идэвхтэй зохион байгуулах нь үр дүнтэй байх боломжтой юм.

Сүүлийн жилүүдэд компьютерын технологи ашиглан үйлдсэн гэмт хэргийн тоо улам бүр өссөөр байна. Олон улсын вирусийн эсрэг ESET компанийн мэргэжилтнүүдийн мэдээллийн аюулгүй байдлын чиглэлээр хийсэн 2013 оны судалгааны тайланд тэргүүлэх хэвлэл мэдээллийн хэрэгсэл, мэдээллийн технологийн корпорацууд хэд хэдэн кибер халдлагад өртсөнийг онцолжээ.

The New York Times, Wall Street Journal, Washington Post, түүнчлэн Twitter, Facebook, Evernote, Apple, Microsoft зэрэг сайтууд халдлагад өртөж, компанийн ажилчид болон үйлчилгээний хэрэглэгчдийн хувийн мэдээлэл, мөн Adobe Acrobat, ColdFusion болон Photoshop зэрэг бүтээгдэхүүний эх код их хэмжээгээр алдагдсан байна. Үүнтэй зэрэгцэн Facebook-ийн Zynga Poker программын тоглогчдыг халдварласан PokerAgent гэх хортой кодыг илрүүлжээ.

Хакеруудын зорилго нь хэрэглэгчдийн хувийн мэдээлэл, мөн тэдний данстай холбогдсон банкны картын талаарх мэдээллийг авах явдал байв. Үүний үр дүнд тэд 16,000 гаруй фейсбүүк хаягийн мэдээллийг хулгайлсан байна. Интернэт мессенжерээр дамжуулан харилцах системийн хэрэглэгчид ч хакеруудын цохилтод өртжээ. ESET-ийн мэргэжилтнүүдийн тодорхойлсон Skype, Gtalk, QIP болон бусад хэд хэдэн мессенжер дэх спам кампанит ажил нь дэлхий даяар хагас сая гаруй хэрэглэгчийг аюулд оруулжээ.

Нортон компанийн үзэж байгаагаар кибер гэмт хэргийн жилийн нийт хохирол 110 тэрбум доллароор хэмжигддэг байна. Энэ болон бусад хэд хэдэн шалтгааны улмаас дэлхий даяар цахим гэмт хэрэгтэй тэмцэхэд ихээхэн анхаарал хандуулах болсныг илтгэж байна.

Дэлхий дээр кибер орон зайн даяаршил үүссэн нь компьютерын харилцаа холбоог ашиглан гэмт хэрэг үйлдэх боломжтой болж, улмаар олон нийтийн томоохон аюулыг бий болгож байна. Үүнтэй зэрэгцэн интернэт технологид суурилсан гэмт хэргийн нийгэм-сэтгэл зүйн зүй тогтол хангалттай судлагдаагүй байна.

Мэдээллийн технологийн хөгжлийн сөрөг үр дагаврын нэг бол гэмт хэргийн шинэ хэлбэр болох өндөр технологийн гэмт хэрэг үүсэх, хөгжих явдал бөгөөд компьютер эсвэл компьютерын сүлжээ нь гэмт хэргийн халдлагын объектын үүрэг гүйцэтгэдэг байна.

Энэ хүрээнд кибер гэмт хэрэгтнүүдийн гэмт үйлдлийн сэтгэл зүйн талыг авч үзэх нь зүйтэй гэж үзэж байна.

Эхний төрлийн гэмт хэрэг нь хүний бие махбодын аюулгүй байдал, амь нас, эрүүл мэндэд халдсан хүчирхийллийн болон бусад аюултай цахим гэмт хэрэг. Бие махбод, эрүүл мэндэд заналхийлэх зорилго нь хохирогчид өөрийн болон түүний ойр дотнын хүмүүсийн амь насны талаар айдаст автуулах явдал юм. Энэ тохиолдолд заналхийлэл агуулсан

мессежийг цахим шуудангаар илгээх байдлаар хохирогчийн сэтгэцэд дарамт үзүүлэх үйлдэл орно.

Олон нийтийн ёс суртахуунд халдсан гэмт хэргийг мөн Кибер аюулгүй байдлын эсрэг гэмт хэргийн тусдаа бүлэг болгон ялгаж үздэг. Үүний нэг нь хүүхдийг садар самуунд сурталчлах гэмт хэрэг (насанд хүрээгүй хүүхдүүдийг оролцуулсан садар самуун сурталчилсан материал бүтээх, тараах, тэдгээрт нэвтрэх) юм.

Кибер терроризм нь орчин үеийн технологид суурилан хэрэгждэг тул судлаачид хамгийн аюултай асуудлын нэг гэж үздэг. Дэлхийн цахим сүлжээг орчин үеийн олон улсын терроризм хэд хэдэн хэлбэрээр ашигладаг: терроризмыг сурталчлах; мэдээлэл, сэтгэл зүйн нөлөөлөл; терроризмыг санхүүжүүлэхэд зориулж хөрөнгө босгох; оролцогчдыг элсүүлэх; мэдээлэл цуглуулах; террорист байгууллагын шинэ бүтцийг бий болгох; террорист шинж чанартай практик материалыг байрлуулах; террористуудтай харилцах дэлхийн сүлжээг ашиглах зэрэг юм. Өнөөгийн шатанд бараг бүх идэвхтэй террорист байгууллагууд өөрсдийн вэбсайттай бөгөөд олонх нь нэгээс олон сайт ажиллуулж, хэд хэдэн хэл ашигладаг байна.

Түүнчлэн Кибер орчин нь хамгийн тохиромжтой хэрэгсэл болох хэд хэдэн уламжлалт гэмт хэрэг байдаг. Тэдний олонх нь (биеэ үнэлэх үйлчилгээг сурталчлах, хар тамхины наймаа, мөрийтэй тоглоом тоглох, мөнгө угаах, хууль бусаар хил нэвтрүүлэх, хууль бус бараа шилжүүлэх гэх мэт) Кибер орчин ашигладаг хэдий ч цахим технологи ашиглахгүйгээр ч санаа зорилгодоо хүрч болох гэмт хэргүүд юм.

Кибер гэмт хэргийн нийгэм-сэтгэл зүйг судлах нь түүний илрүүлэлтийн байдалд дүн шинжилгээ хийхээс эхэлдэг байна. Манай орны энэ төрлийн гэмт хэргийн илрүүлэлтийн байдал нь кибер гэмт хэрэгтнүүдийг судлахад хангалтгүй байна.

Кибер гэмт хэрэгтний хувийн шинж чанар нь зөвхөн криминологийн төдийгүй нийгэм-сэтгэлзүйн судалгааны объектын хувьд сонирхолтой байдаг. Гэсэн хэдий ч ийм судалгааны хамрах хүрээ нь гэмт хэргээс урьдчилан сэргийлэхийн тулд дүн шинжилгээ хийхэд шаардлагатай гэмт этгээдийн хувийн шинж чанаруудаар хязгаарлагддаг.

Мөрдөн байцаалтын явцад гэмт хэргийн талаарх анхан шатны мэдээлэлд илэрдэг хувийн шинж чанарыг илэрхийлэх бүх хэлбэрийг тодорхойлох нь гэмт хэрэгтний ерөнхий, дараа нь онцлог шинж чанаруудын талаар ойлголттой болох боломжийг олгодог.

Гэмт хэрэг бүхэн ул мөр үлдээдэг. Хэргийн газраас олдсон эд мөрийн баримтаар гэмт хэрэгтний хувийн, нийгэм-сэтгэл зүйн шинж чанар, зан чанар, гэмт хэргийн туршлага, мэргэжил, нийгмийн мэдлэг, нас, хохирогчтой харилцах харилцаа гэх мэт мэдээлэл илэрч болно.

Колбергийн ёс суртахууны хөгжлийн загвар

Сэтгэл судлалын хөгжлийн үр дүнд нэг хэсэг мартагдаад байсан Пиажегийн үзэл санаа Лауренс Колберг нэртэй сэтгэл судлаачийн докторын судалгааны ажлаар шинэчлэгдэн боловсруулагдсан загвараар дахин нэг удаа сэргэн гарч ирсэн. Судалгааны

үр дүнд Колберг Пиажегийн 16 насанд дуусдаг гэх ёс суртахууны хөгжлийг илүү удаан хугацаанд үргэлжилдэг ба илүү ярвигтай бүтэцтэй гэсэн санааг дэвшүүлжээ.[12]


Lawrence Kohlberg
(1927-1987)

Нийт 72 хүүхдэд хийсэн судалгаанд 10-13 насны холимог бүлэгтэй 16 насны өөр нэг бүлгийг харьцуулан судалжээ. Дараа нь Америкийн бусад муж бусад улс орноос гэмт хэрэгт холбогдож байсан хүүхдүүд болон бага насны хүүхдүүдийг хамруулж, ёс суртахуунтай холбоотой олон төрлийн өгүүлэл, бодит явдлыг уншиж өгч тухайн өгүүлэлд дурдагдаж байгаа хүнд бэрхшээлтэй нөхцөл байдалд үзүүлж буй хариу үйлдлүүдийг нь судалж байлаа. Туршилтын асуултуудад тийм эсвэл үгүй гэж хариулах нь чухал биш харин бодит байдалд тулгуурлан хэрхэн хариулж байгааг Колберг чухалчилж үздэг байсан. Эдгээр өгүүллээс хамгийн түгээмэл нь иймэрхүү байсан:

"*Нэгэн эмэгтэй маш ховор төрлийн хорт хавдар туссан ба амь нас нь хүнд нөхцөл байдалд байлаа. Эмч нар өвчтөнг аврах цорын ганц эм байгаа гэжээ. Энэ эмийг тухайн өвчтөнтэй нэг тосгонд амьдардаг эмийн санч бүтээсэн байжээ. Эмийг хийхэд өртөг ихтэй байсан ч эмийн санч 10 дахин их мөнгө нэхдэг байж. Эмийн санч түүхий эдээ 200 доллароор авдаг ч эмийнхээ жаахан тунг 2000 доллароор үнэлжээ. Өвчтөн эмэгтэйн нөхөр болох Хайнз өөрийн таньж мэдэх бүх хүмүүсээс мөнгө зээлсэн ч нийт 1000 доллар л цуглуулсан нь авах эмийн өртгийн тал нь л байлаа. Хайнз эмийн санчид эхнэрийнх нь бие маш муу байгааг тайлбарлан эмийг өөрт нь арай хямдхан зарахыг эсвэл үлдсэн мөнгийг нь дараа төлөх боломж олгохыг хүсжээ. Гэвч эмийн санч:*

- Үгүй, эмийг би өөрөө зохион бүтээсэн ба үүгээрээ их мөнгө олохыг хүсэж байна гэжээ. Үүний дараа Хайнзын итгэл алдарч эмийн сан руу нууцаар орж эмийг хулгайлжээ. Энэ хүний энэ үйлдэл та нарын бодлоор зөв үү?

Колберг туршилтаараа энэ төрлийн өгүүллүүдэд өгч буй хариултуудаар хүмүүсийг 3 түвшний нийт 6 үе шаттай ёс суртахууны хөгжлийг туулдаг гэжээ. Эдгээр үе шатуудтай холбоотойгоор

1. Хүний дотоод мөн чанар ёс суртахууны хөгжил байнга үргэлжилдэг
2. Ховор тохиолдол биш л бол хөгжлийн үе шат дарааллаараа явагддаг ба аль нэг үе шатыг алгасдаггүй
3. Дээд түвшний үе шат бусад доод үе шатуудаа бүгдийг нь хамааруулдаг гэдгийг тодорхойлжээ.

Ёс суртахууны хөгжил, гэмт явдлын хамаарлыг судалсан эмпирик судалгаанууд

Ёс суртахууны хөгжил ба гэмт явдлын хамаарлыг судалсан судалгаануудын нийтлэг дүгнэлт нь гэмт этгээдүүдийн ёс суртахууны хөгжлийн дутмаг байдал юм. Эндээс үзэхэд гэмт этгээдүүд Колбергийн загварын эхний 3 түвшнээс хэтэрдэггүй гэж хэлж болохоор байна. Учир нь тэдний хувьд ёс зүйн үнэ цэн, зарчим, нийгмийн сайн

[12] Saltzstein, Herbert D. 2008. "Moral Development." In Salkind, Neil J., Encyclopedia of Educational Phsycology, Vol.2. A SAGE Reference Publication. Thousand Oaks, London, New Delhi: Sage Publications, pp.681-686

сайхан, хууль дээдлэх, бусад хүмүүсийн эрх ашиг огт чухал биш юм. Гэмт этгээдүүдийн хувьд ёс суртахууны түвшин доогуур байх нь бусдыг үл ойшоох, өөрийн буруутай үйлдлийн үр дүнг үл ойшоох, зөвхөн өөрийн хүсэл сонирхлыг бодох зэргээр илэрдэг. Ялангуяа цахимаар гэмт хэрэг үйлддэг этгээдүүдэд хийсэн судалгаагаар ёс суртахууны хөгжил гэмт хэргийн хамаарал тод товруун илэрдэг.

Хакерууд бусдад учруулж байгаа хохиролдоо огтхон ч харамсдаггүй бөгөөд хөгжилдөхийн тулд сая сая долларын системийг гэмтээдэг ба огт танихгүй хүмүүст учруулж байгаа хор уршигтаа огтхон ч харамсах сэтгэл төрдөггүй.

Палмер ёс суртахууны хөгжил болон хүчирхийллийн хамаарлыг судалсан судалгаандаа ёс суртахууны хөгжил нь хүүхдийн бага наснаас эхлэн сууж эхэлдэг ба үүнд эцэг, эх болон гэр бүлийн бусад гишүүд чухал нөлөө үзүүлдэг гэжээ. Палмер гэр бүлийн зүгээс хараа хяналтгүй, тусламж дэмжлэггүй, хөндий хүйтэн, хатуу ханддаг хүүхдүүд анхаарал, хайр, халамжид өссөн хүүхдүүдээс ёс суртахууны хувьд тааруу, гадаад ертөнцийг үзэн ядах үзэлтэй болдог гэж дүгнэжээ. Бага наснаас нь эхлэн бий болдог энэ төрлийн хандлага цаашлаад дадал зуршил болтлоо сууж өгдөг байна. Эцэст нь хувь хүн аливаа зүйлийг үнэлэхэд шаардлагатай ёс суртахууны суурь ойлголт авахгүй байвал уур уцаараас уур уцаар, хатуугийн эсрэг улам хатуу харилцаа үүсэж юмсыг өөр өнцгөөс харах чадвар нас биед хүрэхэд улам багасах болно.

Эдгээр жишээ болон судалгаануудаас дүгнэхэд гэмт хэрэгтнүүд бусад хүмүүстэй харьцуулахад ёс суртахууны түвшин багатай болох нь харагдаж байна.[13] Мөн Стамсын 2006 онд хийсэн судалгаанд нийгэм, эдийн засаг, демографик өөрчлөлтүүдтэй оюун ухааны түвшин зэргийг харьцуулсан ч ёс суртахууны доройтол нь хүүхэд залуучуудын гэмт хэрэг үйлдэх түвшинтэй шууд хамааралтай байсаар байжээ. Үүнээс үзвэл ёс суртахуунтай холбоотой гэмт явдлаас урьдчилан сэргийлэх стратеги нь ёс суртахууны хөгжлийг доройтуулж, удаашруулж байгаа хүчин зүйл рүү анхаарал хандуулах шаардлагатай байна. Хэрэв хувь хүний ёс суртахууны хөгжлийг дэмжих үр нөлөөтэй программ хөгжүүлж ёс суртахууны хөгжилд саад учруулж байгаа хүчин зүйлсийг үгүй болгох эсвэл нөлөөг нь хамгийн бага түвшинд аваачиж чадвал тэр үед гэмт хэрэг, зөрчлийн түвшинд мэдэгдэхүйц бууралт гарах боломжтой юм.

Сэтгэл судлалын онолууд нь гэмт хэрэгтэн болон энгийн хүмүүсийн дунд тодорхой ялгаа байгааг тогтоосон байдаг. Энэ ялгаа нь заримдаа гэмт хэрэгтнүүд оюуны хөгжил дутмаг, бусдыг огт боддоггүй, хоромхон зуурын жаргалаас илүүг үнэлж чаддаггүй, дотоод үзэл суртал, зөрчилдөөнөөс шалтгаалан нэг алхмын цаадхыг тооцоолж чадахгүй байх, ёс суртахууны хөгжил муу байх зэргээр илэрдэг.

Позитивист талаасаа биологийн онолуудтай олон ойлголт давхацдаг сэтгэл судлалын онолууд гэмт хэргийг хувь хүнээс илрэх эмгэг гэж үзэх ба бие хүний нийгэмших үйл явц бусад хүнийхтэй ижил түвшинд хүрэхгүй байх, хандлага төлөвшил суухгүй байх, өөрийгөө хянаж захирч чадахгүй байх зэргийн үр дүн гэж үзэж болно.

Үүнээс үзвэл, Эйкхорны үзсэнээр асуудлыг тодорхойлж цаг алдахын оронд асуудлынхаа шалтгааныг олж тогтоох шаардлагатай юм. Харин судалгаанд дурдагддаг

[13] Tarry, Hammond and Emler, Nicholas. 2007. “Attitudes, Values and Moral Reasoning as Predictors of Delinquency.” British Journal of Developmental Psycholog, Issue 25, pp.169-183

гэмт хэргийн шалтгаануудын ялгаа нь Эйкхорны үзсэнээр өдөөн хатгалга ба байнга илрэхэд бэлэн байдаг дотоод чиг хандлагуудаас үүдэлтэй юм.

Эндээс үзэхэд гэмт хэрэг, зөрчлийн үндсэн шалтгааныг тодорхойлоход сэтгэл судлалын шинжлэх ухаан томоохон хувь нэмэр оруулна. Хэдий тийм болов ч зөвхөн сэтгэл судлал талаасаа биш илүү нийлмэл, хувь хүний хүмүүжилтэй холбоотой өнцгөөс нь харвал илүү үр дүнд хүрч болох юм.

§1.2. Кибер гэмт хэрэг, түүнийг ангилж буй хэлбэр

Мэдээлэл, харилцаа холбооны технологийн системийг хүн төрөлхтний оршин тогтнох бүхий л салбарт ашиглах хандлага бий болж байгаа бөгөөд үүнийг дэлхий нийтээр хүлээн зөвшөөрсөн[14]. Нөгөөтээгүүр, мэдээллийн системүүд нь хүний үйл ажиллагааг илүү олон төрлийн болгох боломжийг олгодог. Жишээлбэл, өдөр тутмын үйл ажиллагааны хурдыг нэмэгдүүлж, хүмүүст илүү ашигтай харилцааг хөгжүүлэх, хадгалах боломжийг олгодог, байгууллагын бүтцэд нөлөөлж, худалдан авсан бүтээгдэхүүний төрлийг өөрчлөх, бизнесийн мөн чанарт нөлөөлдөг.

Энэ утгаараа мэдээлэл, мэдлэг нь эдийн засгийн амин чухал нөөц болдог. Энэ нөхцөл байдлын үр дүнд шинэ боломжуудын зэрэгцээ мэдээллийн системээс байнга ашиг хүртэх хэрэгцээ шинэ аюул заналхийллийг авчирдаг. Мэдээллийн салбарын эрчимтэй шинэчлэл, эрдэм шинжилгээний судалгаа нь аюул заналхийллийг хязгаарлахын тулд шинэ боломжуудыг байнга хөгжүүлж байдаг. Энэ хүрээнд байнга тулгардаг асуудлын нэг бол кибер халдлага буюу цахим гэмт хэрэг юм.

Гэмт хэрэгтэй тэмцэх үйл ажиллагаа үргэлж хувьсан өөрчлөгдөж байхыг шаардсан динамик шинжтэй тул шинээр үйлдэгдэх болсон гэмт хэргийг судалж, танин мэдэхгүйгээр түүнийг таслан зогсоох, илрүүлэх талаар ярих боломжгүй билээ.

Гэмт хэрэг, гэм буруугийн тухай ойлголтууд түүхийн туршид хувь хүнтэй холбоотой байсаар ирсэн. Улс орнууд өөрсдийн соёл, цар хүрээг харгалзан гэмт хэрэгтэй тэмцэх ялгаатай стратеги баримталж ирсэн. Гэмт хэргийн гаралт өндөртэй улс орнууд хөгжлийнхөө төлөө тэмцэж байна. Энэ нь нийгэм, эдийн засгийн сөрөг үр дагавартай. Хэрэв бид гэмт хэргийн тухай ойлголтыг Фройдын хүрээнд авч үзвэл хүний түрэмгий буюу хор хөнөөлтэй үйлдэл нь "байгалийн" (id) болон "соёлын" (би болон суперэго) шалтгаантай байдаг.

1990-ээд оны дунд үеэс интернэт дэлхий даяар, ялангуяа аж үйлдвэржсэн барууны ертөнцөд амьдарч буй хүмүүсийн амьдралын салшгүй хэсэг болсон.

Вебстерийн онцолж буйгаар интернэт нь манай "хумигдаж буй" ертөнцөд амьдралтай холбоотой шинэ боломж, сорилтуудыг бий болгодог даяаршлын үйл явцын нэг хэсэг[15] гэж үздэг. Энэ байдал нь хяналт тавихад хэцүү бөгөөд цахим ертөнцөд аюул дагуулж байна. Интернэтийг гэмт хэргийн хүрээнд авч үзэхэд хэвлэл мэдээллийн хэрэгсэл чухал үүрэг гүйцэтгэдэг[16]. Кибер гэмт хэргийн тухай ярихад орон нутгийн гэмт хэргийн нөхцөл байдлын зэрэгцээ бусад улс орныг хамарсан хил дамнасан гэмт хэрэг ч гарч ирдэг. Тухайлбал, хүн худалдаалах, хууль бусаар хил нэвтрүүлэх, терроризм гэх мэт бүх нийтийн тулгамдсан асуудлын хүрээнд шалгаж байгаа гэмт хэргүүдийг дурдаж болно.

Кибер гэмт хэргийн тухай ойлголтын талаар тодорхой тодорхойлолт байдаггүй ч олон судлаачид ерөнхийдөө ойролцоо тодорхойлолтуудыг гаргаж ирсэн.

[14] Lupton, D. (2014). Digital Sociology. London: Routledge.
[15] Webster, F. (2003). Theories of the Information Society. London: Routledge
[16] Yar, M. (2006). Cybercrime and Society. Sage Publications.

Жишээлбэл, Томас ба Лоадер кибер гэмт хэргийг "тодорхой талууд хууль бус гэж үзсэн, дэлхийн цахим сүлжээгээр дамжуулан явуулж болох компьютерын зуучлалын үйл ажиллагаа"[17] гэж үздэг.

Гэмт этгээдийг олоход хүндрэлтэй байдаг нь кибер гэмт хэрэгт тулгардаг бэрхшээлүүдийн хамгийн түгээмэл асуудал юм. Интернэтийн орчин нь нийгмийн баримжаагаа өөрчилснөөр кибер харилцан үйлчлэлийг нэмэгдүүлж, хувь хүмүүст өөрийгөө дахин нээж, "бодит ертөнц"-өөс хол байгаа шинэ Кибер хүн болгон хувиргах боломжийг олгодог[18].

Нийгмийн аливаа харилцаа шууд бус, цахим платформоор дамжих болсон нь гэмт хэрэг, зөрчилд ч нөлөөгөө үзүүлж, үйлдлийн хэрэгсэлд ашиглагдах болсон нь томоохон асуудлыг үүсгэж байна. Энэ байдал нь криминологийн хувьд ялангуяа гэмт хэрэгтнийг олж тогтооход хүндрэл учруулдаг.

Иймд цаг үеийн хэрэгцээ шаардлагад үндэслэн Кибер орчинд үйлдэгдэж буй гэмт хэргийн талаар судалгаа явуулж, түүнтэй тэмцэх стратегийг боловсруулж, үр дүнг хууль сахиулах байгууллагын үйл ажиллагаанд нэвтрүүлэх нь ач холбогдолтой.

Кибер халдлага нь ерөнхийдөө "хакеруудын компьютерын сүлжээ, системийг гэмтээх, устгах оролдлого" гэж тодорхойлогддог[19].

Хамгийн энгийн түвшинд кибер гэмт хэргийг компьютер ашиглахтай холбоотой гэмт хэргүүд гэж тайлбарлаж болно.

Паркер[20] болон Фурнель[21] нар компьютер ба кибер гэмт хэргийн ойлголтуудыг ялгаж, дараах тодорхойлолтуудыг санал болгож байна.

1. 'Компьютерын тусламжтайгаар үйлдэгдсэн гэмт хэрэг' (Интернэтээс өмнө гарч байсан боловч кибер орон зайд шинэ амьдрал авч байгаа гэмт хэрэг, жишээ нь залилан, хулгай, мөнгө угаах, бэлгийн дарамт, үзэн ядалт, порнограф)

2. 'Компьютерт суурилсан гэмт хэрэг' буюу 'кибер гэмт хэрэг' (интернэт бий болсноор үүссэн бөгөөд үүнээс өөр байж болохгүй гэмт хэрэг, тухайлбал, хакердах, вирусийн халдлага, веб сайтад халдсан гэмт хэрэг) нь гэмт этгээд хувийн кибер домэйнийг ашигласан гэмт хэрэг юм.

Харин судлаач Д.Уолл[22] кибер гэмт хэргийг дөрвөн төрөлд хуваадаг.

1. Кибер халдлага буюу хувийн цахим орон зайд нэвтрэх эсвэл хохирол учруулах;

2. Кибер хууран мэхлэлт. Тухайлбал, зээлийн картын луйвар, оюуны өмчийн зөрчил;

3. Бэлгийн харьцааг илэрхийлсэн материалын онлайн худалдаа;

[17] Thomas, D. & Loader, B. (2000). Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. London: Routledge.
[18] Poster, M. (1990). The Mode of Information: Post-Structuralism and Social Contexts. Cambridge: Polity.
[19] Oxford Dictionary, 2018
[20] Parker, D.B. (1998). Fighting Computer Crime: A New Framework For Protecting Information. John Wiley & Sons, Inc. New York, NY, United States.
[21] Furnell, S. (2002). Cybercrime: Vandalizing The Information Society. London: Addison-Wesley.
[22] Wall, D. (2001). Cybercrimes and the Internet. in D. Wall (Ed.), Crime and the Internet. London: Routledge.

4. Хувь хүн бусдад хор хөнөөл учруулж болох янз бүрийн арга замыг илэрхийлдэг кибер хүчирхийлэл. Ийм хор хөнөөлд кибер дарамт, кибер дээрэлхэлт, болзошгүй террорист үйлдлийг сурталчлах мэдээлэл багтдаг.

Эдгээр гэмт үйлдлийн эхний хоёрт “өмчийн эсрэг гэмт хэрэг”, гуравдугаарт “ёс суртахууны эсрэг гэмт хэрэг”, дөрөвдүгээрт “хүний эрүүл мэндийн эсрэг гэмт хэрэг” байна. Мөн эхний ангилал нь "компьютерт чиглэсэн" үйлдлүүд бол сүүлийн гурван ангилал нь "компьютерын тусламжтайгаар" үйлдлүүд гэж тодорхойлогддог[23].

Өнөөгийн байдлаар дэлхийд учруулж буй заналхийллээр нэгдүгээрт кибер гэмт хэрэг, хоёрдугаарт терроризм орж байна. Монгол Улсад 2021 оны эхний хагас жилд 776 кибер орчинд үйлдэгдсэн гэмт хэрэг бүртгэгдсэн нь 2015 оноос даруй 79%-иар өссөн бөгөөд өнгөрсөн дөрвөн жилд тус гэмт хэргийн хохирогчид нийтдээ 27.4 тэрбум төгрөгийг гадаад руу шилжүүлж алдсан гэх судалгаанаас энэ төрлийн гэмт хэргийн иргэдэд учруулж буй хохирлын хэмжээ, хор уршиг хэт өндөр түвшинд байгаа төдийгүй энэ гэмт хэрэгтэй тэмцэх ажиллагааг эрчимжүүлэх шаардлага тулгамдаж байгаа болохыг харуулж байна.

Нийгэмд Кибер орчинд үйлдэгдсэн гэмт хэргийг Монгол Улсын Эрүүгийн хуулийн шинэчилсэн найруулгын 26 дугаар бүлэгт заасан “Кибер аюулгүй байдлын эсрэг гэмт хэрэг” гэж ойлгох явдал түгээмэл ажиглагдаж байна. Гэтэл Эрүүгийн хуулийн 26 дугаар бүлэгт “Кибер орчинд хууль бусаар халдах”, “Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах” гэсэн зөвхөн хоёр төрлийн гэмт хэрэг заасан бөгөөд гэмт хэргийн объект кибер аюулгүй байдал, халдлагын зүйл нь чөлөөтэйгөөр нэвтрэх боломжгүй аливаа “мэдээлэл” байдаг.

Харин кибер орчинд ямар ч төрлийн гэмт хэрэг үйлдэгдэж болох учир “Кибер аюулгүй байдлын эсрэг гэмт хэрэг”, “Кибер орчин үйлдэгдэж буй гэмт хэрэг” гэсэн ойлголтуудыг салгаж ойлгох нь зүйтэй. Тухайлбал, кибер орчинд ихээр үйлдэгддэг залилах, бусдыг заналхийлэх, илт худал мэдээлэл тараах зэрэг гэмт хэргүүдийг дурдаж болох юм.

Бидний энэхүү судалгааны ажил нь кибер аюулгүй байдлын эсрэг болон Кибер орчинд үйлдэгдэж буй гэмт хэргийн талаар ерөнхийлөн авч үзэж, тодорхой дүгнэлт, санал боловсруулахад чиглэгдсэн юм.

Кибер гэх нэршил нь кибернетик гэх үгтэй утга дүйх ба утгачлан тайлбарлавал, нарийн тооцоолон бодох техник-технологийн туслалцаатайгаар мэдээлэл боловсруулан үйл ажиллагааг удирдах буюу залуур зүй гэж ойлгогдоно. Кибер гэмт хэргийн үндсэн асуудал нь компьютерын мэдээлэл, сүлжээний эсрэг гэмт хэрэг хамаарч байна уу, эсвэл компьютерын мэдээлэл, сүлжээний тусламжтай үйлдсэн гэмт хэрэг хамаарч байна уу гэдэгт төвлөрдөг.

Кибер гэмт хэрэг гэдэгт юуг ойлгох талаар судлаачдын олон янзын байр суурь байдаг. Тухайлбал, судлаач Ц.Хүрэл-Очирын тэмдэглэснээр “...Кибер гэмт хэрэг гэдэг нь товчхондоо компьютерын гэмт хэрэг болон интернэтийн гэмт хэргийг нэрлэж буй нэр томьёо юм. Интернэтийн гэмт хэрэг гэдгийг “компьютерын сүлжээгээр үйлдэгдэж буй өөр өөр төрлийн гэмт хэргүүдийн нийлбэр” гэж томьёолж болох юм” гэж үзжээ.

[23] Smith, R., Grabosky, P. & Urbas, G. (2004). Cyber Criminals on Trial. Cambridge, England: Cambridge University Press.

Олон улсад кибер гэх тодотголтой гэмт хэрэгт: Кибер халдлага, фишинг, онлайн мөрдлөг, заналхийлэл, скимминг буюу картны гэмт хэрэг, онлайн залилан, садар самуун дүрс бичлэг тараах, интернэтэд суурилсан оюуны өмчийн эсрэг гэмт хэргүүдийг багтаан ойлгодог.

Өөрөөр хэлбэл, Эрүүгийн хуулийн тусгай ангийн 26 дугаар бүлэгт заасан гэмт хэргийн төрлүүдээр хязгаарлагддаггүй. Манай улсын хувьд Кибер орчинд үйлдэгдэж буй гэмт хэргийн тоо сүүлийн жилүүдэд харьцангуй өссөн үзүүлэлттэй байгаа нь өнөөгийн цахимжсан нийгэмд хэн бүхэн аюулд өртөх магадлал өндөр болж байгааг илэрхийлнэ.

Монгол Улсын мэдээллийн аюулгүй байдал хурцадмал нөхцөлд байгаа буюу ОУ-ын “BIG DATA” хэрэгжүүлэх байгууллагаас гаргасан дүгнэлтээр аюулд өртөх магадлал бүхий орнуудын 5 дугаарт эрэмбэлэгдэж буй талаар судалгаа гарчээ.

Үүнээс үзвэл, манай орны цахим хэрэглээний түвшин “цахим нийгмийн” хэмжээнд хүрчээ. "Цахим нийгэмшил" гэдэг нь технологийг нийгэм дэх тусдаа орон зайд байршуулахаас илүүтэйгээр нийгмийн томоохон оршин тогтнох хэсэг гэж хүлээн зөвшөөрч, өдөр тутмын амьдралын практик болгон хүлээн зөвшөөрдөг ойлголт юм[24].

Цахим технологи нь засгийн газрын зөвшөөрөлтэй тандалт хийх боломжийг нэмэгдүүлдэг. Энэ нь шүүхийн тогтолцооны эрх мэдлийн төлөөллийг улам бүр хянаж, баримтжуулж, тэдний үйлдэл, зан авирын төлөө хариуцлага хүлээлгэдэг хяналтыг дэмждэг онцлогтой.

Хяналт шалгалтын тухай ойлголтыг олон нийтийн мэдээллийн хэрэгслийн өнцгөөс харвал нийгмийн эсэргүүцлийн хөдөлгөөнүүд, улс төрийн мэдээлэл түгээх, нийгмийн зохицуулалтын хэрэгсэл болгон ашиглах нь дарангуйлагч улс орнуудын онлайн хяналтыг эрчимтэй явуулахад хүргэсэн. Тухайлбал, Бүгд найрамдах Хятад ард Улс, Иран, Умард Солонгос зэрэг улсуудыг дурдаж болох юм.

Цахим хяналтын өөр нэг тал бол хувийн нууцыг задруулах явдал юм. Хүн бүр хялбархан хандах боломжтой олон нийтийн мэдээллийн хэрэгслийн тусламжтайгаар хүмүүсийн хувийн нууцыг хүн бүр хянах боломжтой бөгөөд энэ нь үргэлж эрсдэл дагуулж байдаг.

Сошиал медиа нь хүмүүсийн соёл, эдийн засаг, нийгмийн амьдралд нөлөөлж, амьдралын салшгүй хэсэг болж, кибер дарамт, хувийн мэдээллийг хулгайлах зэрэг гэмт хэргийн бай болж байна. Нийгмийн сүлжээнд бүртгүүлэх үед хувийн мэдээллийг хулгайлах онцгой эрсдэлүүд үүсдэг бөгөөд энэ нь хэрэглэгчийн төрсөн он, сар, өдөр, төрсөн газар, гэрийн хаяг, гэр бүлийн байдал, гэр бүлийн гишүүдийн нэр зэрэг "хувийн мэдээллийг" хууль бусаар ашиглахыг шаарддаг.

Энэ төрлийн мэдээллийг санхүүгийн үйлчилгээнд баталгаажуулахын тулд ихэвчлэн ашигладаг бөгөөд олон нийтийн мэдээллийн хэрэгслээр хуваалцах нь залилах гэмт хэргийн эх сурвалж болдог.

Энэ утгаараа фейсбүүк, твиттер зэрэг сошиал медиа хэрэглэгчид бусдаас илүү хувийн мэдээллийг хулгайлах гэмт хэргийн хохирогч болох магадлал өндөр ба идэвхтэй хэрэглэгч байх хугацаа нэмэгдэхийн хэрээр хохирогч болох эрсдэл нэмэгддэг нь харагдаж байна.

[24] Lupton, D. (2014). Digital Sociology. London: Routledge.

Олон нийтийн мэдээллийн хэрэгслээр дамжуулан дэлгэсэн мэдээллийг уламжлалт гэмт хэрэг үйлдэхэд хялбар болгоход ашиглаж болно. Жишээлбэл, аяллын төлөвлөгөө эсвэл бодит цагийн байршлаа тэмдэглэдэг хэрэглэгчид бодит ертөнцөд хулгайчдад боломж олгох эрсдэлтэй.

Сошиал медиа нь харилцаа холбооны хэрэгсэл төдийгүй энэ орчинд хариу үйлдэл үзүүлэх цаг маш хурдан явагддаг тул гэмт хэргийн чухал хэрэгсэл болоод байна. Нөгөөтээгүүр нийгмийн сүлжээ бол хууль сахиулах байгууллагын ажилтнуудын гэмт хэргээс урьдчилан сэргийлэх хэрэгсэл юм.

Facebook, Twitter, YouTube зэрэг олон нийтийн мэдээллийн сайтууд олон сая идэвхтэй хэрэглэгчидтэй бөгөөд хүмүүс эдгээр веб сайтуудыг ашиглан хоорондоо шууд харилцдаг нь үүний илрэл билээ.

Кибер гэмт хэргийн ангилал (Кибер аюулгүй байдлын эсрэг гэмт хэрэг, кибер орчинд үйлдэгддэг гэмт хэрэг)

Кибер аюулгүй байдлын эсрэг гэмт хэргүүд гарч, хүмүүсийн сэтгэлийг түгшээж байгаа энэ үед эдгээр гэмт хэргүүдийг судлах, ангилах шаардлага гарч ирж байна.

Компьютерын сүлжээ, тэр дундаа интернэтийн салбарт тулгамдаж буй асуудлуудыг бүрэн үнэлж, дүгнэж чадахгүй байгаа нь шинэ төрлийн гэмт хэрэг, зөрчлүүд гарч ирж байгаатай шууд холбогдоно. Үүний үр дүнд ямар үйлдэлд шийтгэл оногдуулах эс оногдуулах нь ойлгомжгүй байдлыг бий болгож байна.

Кибер аюулгүй байдлын эсрэг гэмт хэргийг хөндөж буй зарим шинжээчид энэ хүрээнд багтах магадлалтай үйлдлүүдийг бүлэгт хувааж ангилах шаардлагагүй гэж үзэж байгаа бол зарим шинжээч эдгээр гэмт хэргийг хэд хэдэн үндсэн бүлэгт авч үздэг.

Нэгдсэн Үндэстний Байгууллагын ангилал

Нэгдсэн Үндэстний Байгууллага нь байгуулсан гэрээ хэлцлээрээ гишүүн орнуудынхаа талаар заавал биелүүлэх шийдвэр гаргах эрхтэй. Юуны өмнө, 1990 онд болсон Гэмт хэргээс урьдчилан сэргийлэх, гэмт хэрэгтэнтэй харьцах тухай VIII их хуралд тавьсан илтгэлд НҮБ-ын Ерөнхий Ассамблейгаас кибер орон зайг зохицуулах тухай шийдвэрүүд багтсан. Үүнээс улбаалан гэмт хэргээс урьдчилан сэргийлэх, хамтран ажиллах тухай эрүүгийн болон байцаан шийтгэх хуульд НҮБ-ын кибер гэмт хэргээс урьдчилан сэргийлэх, хянах үндсэн чиглэлийг нэмж оруулсан[25].

2001 онд НҮБ-ын Ерөнхий Ассамблей олон улсын хамтын ажиллагааг хангах, дэмжих, кибер гэмт хэрэгтэй тэмцэх чиглэлээр эрх баригчдыг сургах зорилгоор "Мэдээллийн технологийг урвуулан ашиглахтай тэмцэх" шийдвэр гаргасан.

Энэ ангиллын дагуу цахим гэмт хэрэг нь дараах байдалтай байна.

1. Компьютерын систем, үйлчилгээнд зөвшөөрөлгүй нэвтрэх

Зөвшөөрөлгүй нэвтрэх: Компьютерын систем эсвэл сүлжээнд зөвшөөрөлгүй нэвтрэх ойлголтыг авч үзэх бөгөөд зарим систем эсвэл бүх программ, түүнд агуулагдаж буй өгөгдөлд хандахыг хэлнэ. Компьютерт зөвшөөрөлгүй нэвтрэх нь шууд эсвэл модемын шугам ашиглан зайнаас нэвтрэх хэлбэртэй ч байж болно.

[25] KARADAĞ Şerife, Siber Uzayda Uluslararası Hukuk Mümkün mü?, Selçuk Üniversitesi, 2019 http://sssjournal.com/Makaleler/1545056113_06_5-36.ID1522_Karada%c4%9f_2827-2833.pdf

Зөвшөөрөлгүй чагнах: Техникийн хувьд компьютер эсвэл сүлжээний систем ашиглан харилцаа холбоог зөвшөөрөлгүйгээр чагнах явдал юм.

Дансны зөрчил: Компьютерын системээс нэвтэрч болох хэн нэгний дансыг ямар нэгэн төлбөр төлөхөөс зайлсхийх зорилгоор хууль бусаар ашиглахыг ойлгоно. Өөрөөр хэлбэл, тухайн хүний зөвшөөрөлгүйгээр тухайн хүний дансыг интернэт, утас болон түүнтэй адилтгах системд хууль бусаар ашиглах явдал юм.

2. Компьютерын хорлон сүйтгэх ажиллагаа

Вирус: Системийн үйл ажиллагаанд саад учруулах зорилгоор компьютерын өгөгдөл, программыг оруулах, байршуулах, өөрчлөх, устгах, таслан зогсоох үйлдэл юм. Тухайлбал, "трояны морь", "вирус", "өт" зэрэг программ хангамжийг ашиглан өгөгдөл, программыг өөрчлөх, устгах, хулгайлах, ажиллах боломжгүй болгох явдал юм.

Цахим залилан: Компьютер, харилцаа холбооны технологи ашиглан мэдээлэл олж авах, өөрчлөх, устгах замаар өөртөө болон бусдад эдийн засгийн хууль бус ашиг олох зорилгоор хохирогчийг хохироох явдал юм.

Гэмт этгээдийн зорилго нь өөртөө болон бусдад санхүүгийн ашиг олох, хохирогчийг ноцтой хохирол учруулах явдал юм. Цахим залилангийн гэмт хэрэг нь гэмт хэрэгтнүүд орчин үеийн компьютерын технологи, сүлжээний системийн давуу талыг ашигладгаараа онцгодог залилангийн гэмт хэргээс ялгаатай.

Картын залилан: Картын төлбөрийн системийг ашиглан залилан мэхлэх, хулгайлах гэмт хэрэг юм. Эдгээр нь зээлийн карт, дебит карт болон түүнтэй төстэй карт ашиглан үйлддэг залилангийн гэмт хэрэг юм. Картын төлбөрийн системийг ихэвчлэн банкнууд эсвэл ижил төстэй санхүүгийн байгууллагууд ашигладаг. Хандалтыг ихэвчлэн карт эсвэл ижил төстэй системээр хийдэг бөгөөд тухайн хэрэглэгч нууц дугаараа оруулах шаардлагатай. Эдгээр картуудыг хулгайлах, хуулбарлах, хуулбарлах, холбооны шугамыг хаах, таслан зогсоох зэргээр луйвар гардаг.

Оролт/гаралт/программын хууран мэхлэлт: Энэ нь компьютерын системд санаатайгаар буруу өгөгдөл оруулах, системээс буруу гаралт авах, систем дэх программуудыг өөрчлөх замаар залилан мэхлэх, хулгайлах явдал юм. Компьютерын мэдээллийн санд буруу мэдээлэл оруулах нь залилангийн нийтлэг хэлбэр юм.

Харилцаа холбооны үйлчилгээг хууль бусаар, зөвшөөрөлгүй ашиглах: Харилцаа холбооны систем дэх протокол, журмын сул талыг ашиглан өөрт болон бусдад эдийн засгийн үр өгөөж өгөх зорилгоор харилцаа холбооны үйлчилгээ болон бусад компьютерын системийг эрхгүйгээр ашиглах юм.

Хуурамчаар материал үйлдэх: Хуурамч материал (мөнгөн тэмдэгт, зээлийн карт, вексель г.м) бүтээх, эсхүл тоон орчинд хадгалагдаж буй баримт бичигт (маягт, тайлан г.м.) өөрчлөлт оруулж, эдийн засгийн хууль бус үр өгөөжийг олж авахыг хэлнэ.

Компьютерын программ хангамжийг зөвшөөрөлгүй ашиглах: Энэ нь хуулиар хамгаалагдсан программ хангамжийг зөвшөөрөлгүй хуулбарлах, хууль бусаар олж авсан компьютерын программ хангамжийг худалдах, хуулбарлах, түгээх, ашиглахыг хэлнэ.

Лицензийн гэрээний дагуу ашиглах: Энэ нь лицензийн эрхийг зөрчиж нэг компьютерт зориулж худалдаж авсан программ хангамжийг нэгээс олон компьютерт

ашиглах явдал юм. Нэг компьютерт худалдаж авсан программ хангамжийг лицензийн эрхийн хүрээнд нэгээс дээш компьютерт ашиглахыг хориглоно.

Хууль бусаар хуулбарлах: Энэ нь лицензийн гэрээгээр хамгаалагдсан программ хангамжийг хадгалсан хэвлэл мэдээллийн хэрэгслийг өөр мэдээллийн хэрэгсэлд хууль бусаар хуулбарлах явдал юм. Ерөнхийдөө энэ нь лицензийн гэрээг дахин зөрчиж, төлбөр төлөхгүйн тулд өмнө нь худалдаж авсан эсвэл хуулбарласан программ хангамжийг өөр зөөвөрлөгч рүү шилжүүлэх явдал юм.

Лицензийн эрхийг зөрчиж түрээслэх: Энэ нь лицензийн эрхийг зөрчиж янз бүрийн мэдээллийн хэрэгслээр бичигдсэн тоглоом, кино, программ хангамжийг түрээслэх явдал юм.

3.Бусад гэмт хэрэг

Хувийн мэдээллийг зүй бусаар ашиглах: Энэ нь өөртөө болон өөр хүнд ашиг тустай, хор хөнөөл учруулах зорилгоор худалдааны болон мэргэжлийн нууц, хувийн мэдээлэл болон бусад үнэ цэнтэй мэдээллийг ашиглах, худалдах, түгээх явдал юм. Тодруулж хэлбэл, банк, эмнэлэг, худалдааны төв, төрийн байгууллага гэх мэт байгууллагад хадгалагдаж буй аливаа хувийн мэдээллийг зөвшөөрөлгүйгээр бусдад ашиг олох, хор хөнөөл учруулах зорилгоор ашиглах явдал юм.

Хуурамч бүртгэл үүсгэх: Энэ нь бусдыг хууран мэхлэх замаар хор хөнөөл учруулах зорилгоор бодит хүмүүсийг дуурайлган эсвэл зохиомол хүмүүсийг бий болгох явдал юм. Энэ арга нь бодит хүмүүсийн мэдээллийг ашиглан тухайн хүний ард нуугддагаараа онцлогтой[26].

Олон улсын цахилгаан холбооны байгууллагын ангилал

ОУЦХБ нь кибер гэмт хэргийг 4 үндсэн агуулга дор нэгтгэсэн. Үүнд:

1) Компьютерын өгөгдөл, системийн нууцлал, бүрэн бүтэн байдал, ашиглалтын эсрэг гэмт хэрэг (хууль бусаар нэвтрэх, өгөгдөл хулгайлах, өгөгдөлд хөндлөнгөөс оролцох гэх мэт),

2) Компьютертой холбоотой гэмт хэрэг (онлайн мөрийтэй тоглоом, хувийн мэдээллийг хулгайлах, хураамжийг хуурамчаар үйлдэх гэх мэт),

3) Агуулгатай холбоотой гэмт хэрэг (арьс өнгөөр ялгаварлан гадуурхах, үзэн ядсан үг хэллэг, хүчирхийллийг магтсан, ташаа мэдээлэл гэх мэт) болон

4) Зохиогчийн эрхийн зөрчил (зохиогчийн эрх, оюуны өмчийн эрхийг зөрчсөн) гэж ангилжээ.

Кибер гэмт хэрэг үйлдэгддэг түгээмэл арга

Цахим гэмт хэрэг нь зорилгын хувьд сонгодог гэмт хэргүүдтэй төстэй ч арга, хэрэгслийн хувьд ялгаатай байдаг. Эдгээр гэмт хэрэг нь интернэт, компьютер, пос машин, гар утас болон бусад төрлийн технологийн хэрэгслийг ийм төрлийн гэмт хэрэг үйлдэх хэрэгсэл болгон ашигладгаараа сонгодог гэмт хэргээс эрс ялгаатай.

[26] TURHAN Oğuz, Siber Suçlar, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/01/Bilgisayar_Aglari_ile_ilgili_Suclar_OguzTurhan.pdf

Эдгээр гэмт хэрэг нь ямар ч биет газар орон шаардлагагүйгээр дэлхийн хаана ч, ямар ч компьютер, интернэт сүлжээгээр үйлдэж болох бөгөөд иргэн, аж ахуйн нэгж, байгууллагад их хэмжээний хохирол учруулж болзошгүй.

Кибер гэмт хэрэг үйлдэгчид гэмт хэрэг үйлдэхдээ нэгээс олон арга, техникийг хэрэглэдэг. Тухайлбал,

• Веб сайтуудын нүүр хуудсыг устгаж, хүссэн газар руу нь чиглүүлэх,

• Нээлттэй сайтуудын контент руу нэвтэрч, өгөгдлийг хуулах замаар мэдээлэл хулгайлах, задруулах,

• Нэвтрэх боломжтой сайтуудыг устгах замаар ашиглах боломжгүй болгох,

• Хувь хүн, албан байгууллагын компьютерт вирус, түүнтэй адилтгах хортой программ суулгаж хохирол учруулах,

- Мэдээлэл хулгайлах замаар дараагийн кибер гэмт хэрэгт ашиглах мэдээлэл олж авах,

• Кибер орчныг хууль ёсны болон хууль бус үйл ажиллагааг сурталчлах талбар болгон ашиглах, эсхүл хууль бус үйл ажиллагааг зохион байгуулах,

• Зохиогчийн эрхээр хамгаалагдсан материал, компьютер тоглоом, программ хангамжийн хамгаалалтын нууц үгийг эвдэж, хууль бусаар ашиглах,

• Кибер орчинд бусдын эрхэд халдах, залилан мэхлэх зорилгоор ашиглах,

• Кибер орчинд хүүхдийн порнографыг үйлдвэрлэх, хадгалах, хуваалцах, ашиглах боломжтой болгох.

Хакердах: Өнөө үед хакерууд системийн аюулгүй байдлыг давж хандалт олж авах, интернэтээр бусад компьютерт хууль бусаар нэвтрэх боломжийг бүрдүүлж байна. Тэд энэхүү хууль бус хандалтыг программчлах эсвэл системийн эмзэг байдлыг ашиглах, хортой программ хангамж ашиглан гүйцэтгэдэг. Системийн аюулгүй байдлын мэргэжилтэн эсвэл админ хууль бус хандалтыг анзаарч, хөндлөнгөөс оролцох хүртэл хакер нь системээс өгөгдөл хулгайлах, өгөгдлийг устгах, системийг гэмтээх зэрэг хууль бус үйлдэл хийх боломжтой.

Фишинг халдлага: Энэ нь кибер гэмт хэрэгтнүүдийг кредит картын мэдээлэл гэх мэт интернэт хэрэглэгчдийн нууц мэдээ, мэдээллийг бэлтгэдэг хуурамч хуудас эсвэл янз бүрийн арга техникээр бэлтгэсэн хуурамч сайт руу чиглүүлэх замаар нууц мэдээллийг оруулах боломжийг олгох зорилготой халдлага юм.

Фишинг халдлага нь өнөөдөр хакеруудын дунд өргөн хэрэглэгддэг арга бөгөөд сүүлийн үед улам бүр идэвхжиж байна. Интернэтийг өргөнөөр ашигласнаар цахим банкны гүйлгээг ухаалаг гар утсаараа компьютер, тэр ч байтугай гар утасны программ ашиглан хялбар, хурдан хийх боломжтой болсон. Харин олон улсад ялангуяа банкны цахим хуудсуудыг хуулбарлан хэрэглэгчийг хуурамч сайт руу чиглүүлэхийг оролддог арга ихээхэн нэмэгдсэн байна.

Компьютерын вирус ба өт: Компьютерын вирусүүд нь кодчилол, программын нэг төрөл бөгөөд сүлжээ эсвэл USB санах ойн хэлбэрийн гадаад хадгалалтын нэгжээр дамжуулан бусад компьютерт халдварладаг. Кодлох замаар халдвар авсан зорилтот

компьютерт вирус хаана суурьших, хэзээ юу хийх, ямар өгөгдлийг устгах, хуулах, системийг хэрхэн гэмтээх зэрэг нь тодорхойлогддог. Ерөнхийдөө вирус нь системийг гэмтээж, аль болох их тархах, аль болох олон системийг гэмтээх гэж оролддог. Вирусийн хамгийн түгээмэл төрөл бол ".exe" өргөтгөл юм.

Ransomware: Өнөөдөр түгээмэл болсон, ялангуяа сүүлийн үед байнга хэрэглэгдэж байгаа энэ арга нь бүх хэрэглэгчдэд, ялангуяа томоохон байгууллага, компаниудад заналхийлж байна. Гэмт хэрэгтэн энэ аргаар системд нэвтэрсэн хортой программ хангамжийг ашиглан систем дэх файл, баримт бичгийг түгжиж, хохирогчоос баримт бичгийг сэргээх төлбөрийг авдаг. Эдгээр гэмт хэрэгтнүүд ихэвчлэн өнөөдөр өргөн хэрэглэгддэг криптовалют болох биткойн болон дериватив криптовалютуудыг ил болгохгүйн тулд төлбөрийг нэргүй данс руу шилжүүлэхийг шаарддаг. "Wannacry" болон "Notpetya" нь алдартай ransomware юм.

Гарын үйлдлийг бүртгэх программ (Keylogger): Эдгээр нь гар ашиглан хэрэглэгчийн оруулсан мэдээллийг барьж аваад халдагчид илгээдэг программ юм. Эдгээр нь бидний хувийн амьдрал, арилжааны болон банкны гүйлгээний аюулгүй байдалд маш ноцтой аюул учруулж байна. Зөвхөн программ хангамж төдийгүй гарын доор байрлуулсан төхөөрөмжөөр гүйцэтгэх боломжтой энэ үйлдэл нь аюулгүй байдлын эсрэг маш ноцтой байдлыг бий болгож байна.

Үйлчилгээний тархалтаас татгалзах халдлага (DDOS): Distributed Deial of Service Attack нь Botnets хэмээх серверийг хэт ачаалснаар үйлчилгээг удаашруулах, хаах зорилготой халдлага юм. Ботнетийн тодорхойлолт нь бот компьютер, зомби компьютер эсвэл боол компьютер гэж нэрлэгддэг системийг суулгасан сүлжээ юм.

Энэ нь нэг буюу хэд хэдэн сервер дээр олон тооны бот компьютер ачаалснаар хийдэг халдлага юм. Ботнет нь серверийн компьютерт олон хүсэлт илгээж, серверийг ажиллах боломжгүй болгохыг оролддог.

Нийгмийн инженерчлэлийн халдлага: Кибер гэмт хэрэгт ашигладаг аргуудын нэг бол нийгмийн инженерчлэлийн арга юм. Нийгмийн инженерчлэл бол хүмүүсийг танихгүй хүнийхээ төлөө хийдэггүй зүйлээ хийлгэх урлаг юм. Энэ нь техник технологи ашиглахаас илүүтэй хүмүүсийг хууран мэхлэх замаар мэдээлэл олж авах явдал юм. Нийгмийн инженерчлэлийн арга нь янз бүрийн мэдээлэл олж авах замаар хүмүүсийг хууран мэхлэн системийг гэмтээж, мэдээлэл хулгайлж, системийг булаан авах зорилготой юм.

Хүсээгүй цахим шуудан (спам): Спам нь хэрэглэгчийн хүсэлтгүйгээр интернэтээр олон тооны хэрэглэгчдэд янз бүрийн агуулгаар илгээгддэг захидал юм.

Спам илгээгч гэгддэг эдгээр хүмүүс олж авсан цахим шуудангийн хаягаараа мэдээллийн сан үүсгэж, янз бүрийн агуулгатай шуудан, ялангуяа төрөл бүрийн салбартай холбоотой зар сурталчилгаа явуулах, эсвэл энэ мэдээллийн санг мөнгөөр зардаг. Спам нь ерөнхийдөө аливаа бүтээгдэхүүнийг сурталчлах, зах зээлд гаргах, порнографын сурталчилгаа, мессежийг дэлхийн үзэгчдэд хүргэх зорилготой.

Хууль бус контент оруулах: Хууль бус контентыг оруулах үйлдэл нь нийтлэхийг хориглодог садар самуун, хувийн эрхийг зөрчсөн, зохиогчийн эрхийг зөрчсөн, хүүхдийн садар самууныг агуулсан контентыг интернэт хэрэглэгчдэд нээлттэй болгох явдал юм.

§1.3. Кибер орчинд үйлдэгдэж байгаа гэмт хэрэгтэй тэмцэх эрх зүйн зохицуулалт

XX зууны дунд үеэс эхлэн ашиглагдаж, хөгжиж эхэлсэн мэдээлэл, харилцаа холбооны технологи нь амьдралын бүхий л салбарт өдрөөс өдөрт асар их өөрчлөлтийг бий болгож, эдгээр технологиор бий болсон шинэ хэрэгсэл, үйлчилгээнүүд нь хүн амын амьдралд нөлөөлсөөр байна.

Мэдээллийн технологи, тэдгээрийн санал болгож буй үйлчилгээ нь мөн чанараараа улс орнуудын үндэсний дэг журамд төдийгүй олон улсын хамтын нийгэмлэгт нөлөөлдөг. Мэдээллийн технологийн бүтээгдэхүүн, мэдээллийн нийгмийн үйлчилгээ нь орчин үеийн хувь хүний өдөр тутмын амьдралыг бараг бүхэлд нь бүрхсэн. Интернэтэд холбогдох боломжтой гар утас, ялангуяа компьютер, бэлэн мөнгөний машин, интернэтээр дамжуулан хийх банкны гүйлгээ, мэдээллийн сүлжээгээр төрийн төрөл бүрийн үйлчилгээ үзүүлэх зэрэг нь орчин үеийн хүн төрөлхтний амьдралыг хөнгөвчлөх томоохон боломжийг олгож байна[27].

Мэдээллийн технологи хурдацтай өөрчлөгдөж, хэлбэржиж, шинж чанар нь энэ салбарт зохицуулалт хийх зайлшгүй шаардлага бий болгож байна. Мэдээллийн технологийн орчинд үйлдэгдэж буй гэмт хэрэг хурдацтай нэмэгдэж, эдгээр гэмт хэргийг илрүүлэхэд учирч буй хүндрэл, үйлдэхэд хялбар байдал, эдийн засгийн хохирлын хэмжээ нь энэ талаар эрх зүйн зохицуулалт хийхэд хүндрэлтэй байгааг тодорхой харуулж байна.

Дэлхий дахинд кибер гэмт хэрэгтэй холбоотой зохицуулалтад хоёр өөр аргыг ашигладаг нь харагдаж байна. АНУ, Англи, Ирланд, Португал зэрэг улсуудыг багтаасан эхний системд одоо байгаа хуулиас гадна тусгай зохицуулалтыг бий болгодог. Германы хууль тогтоомжоор анхлан нэвтрүүлсэн хоёр дахь системд эрүүгийн үйлдлийг одоо мөрдөж буй хууль тогтоомжийн хүрээнд шалгадаг бөгөөд тусдаа бүлэг, хуулиудыг гаргадаггүй. Энэ системд гэмт хэргийн тодорхойлолтыг цахим гэмт хэрэг гэж өөрчлөх, хуулиудад шинээр акт оруулах замаар тулгарсан асуудлыг шийдвэрлэхийг оролддог.

Дэлхий дахинд өрнөж буй хурдацтай хөгжилтэй зэрэгцэн манай улсад цахим хэрэглээ амьдралын эерэг, сөрөг аль ч үе шатанд эрчимтэй ашиглагдаж байна.

Кибер халдлага нь ихэвчлэн хулгай (төлбөрийн картын өгөгдөл, хэрэглэгчийн мэдээлэл, компанийн нууцлал эсвэл оюуны өмчийн), сүлжээнд зөвшөөрөлгүй нэвтрэх, санхүүгийн болон нэр хүндэд хохирол учруулах зорилгоор ашигладаг болох нь тогтоогдсон. Энэ төрлийн гэмт хэргийг таслан зогсоох, мөрдөн шалгах ажиллагаа явуулахын тулд салбарын зарим нэр томьёоны талаар ойлголттой байх шаардлагатай. Тухайлбал, 2021 оны 12 дугаар сарын 17-ноос дагаж мөрдөж байгаа “Кибер аюулгүй байдлын тухай” хуулийн 4 дүгээр зүйлд дараах нэр томьёонуудыг тайлбарлан оруулсан байдаг. Үүнд:

"кибер аюулгүй байдал" гэж кибер орчинд мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдал хангагдсан байхыг;

"кибер орон зай" гэж интернэт болон бусад мэдээлэл, харилцаа холбооны сүлжээ, тэдгээрийн ажиллагааг хангах мэдээллийн дэд бүтцийн харилцан хамааралтай цогцоос бүрдсэн биет болон биет бус талбар;

[27] TAŞCI Ufuk ve CAN Ali, “Türkiye’de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014,” Fırat Üniversitesi Sosyal Bilimler Dergisi 25, Sayı 2 (Temmuz, 2015): 232.

"кибер орчин" гэж мэдээлэлд хандах, нэвтрэх, цуглуулах, түүнийг боловсруулах, хадгалах, ашиглах боломж олгож байгаа мэдээллийн систем, мэдээллийн сүлжээний орчныг;

“бүрэн бүтэн байдал" гэж мэдээллийг зөвшөөрөлгүй устгах, өөрчлөхөөс хамгаалсан байхыг;

"нууцлагдсан байдал" гэж мэдээлэлд зөвшөөрөлгүй хандах, нэвтрэх боломжгүй байхыг;

"хүртээмжтэй байдал" гэж зөвшөөрөгдсөн хүрээнд мэдээлэлд хандах, нэвтрэх, цуглуулах, ашиглах боломжтой байхыг;

“мэдээллийн систем" гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.1-д заасныг;

"мэдээллийн сүлжээ" гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.2-т заасныг;

"кибер аюулгүй байдлын эрсдэлийн үнэлгээ" гэж цахим мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдал алдагдах, аюул занал тохиолдох магадлал, эмзэг байдлын түвшин, түүнээс үүсэх үр дагавар, эрсдэлийг бууруулах, урьдчилан сэргийлэх арга хэмжээг тодорхойлох мэргэшсэн үйл ажиллагааг;

“мэдээллийн аюулгүй байдлын аудит" гэж кибер аюулгүй байдлын хууль тогтоомж, холбогдох журам, стандартад нийцсэн эсэхэд дүгнэлт гаргах, зөвлөмж өгөх хараат бус хөндлөнгийн мэргэжлийн үйл ажиллагааг;

"мэдээллийн системийн үйлдлийн бүртгэл" гэж тухайн мэдээллийн системд хандсан, нэвтэрсэн, боловсруулсан, цуглуулсан, ашигласан үйлдэл, цаг хугацааг тодорхойлох бүртгэлийг;

"онц чухал мэдээллийн дэд бүтэцтэй байгууллага" гэж кибер аюулгүй байдал алдагдсанаар хэвийн үйл ажиллагаа нь доголдож Монгол Улсын үндэсний аюулгүй байдал, нийгэм, эдийн засагт хохирол учруулж болох мэдээллийн систем, мэдээллийн сүлжээ бүхий байгууллагыг;

"кибер аюулгүй байдлын зөрчил" гэж мэдээллийн системийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдалд заналхийлж байгаа аливаа үйлдэл, эс үйлдлийг;

"кибер халдлага" гэж мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдлыг алдагдуулах зорилго бүхий үйлдлийг;

"үндэсний хэмжээний кибер халдлага" гэж онц чухал мэдээллийн дэд бүтэцтэй байгууллагын мэдээллийн систем, мэдээллийн сүлжээнд халдсаны улмаас тухайн байгууллагын хэвийн үйл ажиллагааг алдагдуулж, Монгол Улсын үндэсний аюулгүй байдал, нийгэм, эдийн засагт хохирол учруулахуйц кибер халдлагыг;

"кибер халдлага, зөрчилтэй тэмцэх төв" гэж кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, мэдээллийн системийг нөхөн сэргээх үйл ажиллагааг зохицуулж, мэргэжлийн удирдлагаар хангах үндсэн чиг үүрэг бүхий этгээдийг;

"төрийн мэдээллийн нэгдсэн сүлжээ" гэж төрийн байгууллага хоорондын мэдээлэл солилцох, кибер аюулгүй байдлыг хангахад чиглэсэн нэгдсэн дэд бүтэц бүхий төрийн интернэт хэрэглээ, албан болон тусгай хэрэглээний сүлжээний цогцыг гэж тус тус заажээ.

Кибер аюулгүй байдлын эсрэг гэмт хэргийн онцлог нь цаг хугацаа, орон зай, нутаг дэвсгэр үл хамааран үйлдэгддэг. Өөрөөр хэлбэл, аливаа хүн аль нэг улсад оршин суудгаас үл хамаарч цахим төхөөрөмж, сошиал орчинд идэвхтэй байдаг л бол энэ төрлийн гэмт хэргийн хохирогч болох эрсдэлтэй.

Тиймээс ийм төрлийн гэмт хэргийг шалгахад цаг хугацаа, хөрөнгө мөнгө, мэргэжилтэн ихээр шаардагдана. Манай улсад хуурамч хаяг ашиглан насанд хүрээгүй хүүхдүүдтэй харилцаа үүсгэж, нүцгэн зургийг нь авч, цаашид тэр зургаар дамжуулан дарамтлах, мөнгө шаардах, эрхшээлдээ оруулахыг санал болгох, хуулиар хориглосон бараа бүтээгдэхүүний худалдаа зохион байгуулах буюу галт зэвсэг, хар тамхи, мансууруулах бодис, согтууруулах ундааны зүйл худалдаалах, бусдын нэр төрд халдах, айлган сүрдүүлэх, гүтгэн доромжлох, ялгаварлан гадуурхах, онлайн худалдаа гэх нэрээр залилах буюу зээлийн картын залилан хийх, урьдчилгаа төлбөрийн залилан, интернэт маркетинг болон жижиглэн худалдааны луйврын гэмт хэрэг түгээмэл бүртгэгджээ.

Цар тахлын үед онлайн худалдаа эрчимжсэнтэй холбоотойгоор энэхүү үйл явцыг гэмт хэрэг үйлдэхдээ ашиглаж буй тохиолдол багагүй бүртгэгдэж, цаашид өсөх шинжтэй байна.

Мөн мөрийтэй тоглоом, азын сугалаа зохион байгуулах нэрийдлээр ашиг олох, иргэдийг хохироох, интернэт дэх оюуны өмчийн эсрэг гэмт хэрэг буюу зохиогчийн эрх болон түүнд хамаарах эрхийг зөрчсөн гэмт хэрэг бас тодорхой хэмжээнд үйлдэгдсээр байна.

Монгол Улсын Эрүүгийн хуулийн 26 дугаар бүлэгт: 26.1 “Кибер орчинд хууль бусаар халдах”, 26.2 “Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах” гэсэн хоёр гэмт хэргийн талаар зүйлчилж зохицуулсан байдаг.

Кибер орчинд хууль бусаар халдах

1.Кибер орчинд зөвшөөрөлгүйгээр хандаж мэдээллийн систем, мэдээллийн сүлжээнд нэвтэрсэн, танилцсан;

2.Кибер орчинд хууль бусаар халдаж мэдээллийг устгасан, гэмтээсэн, өөрчилсөн, засварласан, нуусан, нэмж оруулсан, хуулбарлаж авсан, ашиглах боломжгүй болгосон;

3.Кибер орчинд хууль бусаар халдаж мэдээллийн систем, мэдээллийн сүлжээг ашиглах боломжгүй болгосон, хэвийн үйл ажиллагааг алдагдуулсан, хандалтад хязгаарлалт тогтоосон, ноцтой саад учруулсан;

Төрийн нууцад хамаарах мэдээлэл агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээнд; төрийн мэдээллийн нэгдсэн сүлжээний албан болон тусгай хэрэглээний сүлжээнд; онц чухал мэдээллийн дэд бүтэцтэй байгууллагын мэдээллийн систем, мэдээллийн сүлжээнд халдсанд;

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

Энэ гэмт хэргийг үйлдэх зорилгоор мэдээллийн систем, мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай программ, техник хэрэгслийг бэлтгэсэн, борлуулсан; программ

хангамжийг тусгайлан зохиосон, зориудаар ашигласан, санаатай тараасан бол ял оногдуулахаар заасан.

Кибер орчинд үйлдэгдэж буй гэмт хэрэг нь дараах шалтгаан, нөхцөлтэй байна:

1. Иргэд нийгмийн сүлжээ хэрэглэгчийн нэвтрэх нэр, нууц үгийг өөрийн нэр, төрсөн огноо, утасны дугаар гэх зэргийг бусад хүн тааварлаж болохуйц хялбар байдлаар /гар утасны дугаар, төрсөн огноо, автомашины дугаар г.м/ үүсгэдэг;

2. Өгөөш бүхий мэдээллийг уншихаар сонирхон дарж нэвтрэх нэр, нууц үгээ алддаг, "зээл олгоно", "илгээмж явуулна" "сугалаанд хожсон", гэх байдлаар иргэдийг төөрөгдөлд оруулж, амар хялбар аргаар мөнгө олох гэсэн санаа, сэдлийг төрүүлж улмаар уг зүйлсийн татвар хураамж, тээврийн зардлыг шилжүүлнэ үү гэх зэргээр цахим мэдээллийн хэрэгслээр түгээгдэж буй мэдээлэл үнэн зөв эсэх талаар нягтлан судалж үздэггүй;

3. Кибер орчинд хүүхдэд тавих хараа хяналт сул, хүүхэд бүх төрлийн сөрөг мэдээллийг авах боломж нээлттэй;

4. Цахим мэдээллийн хэрэгслийг зохих түвшинд ашиглах мэдлэг дутмаг, хувь хүний амар хялбар аргаар мөнгө олох гэсэн сэтгэл зүйн онцлог, хайхрамжгүй байдал тодорхой хэмжээгээр нөлөөлсөн гэж үзэхээр байна.

Үүнээс гадна Европын зөвлөл мэргэжлийн экспертүүдийн хороо байгуулж, хууль зүйн асуудлыг хэлэлцсэний үр дүнд Зөвлөмж №R(89)9 гаргасан байна. Энэхүү зөвлөмжид компьютертэй холбоотой хууль зөрчсөн үйлдлүүдийн жагсаалтыг гаргасан байжээ.[28]

Мөн 1990 онд энэхүү асуудлыг Монтреал хотод болсон Харьцуулсан эрх зүйн Олон улсын Академийн 13 дугаар Конгресс болон Гавана хотод болсон НҮБ-ын 8 дугаар Эрүүгийн эрх зүйн Конгресс[29], 1992 онд Холбооны бүгд найрамдах Герман улсын Вурцбург хотод Олон улсын конференци[30] дээр хэлэлцжээ.

Европын Холбоо нь Интернэтийн орчны хууль бус, хохирол учруулахуйц үйлдлийн эсрэг тэмцэхээр олон төрлийн арга хэмжээ авч байна. 1998 оны 4 дүгээр сард Европын Хороо Зөвлөлд Кибер аюулгүй байдлын эсрэг гэмт хэргийг судалсан тайлангаа танилцуулжээ. 1999 оны 10 дугаар сард Европын Зөвлөлийн тэргүүний уулзалтаар өндөр технологийн гэмт хэргийн тодорхойлолт, санкцийн ерөнхий ойлголтыг бий болгох хэрэгтэй гэж үзжээ. Европын Парламент өндөр технологитой холбоотой гэмт үйлдлийг эрх зүйн зохицуулалтад тусгах шаардлагатай гэж үзсэн байна.

Үндэстэн дамнасан зохион байгуулалттай, гэмт хэргийн экспертүүдийн Их наймын өндөр технологийн ажлын хэсгийн зүгээс 1997 онд компьютерын гэмт хэрэгтэй тэмцэх 10 зарчмыг боловсруулсан бол 1998 оны 3-р сард 7 өдөр 24 цагийн турш ажиллах экспертүүдийн сүлжээг өндөр технологийн гэмт хэргийг мөрдөхөд туслалцаа үзүүлэхээр байгуулжээ. Аливаа өндөр технологи ашиглах гэмт хэрэгтэнд нуугдах боломж олголгүй,

---

[28] Компьютертэй холбоотой гэмт хэрэг: Зөвлөмж № R(89) 9 198 9 оны 9 дүгээр сарын 13-ны өдөр Еюропын Зөвлөлийн Сайд нарын Хорооны баталж, Гэмт хэргийн асуудал эрхэлсэн Европын Хороонд илтгэсэн байна

[29] Ulrich Sieber: The International Emergence of Criminal Information Law, 1991, 56 p.

[30] Ulrich Sieber (ed.): Information Technology Crime – National Legislation's and International Initiatives, 1994, 49 p.

хуулийн дагуу шүүхийн өмнө хариуцлага тооцох зорилготой ажээ. Олон улс орон дээр дурьдсан 10 зарчмыг олон улсын гэрээ, үндэсний хууль тогтоомж, бодлогод тусгасан байдаг. Зарим улс энэхүү экспертийн сүлжээнд холбогдож эхэлжээ.

1999 онд АНУ-ын Калифорни мужийн Стенфордын Их сургуулийн Хүүверын институт Кибер гэмт хэрэг, терроризмтэй тэмцэх олон улсын хамтын ажиллагааны тухай конференци байгуулжээ[31].

Мөн Олон улсын хүчний байгууллага-Интерпол 1981 онд анхны Интерполын компьютерын гэмт хэргийн мөрдөн байцаагч нарын сургалт семинарыг явуулсан байдаг. 1995, 1996, 1998, 2000 онд Интерпол Компьютерын гэмт хэргийн тухай олон улсын конференци байгуулж, сүүлд 2003 оны 10 дугаар сард Солонгос улсын Сөүл хотод хуралджээ.

Стенфордын Их сургуулийн Хүүверын институтийн Кибер гэмт хэрэг, терроризмын тухайн олон улсын гэрээний төслийн 3 дугаар зүйлд ийнхүү тусгажээ:

1. Энэхүү Гэрээний дор дурьдсан гэмт үйлдлийг зөвшөөрөлгүй аливаа этгээд хууль бусаар, санаатайгаар үйлдсэн бол гэмт хэрэг үйлдсэнд тооцно:

- Гэрээнд хууль бус үйлдэлд тооцсон, эсвэл өмчлөгч этгээдэд мэдэгдэлгүйгээр, мэдэгдэхгүй байх зорилгоор кибер системийг зогсоосон, эсвэл зогсохыг мэдсээр байж, кибер системийн мэдээлэл буюу программыг зохиосон, хадгалсан, өөрчилсөн, устгасан, дамжуулсан, будилуулсан, буруу дамжуулсан, мэхлэсэн, саад хийсэн;
- Хувь хүн болон түүний өмчид бодит хохирол учруулах зорилгоор хуурамч мэдээлэл боловсруулахаар кибер системийн мэдээллийг зохиосон, хадгалсан, өөрчилсөн, устгасан, дамжуулсан, будилуулсан, буруу дамжуулсан, мэхлэсэн, саад хийсэн;
- Нэвтрэхийг хориглосон кибер орчинд тодорхой зорилгоор нэвтэрсэн;
- Хяналтын болон хууль ёсны эсэхийг шалгах механизмд саад болсон;
- Гэрээний 3,4 дүгээр Зүйлд заасан аливаа үйлдлийг хийхээр ямарваа тоног төхөөрөмж буюу программыг үйлдвэрлэсэн, худалдсан, ашигласан, олон нийтэд үзүүлсэн;
- Гэрээнд заасан аливаа хууль бус, хориглосон үйлдлийг хийхэд кибер системийг ашигласан;
- Мужийн нэгжийн дэд бүтцийг хямралд оруулах зорилгоор Гэрээний 3,4 дүгээр Зүйлд заасан аливаа үйлдлийг хийсэн.

Европын Зөвлөлийн Кибер гэмт хэргийн тухай конвенцид:

Хэсэг 1 - Эрүүгийн эрх зүй

Компьютерын мэдээлэл, системийн нууцлал, нэгдмэл байдал,

хууль ёсны байдлын эсрэг гэмт хэрэг

[31] http://www.oas.org/juridico/english/conference agenda.htm

Зүйл 2. Хууль бусаар нэвтрэх

Зүйл 3. Хууль бусаар дамжуулалтыг таслах

Зүйл 4. Мэдээлэлд саад хийх

Зүйл 5. Системд саад хийх

Зүйл б. Хууль бусаар тоног төхөөрөмжийг ашиглах[32] хэмээн заасан байна.

[32] http://conventions.coe.int/treaty/EN/projets/FinalCybercrime.htm

Хүснэгт 1. Зарим улсын хууль тогтоомжид кибер гэмт хэргийн талаарх эрх зүйн зохицуулалт

№	Улс	Ял, шийтгэл
1	**Австри**	Нууцын тухай хууль (Privacy Act; 2000.01.01) Хэсэг 10. Зүйл 52. Захиргааны хариуцлага (1) Тухайн гэмт үйлдэл нь шүүхийн шийдвэрийн хариуцлага тооцох үйлдэлд хамаарахгүй буюу бусад захиргааны хариуцлагын зүйлээр хариуцлага тооцох боломжгүй бол захиргааны буруутай үйлдэлд тооцож, 260,000 хүртэл торгууль оногдуулна. а/ Тухайн этгээд санаатайгаар мэдээллийн санд нэвтэрсэн буюу санаатайгаар хууль бус, шууд, тодорхой нэвтрэх үйлдэл хийсэн б/ Мэдээллийн нууцлал гэсэн 15-р зүйлийг зөрчиж, мэдээллийг дамжуулсан, тус хуулийн 4 6, 4 7-р зүйлийн дагуу тухайн этгээдэд хариуцуулсан мэдээллийг бусад зорилгоор ашигласан в/ хууль ёсны шийдвэрийн эсрэг мэдээллийг ашигласан, мэдээллийг нуун дарагдуулсан, хуурамч мэдээллийг засахгүй орхисон, хуурамч мэдээллийг устгахгүй орхисон г/ Хэсэг 7, Зүйл 27-д заасныг зөрчин, мэдээллийг санаатайгаар устгасан бол хариуцлага тооцно.
2	**Бельги**	Бельгийн Парламент 2000 оны 11 сард Эрүүгийн хуульдаа компьютерын гэмт хэргийн тухай шинэ заалт батлан оруулж, 2001 оны 2 сарын 13-наас хүчин төгөлдөр болжээ. Эрүүгийн гэмт үйлдэлд хамаарах 4 үндсэн асуудлыг хуульчилсан нь компьютерын хуурамч баримт бичиг, компьютерын залилан мэхлэлт, хакерын ажиллагаа, хортой үйл ажиллагаа болно. IV. Компьютерын хакерын ажиллагаа Эрүүгийн хуулийн Зүйл 550(b) 1. Аливаа этгээд зөвшөөрөлгүй гэдгээ мэдсээр байж, компьютерын системд нэвтрэх буюу холбоотой байвал 3 сараас 1 жил хүртэл хугацаагаар хорих, (5,200-5,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ. Хэрэв залилан мэхлэх зорилгоор энэхүү үйлдлийг хийсэн бол 6 сараас 2 жил хүртэл хугацаагаар хорих ял шийтгэнэ. 2 Аливаа этгээд залилан мэхлэх, эсвэл хохирол учруулах зорилгоор компьютерын системд нэвтэрсэн бол 6 сараас 2 жил хүртэл хугацаагаар хорих, (5,200-20,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ. 3 Дээрх 1, 2-р заалтад заасан гэмт хэргийг үйлдэж байгаагаа мэдсэн аливаа этгээд компьютерын системийн хадгалсан, боловсруулсан, дамжуулсан мэдээлэлд нэвтэрсэн, эсвэл мэдээллийг олж авсаар байвал, эсвэл компьютерын системийг хэрэглэсэн, эсвэл санамсаргүйгээр компьютерын системийн хадгалсан, боловсруулсан, дамжуулсан мздээлэлд хохирол учруулсан бол 1-3 жил хоригдох, (5,200-10,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ. 4.Дээрх 1, 2-р заалтад заасан гэмт хэргийг үйлдэхээр завдсан бол тухайн заалтын дагуу хариуцлага хүлээнэ. 5. Дээрх 1-4 заалтад заасан гэмт хэргийг залилан мэхлэх, эсвэл хохирол учруулах зорилгоор үйлдэхэд оролцсон, гүйцэтгэсэн, зуучилсан аливаа этгээд 6 сараас 3 жил хүртэл хугацаагаар хорих, (5,200-20,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ. 6.Дээрх 1-5 заалтад заасан гэмт хэргийг үйлдэхэд зохион байгуулсан, эсвэл хатгасан аливаа этгээд 6 сараас 5 жил хүртэл хугацаагаар хорих, (5,200-40,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ. 7.Дээрх 1-3 заалтад заасан гэмт хэргийн үр дүнд олж авсан мэдээлэл болохыг мэдэж байсан, хадгалсан, бусад этгээдэд задалсан буюу нээлттэй болгосон, тухайн мэдээллийг ашигласан бол б сараас 3 жил хүртэл хугацаагаар хорих, (5,200-20,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ.
3	**Бразил**	2000 оны 7 сарын 14-ны өдөр №9,983 дугаарын хууль дараахь зүйл заалтыг баталжээ: Мэдээллийн системд хуурамч мэдээлэл оруулах

		Зүйл 313-А. Өөртөө буюу бусад этгээдэд давуу байдал бий болгох, эсвэл хохирол учруулахаар мэдээллийн системийн болон Олон нийтийн мэдээллийн сангийн зөв мэдээллийг өөрчлөх, ашиглагдахгүй болгох зорилгоор хуурамч мэдээлэл оруулах, хуурамч мэдээлэл оруулахыг зөвшөөрөл бүхий албан тушаалтан хялбар болгох үйлдлийг хэлнэ. Ял: **2-12** жил хорих, торгох ял шийтгэнэ. Мэдээллийн системд зөвшөөрөлгүй өөрчлөлт, сайжруулалт хийх Зүйл 313-Б. Албан тушаалтан зөвшөөрөлгүйгээр мэдээллийн систем буюу компьютерын программд өөрчлөлт, сайжруулалт хийсэн үйлдлийг хэлнэ. Ял: 3 сараас 2 жил хүртэл хугацаагаар баривчлах, торгох ял шийтгэнэ.
4	**Канад**	Канадын Эрүүгийн хууль 342.1 хэсэг: (1) Аливаа этгээд хууль бусаар, ямар ч эрхгүйгээр a/ шууд болон шууд бусаар ямарваа нэгэн компьютерын үйлчилгээг b/ электрон-соронзон, дуу авианы, механик болон бусад тоног төхөөрөмж ашиглан, шууд болон шууд бусаар дундаас нь барьж авах, эсвэл дундаас барьж авахад хүргэж байгаа компьютерын системийн аливаа үйлдэл хийсэн ɑa болон б хэсэгт заасан гэмт хэргийг үйлдэхэдкомпьютерын системийг шууд болон шууд бусаар ашигласан, эсвэл ашиглахад хүргэж байгаа үйлдэл хийсэн буюу мэдээлэл, компьютерын системтэй холбоотой гэмт хэргийг үйлдсэн d/a, б, с хэсэгт заасан гэмт хэргийг үйлдэхийн тулд бусад этгээдэд компьютерын нууц үгийг хэрэглэх, эзэмших, мөрдөн олоход тусалсан бол гэмт хэрэг үйлдсэн гэм буруутай этгээдэд тооцож, 10 жилээс хэтрэхгүй хугацаагаар хорих, эсвэл шүүгчийн захирамжаар хариуцлага тооцно.
5	**Чили**	Чили улс 1993 оны 6 сарын 7-нд Автомат мэдээллийг боловсруулсан гэмт хэргийн тухай №19.223 хуулийг хэвлэн нийтэлсэн байна. (Law on Automated Data Processing Crimes no. 19.223) Зүйл 2. Мэдээлэл боловсруулах системд хууль бусаар нэвтэрсэн, эсвэл мэдээлэл боловсруулах системийн мэдээллийг хууль бусаар ашигласан, эсвэл мэдээллийг дамжуулалт дундаас барьж авсан бол ялын бага болон дунд түвшний хэмжээгээр ял шийтгэнэ.
6	**БНХАУ**	1994 оны 2 сарын 18-ны өдрийн БНХАУ-ын Төрийн зөвлөлийн №147 тогтоол. Компьютерын мэдээллийн аюулгүй байдлыг хангах тухай БНХАУ-ын зохицуулалт Бүлэг 4. Хуулийн хариуцлага Зүйл 23'. Олон нийтийн хамгаалалтын байгууллага компьютерын вирус суулгасан, компьютерын мэдээллийн системд аюултай бусад мэдээлэл суулгасан, зөвшөөрөлгүйгээр компьютерын мэдээллийн системийн тусгай хамгаалалтын бүтээгдэхүүнийг худалдсан бол сануулга өгөх, эсвэл хувь хүнд 5,000 хүртэл юан, байгууллагад 15,000 хүртэл юаны торгууль оногдуулна. Хэрэв хууль бус ашиг олсон бол тухайн орлогыг улсын орлого болгож, хууль бус орлогыг 3 дахин нэмэгдүүлсэн хэмжээгээр торгоно. Мөн 1997 оны 12 сарын 11-нд Төрийн Зөвлөл баталж, 1997 оны 12 сарын 30-нд хэвлэн нийтэлсэн Компьютерын мэдээллийн сүлжээ, Интернэт хамгаалалт, Удирдлагын зохицуулалтын тухай тогтоолд хариуцлагыг давхар тусгажээ.

7	**Чехийн Бүгд Найрамдах улс**	Тусгайлсан эрх зүйн зохицуулалт байхгүй боловч Эрүүгийн хуульд зүйлчилж болох заалтууд байна: 182 зүйл. Олон нийтийн хэрэглээний үйлчилгээний нэгжид хохирол учруулах, аюултай байдалд оруулах 249 зүйл. Бусад хүмүүсийн хууль ёсны баримт бичгийг зөвшөөрөлгүй ашиглах 257 зүйл. Мэдээллийн сан дахь мэдээлэлд хохирол учруулах, бууруугаар ашиглах
8	**Дани**	Эрүүгийн хуулийн 2 63 зүйл: a/ Хууль бусаар бусад этгээдийн мэдээлэл боловсруулах системд ашигладаг мэдээлэл буюу программд нэвтэрсэн бол торгох, 6 сар хүртэл хугацаагаар хорих ял шийтгэнэ. b/ Заалт 1, 2-т заасан гэмт хэргийг бусад этгээдийг хянах, эсвэл компанийн худалдааны нууцыг агуулсан мэдээллийг олох зорилгоор, эсвэл бусад хүндрүүлэх нөхцөлийг агуулсан үйлдэл хийсэн бол 2 жил хүртэл хугацаагаар хорих ял шийтгэнэ.
10	**Финлянд**	Эрүүгийн хуулийн Бүлэг 38 Хэсэг 8: Мэдээллийг хортойгоор ашиглах. Бусдын , хувийн мэдээллийг ашиглан, хамгаалалтын системийг эвдэлж, электрон болон бусад хэлбэрээр мэдээллийг боловсруулж, хадгалж, дамжуулж байгаа компьютерын системийг эвдлэн орсон, эсвэл тухайн системийн тодорхой хэсгийг эвдлэн орсон бол торгох, 1 уил хүртэл хугацаагаар хорих ял шийтгэнэ. Тусгай тоног төхөөрөмж ашиглан, компьютерын систем, эсвэл тухайн системийн тодорхой хэсгийг эвдлэлгүй нэвтэрч, тухайн компьютерын системд хадгалагдах мэдээллийг авсан бол ял шийтгэнэ. Завдсан тохиолдолд мөн ял шийтгэнэ.
11	**Франц**	Шинэ Эрүүгийн хууль 1993 оны 3 сарын 1-нд хүчин төгөлдөр болжээ. Бүлэг 3. Автомат мэдээлэл боловсруулах систем үрүү дайрах 323-1 зүйл. Хууль бусаар автомат мэдээлэл боловсруулах системд нэвтэрсэн, эсвэл тодорхой хэсэгт хэвтэрсэн бол 1 жил хүртэл хугацаагаар хорих, 100,000 хүртэл торгох ял шийтгэнэ. Гэмт хэрэг үйлдсэний улмаас системийн мэдээллийг устгасан, өөрчилсөн, эсвэл системийн үйлдэл хийх ажиллагаа өөрчлөгдсөн бол 2 жил хүртэл хугацаагаар хорих, 200,000 хүртэл торгох ял шийтгэнэ. 323-2 зүйл. Системийн үйлдэл хийх ажиллагаанд саад болсон, эсвэл гажуудуулсан бол 3 жил хүртэл хугацаагаар хорих, 300,000 хүртэл торгох ял шийтгэнэ. 323-3 зүйл. Залилан мэхлэх зорилгоор автоматмэдээлэл боловсруулах системд суулгасан, эсвэл автомат мэдээлэл боловсруулах системийн мэдээллийг өөрчилсөн бол 3 жил хүртэл хугацаагаар хорих, 300,000 хүртэл торгох ял шийтгэнэ. 323-4 зүйл. Зохион байгуулагдсан бүлэгт оролцсон, урьдчилан үгсэж тохиролцсон бүлэг 323-1-ээс 323-3 хүртэл заалтад заасан гэмт хэргийг үйлдсэн бол онц ноцтой гэмт хэрэг үйлдсэнд тооцно.
12	**ХБНГУ**	Эрүүгийн хууль Хэсэг 202a. Мэдээллийн тагнуул 1. Зөвшөөрөлгүйгээр өөрийн буюу бусдын төлөө өөрт байхгүй, зөвшөөрөлгүй нэвтрэхээс тусгайлан хамгаалагдсан мэдээлэлд нэвтэрсэн бол 3 жил хүртэл

		хугацаагаар хорих, торгох ял шийтгэнэ. 2. 1 заалтад заасан мэдээлэлд нүдээр шууд үзэх боломжгүй электрон буюу соронзон хэлбэрээр хадгалагдаж, дамжуулагдаж байгаа мэдээллийг хамруулна. Эрүүгийн хууль Хэсэг 303а. Мэдээллийг өөрчлөх 1.Хууль бусаар мэдээллийг арилгасан, өөрчилсөн, дахин ашиглахгүй болгосон бол 2 жил хүртэл хугацаагаар хорих, торгох ял шийтгэнэ. 2.Завдсан тохиолдолд мөн ял шийтгэнэ. Эрүүгийн хуулийн Хэсэг 303 b. Компьютерын хортой үйл ажиллагаа 1. Бусад этгээдийн бизнес, аж ахуй, захиргааны үйл ажиллагаанд чухал шаардлагатай мэдээлэл боловсруулах үйл ажиллагаанд саад хийсэн бол 5 жил хүртэл хугацаагаар хорих, торгох ял шийтгэнэ: - 300а/1/ хэсэгт заасан гэмт хэрэг үйлдсэн - компьютерын систем буюу мэдээлэл зөөвөрлөгчийг устгасан, хохирол учруулсан, дахин ашиглагдахгүй болгосон, өөрчилсөн 2.Завдсан тохиолдолд мөн ял шийтгэнэ.
13	**Грек**	Эрүүгийн хуулийн 370с2 зүйл: Хууль ёсны эзэмшигчийн хамгаалалт, хязгаарлалтыг эвдлэн, компьютер буюу компьютерын санах ойд хадгалагдсан болон холбоо харилцаагаар дамжуулагдаж ' буй мэдээллийг хууль бусаар олж авсан бол 3 сар хүртэл хугацаагаар хорих, 10,000 драхма хүртэл торгох ял шийтгэнэ. Хэрэв тухайн үйлдэл нь олон улсын асуудал болон Улсын аюулгүй байдалтай холбоотой бол 148 зүйлээр ял шийтгэнэ. Хэрэв гэмт хэргийг мэдээллийг хууль ёсоор эзэмшигчийн туслалцаатай хийсэн бол дээр дурьдсан заалтыг баримтлан, ял шийтгэнэ.
14	**Унгар**	Эрүүгийн хуулийн 300с зүйл: Компьютерын залилан мэхлэлт. 1. Хууль бусаар өөртөө ашиг олохоор хохирол учруулсан, электрон мэдээлэл боловсруулах замаар саад хийсэн, программыг өөрчилсөн, мэдээллийг устгасан, хуурамч буюу бүрэн бус мэдээлэл оруулсан, бусад гэмт хэрэг үйлдэх зорилгоор хууль бус үйлдэл хийсэн бол 3 жил хүртэл хорих ял шийтгэнэ. 2.Хэрэв: а/ их хэмжээний хохирол учирсан бол 5 жил хүртэл хугацаагаар хорих б/ онц их хэмжээний хохирол учирсан бол 2 жилээс 8 жил хүртэл хугацаагаар хорих ял шийтгэнэ. 3. Нийтийн, хөдөлгөөнт гар утасны -электрон карт ашиглаж, гэмт хэрэг үйлдсэн, эсвэл хөдөлгөөнт гар утасны микропрограммыг өөрчилж, мэдээлэлд холбогдсон бол залилан мэхлэлтэд тооцогдоно.
15	**Ирланд**	Эрүүгийн хууль 1991 Хэсэг 5: 1. Хууль бусаар компьютер ашиглаж,

		а/ Мужийн дотроос Мужийн гадна, дотно хадгалагдах аливаа мэдээлэлд нэвтэрсэн б/Мужийн гаднаас Мужийн дотор хадгалагдах аливаа мэдээлэлд нэвтэрсэн бол 500 хүртэл торгох, 3 **сар** хүртэл хугацаагаар хорих ял дангаар буюу хамт шийтгэнэ. 2. 1 заалт хууль бусаар тодорхой мэдээлэлд нэвтэрсэн, тодорхой мэдээллийн төрөлд нэвтэрсэн, тодорхой этгээдэд хадгалагдах мэдээлэлд нэвтэрсэн бүх этгээдэд хамаарна.
17	**Энэтхэг**	Мэдээллийн технологийн тухай хууль 2000 (2000 оны №20) Бүлэг 11. Компьютерын систем дахь хакерын ажиллагаа (1) Санаатайгаар, эсвэл тухайн үйлдэл хор хохирол авчрахыг мэдсээр байж, олон нийт, хувь хүний компьютерын эх сурвалж дээрхи мэдээллийг устгах, арилгах, өөрчлөх, эсвэл мэдээллийн үнэт байдлыг алдуулах, дахин ашиглахгүй болгосон үйлдлийг хакерын ажиллагаанд тооцно. (2) Хакерын ажиллагаа хийсэн бол 3 жил хүртэл хугацаагаар хорих, 200,000 рупигээр торгох йл дангаар буюу хамт шийтгэнэ.
18	**Израиль**	1995 оны Компьютерын тухай хууль 4 хэсэг: Хууль бусаар компьютерын мэдээлэлд нэвтэрсэн бол 3 жил хүртэл хугацаагаар хорих ял шийтгэнэ. Мэдээлэлд нэвтрэх гэдэг нь компьютерт холбогдох хэрэгсэл ашигласан, хэрэгслийн тусламжтай нэвтэрсэн, хууль бусаар нууцаар нэвтэрсэн үйлдлийг ойлгоно.
19	**Итали**	Эрүүгийн хуулийн 615зүйл: Компьютерын болон холбоо харилцааны системд хууль бусаар нэвтрэх. Хамгаалалтын хэрэгслээр хамгаалагдсан компьютерын болон холбоо харилцааны системд хууль бусаар нэвтэрсэн, эсвэл хамгаалалтын албаны ажилтны мэдэгдлийн үл зөвшөөрч, холбогдсон бол 3 жил хүртэл хугацаагаар ял шийтгэнэ. Хэрэв: 1/ Албан тушаалаа урвуулан ашиглаж гэмт хэрэг үйлдсэн бол 2/ Зэвсэглэсэн этгээд хүч хэрэглэн байж, гэмт хэрэг үйлдсэн бол 3/ Системд, мэдээлэлд, мэдээллийт хадгалах программд хохирол учруулсан бол 1 жилээс 5 жил хүртэл хугацаагаар хорих ял шийтгэнэ. Хэрэв компьютерын болон холбоо харилцааны системд хууль бусаар нэвтрэхэд зэвсэгт хүчний ашиг сонирхолд тулгуурлан, олон нийтийн аюулгүй байдалд сөргөөр нөлөөлөх байдал үүссэн бол 1 жилээс 5 жил хүртэл, эсвэл 3 жилээс 8 жил хүртэл ял шийтгэнэ. 615 зүйл. Компьютерын болон холбоо харилцааны системд нэвтрэх кодыг хууль бусаар эзэмших, тараах Өөртөө буюу бусдад ашиг олох, бусдад хохирол учруулах зорилгоор хамгаалалтын хэрэгслээр хамгаалагдсан компьютерын болон холбоо харилцааны системд нэвтрэх код, түлхүүр үгийг эзэмших, хуулбарлах, бусдад дамжуулсан бол 1 жил хүртэл хугацаагаар хорих, 10 сая лир хүртэл хэмжээгээр торгох ял шийтгэнэ.

		Хэрэв энэ гэмт хэргийг 617 зүйлд заасан гэмт хэргийн хамт үйлдсэн бол 1 жилээс 2 жил хүртэл хугацаагаар хорих, 10 саяас 20 сая лир хүртэл хэмжээгээр торгох ял шийтгэнэ. 615. Компьютерын системд хохирол учруулах, зогсоох зорилготой программыг тараах. Өөрөө буюу бусдын хийсэн, компьютерын болон холбоо харилцааны системд, системийн мэдээлэл, программыг хэсэгчлэн буюу бүрэн зогсоох, өөрчлөх зорилготой программыг тараасан, дамжуулсан бол 2 жил хүртэл хугацаагаар хорих, 20 сая лир хүртэл хэмжээгээр торгох ял шийтгэнэ.
20	**Япон**	Зөвшөөрөлгүй компьютерт нэвтрэх тухай хууль (Unauthorized Computer Access Law) 1999 оны №128 хууль (2000 оны 2 сарын 3-нд хүчин төгөлдөр болсон) (Зөвшөөрөлгүй компьютерт нэвтрэх үйлдлийг хориглох) Зүйл 3. Зөвшөөрөлгүй компьютерт нэвтрэхийг хориглоно. Зөвшөөрөлгүй компьютерт нэвтрэх гэдэгт дараахь үйлдлийг хамааруулна: 1 тусгай компьютер, харилцаа холбооны шугам, бусад этгээдийн кодыг ашиглан, нэвтрэх хяналтын үйлдлийг хариуцсан компьютерт холбогдож, нэвтрэх хяналтын үйлдлээр хязгаарлагдсан хэрэглээг ашиглах боломжтой болгох үйлдэл, 2 нэвтрэх хяналтын үйлдлийн хязгаарлалтыг бууруулах, хязгаарлагдсан хэрэглээг нэвтрэх хяналтын үйлдэлд мэдэгдэхгүй ашигласан үйлдэл, 3 нэвтрэх хяналтын үйлдэл бүхий компьютерт холбогдсон тусгай компьютер, харилцаа холбооны шугамаар дамжуулан, нэвтрэх хяналтын үйлдлийг суулгаж, хязгаарлалтаас зайлсхийж, мэдээлэл, коммандыг боловсруулах үйлдэл (Зовшөөрөлгүй компьютерт НЭВтрэхийг хялбар болгох үйлдлийг хориглох) Зүйл 4. Бусад этгээдэд нэвтрэх боломж олгох хувийн мэдээлэл, тусгай компьютерыг ашиглах хувийн мэдээллийг дамжуулах, ашиглахыг хориглоно. (Эрүүгийн хариуцлага) Зүйл 8. Хэрэв дээр дурьдсан гэмт хэргийг үйлдсэн бол 1 жил хүртэл хугацаагаар хорих, 500,000 иен хүртэл хэмжээгээр торгох ял шийтгэнэ. (1) Зүйл 3-н 1 параграф, Зүйл 4 заасан гэмт хэрэг үйлдсэн бол 300,000 иен хүртэл хэмжээгээр торгох ял шийтгэнэ.
21	**Голланд**	Эрүүгийн хуулийн 138а зүйл: Санаатайгаар, хууль бусаар мэдээлэл хадгалах, боловсруулах автоматжуулсан систем, түүний тодорхой хэсэгт нэвтэрсэн бол компьютерын амгалан тайван байдлыг алдагдуулсан гэмт буруутайд тооцож, 6 сар хүртэл хугацаагаар хорих, 10,000 гилдер хүртэл торгох ял шийтгэнэ. (a) Хамгаалалтын системийг эвдэлсэн бол (b) хуурамч дохио, түлхүүрийн тусламжтайгаар, хуурамчаар чадвартай мэт үйлдэл хийн, техникийн байдлаар саад хийж, нэвтэрсэн бол эрүүгийн хариуцлага хүлээлгэнэ.
23	**Швед**	Эрүүгийн хуулийн Бүлэг 4, Хэсэг 9с: Хэсэг 8, 9 зааснаас бусад тохиолдолд, хууль бусаар автоматжуулсан мэдээлэл боловсруулах ажиллагааны тэмдэглэлд нэвтэрсэн, эсвэл хууль бусаар тэмдэглэлийг өөрчилсөн, устгасан, эсвэл өөрчилсөн, устгасан тэмдэглэлийг бүртгэлд оруулсан бол 2 жил хүртэл хорих, торгох ял шийтгэнэ. Тэмдэглэлд электроник болон автоматжуулсан мэдээлэл боловсруулах ажиллагаанд хэрэглэгдэх бусад мэдээллийг ойлгоно.

		Завдсан болон бэлдсэн тохиолдолд Эрүүгийн хуулийн Бүлэг 23 заасны дагуу хариуцлага тооцох бөгөөд төгссөн гэмт хэргээс бага шийтгэл онооно.
24	**Швейцарь**	Эрүүгийн хуулийн 14 3 зүйл: Мэдээлэл боловсруулах системд хууль бусаар нэвтрэх Зөвшөөрөлгүйгээр, ашиг олох зорилгагүйгээр электрон тоног төхөөрөмжийн тусламжтайгаар зөвшөөрөлгүй нэвтрэхээс тусгайлан хамгаалагдсан мэдээлэл боловсруулах сйстемд нэвтэрсэн бол торгох, хорих ял шийтгэнэ.
	Латви	Эрүүгийн хуулийн 241 хэсэг: Компьютерын сйстемд дураар нэвтрэх (1) Компьютерын системд дураар нэвтэрч, мэдээлэл авах боломж бүрдүүлсэн бол хорих, сарын орлогыг 80 дахин нэмэгдүүлсэнтэй тэнцэх хэмжээнд хүртэл торгох ял шийтгэнэ. Компьютерын системд дураар нэвтэрч, хамгаалалтын программ хангамжийг эвдсэн, эсвэл харилцаа холбооны шугаманд нэвтэрсэн бол 1 жил хүртэл хугацаагаар хорих, сарын хамгийн бага орлогыг 150 дахин, нэмэгдүүлсэнтэй тэнцэх хэмжээнд хүртэл торгох ял шийтгэнэ.
25	**Нэгдсэн вант улс**	Компьютерыг буруугаар ашиглах тухай хууль 1990 Бүлэг 18. Компьютерын материалд хууль бусаар нэвтрэх (1) Хэрэв дараахь гэмт хэргийг үйлдсэн бол гэм буруутайд тооцно: a/ аливаа мэдээлэл, программ хадгалах компьютерт нэвтрэх боломжийг хамгаалах зорилгоор компьютерээр төрөл бүрийн үйлдэл хийсэн b/ хамгаалж буй нэвтрэх боломж нь зөвшөөрөлгүй c/ үйлдэл хийж байхдаа тухайн үйлдлээ бүрэн ухамсарласан (2) Гэмт хэрэг үйлдэхдээ дараахь зорилгыг агуулсан байх шаардлагагүй: a/ тодорхой программ, мэдээллийг олохын тулд b/ тодорхой төрлийн программ, мэдээллийн олохын тулд c/ тодорхой компьютерын программ, мэдээллийг олохын тулд (3) Дээр дурьдсан гэмт хэрэг үйлдсэн бол 6 сар хүртэл хугацаагаар хорих, стандарт хэмжээний 5-р түвшин хүртэл хэмжээгээр торгох ял шийтгэнэ.

Интернэт ашиглах хууль бус үйлдлийг зохицуулахад компьютерт шууд холбогдсон болон шууд холбогдолгүй үйл ажиллагаа явуулах технологийн арга барилыг харгалзан үзэх шаардлагатай бөгөөд тухайн арга барилд нууц, иргэний эрх чөлөөний хамгаалалт зэрэг олон чухал нийгмийн сонирхол байгааг анхаарах хэрэгтэй.

Хуулийн байгууллагын хувьд мэдээлийн эх сурвалж, сургалт судалгааны ажил зайлшгүй шаардагдахаас гадна шинэ төрлийн мөрдөн шалгах багаж хэрэгсэл, чадварлаг боловсон хүчин, орон нутгийн нэгж бүрт ажиллах хэсэг, олон улсын нягт хамтын ажиллагаа шаардлагатай байна.

Хэрэглэгчдийн "кибер ёс зүй" хэмээх ойлголтыг төлөвшүүлэх, хууль бус үйлдлийн эрсдлийг бууруулах, хамгаалахад хэрэглэгчдийн мэдлэгийг дээшлүүлэх арга хэмжээ авах хэрэгтэй[33].

Хувийн нууц бол хууль ёсны эрх бөгөөд олон улс орон хуульдаа хүлээн зөвшөөрсөн байдаг боловч хууль зүйн болон соёл, уламжлалын ялгаанаас шалтгаалан, тодорхой онцлогтой. Ихэнх улс хувийн нууцыг хуулиар хамгаалж, олон улсын гэрээ, конвенцид стандарт зарчмыг тусгасан байдаг бол одоо кибер технологийн хүрээнд энэ асуудлыг маш тодорхой болгох шаардлага гарч байна.

АНУ-ын Дээд шүүхийн 1997 оны 0б дугаар сарын 02-06-ны өдрийн шийдвэрт: "Интернэт үсрэнгүй хөгжиж буй үзэгдэл цаашид үргэлжлэх болно. Нотлох баримтгүй буюу дутмаг байдлаас болж, үндсэн хуульт ёсонд хийдэл үүсэхээс сэргийлж, эрх зүйн зохицуулалтыг улам нарийвчлан боловсронгуй болгож, цаашид гарах сөрөг үзэгдлийн эсрэг бодитой арга хэмжээ авах хэрэгтэй болж байна. Ингэснээр бид бодит бус хэмээх хүмүүсийн сэтгэгдлийг өөрчилж, кибер орчинд ч зохицуулалт үйлчлэх боломжтой харуулах болно" гэжээ.

[33] http: //www.usdoj .gov/criminal/cybercrime/unlawful..htm

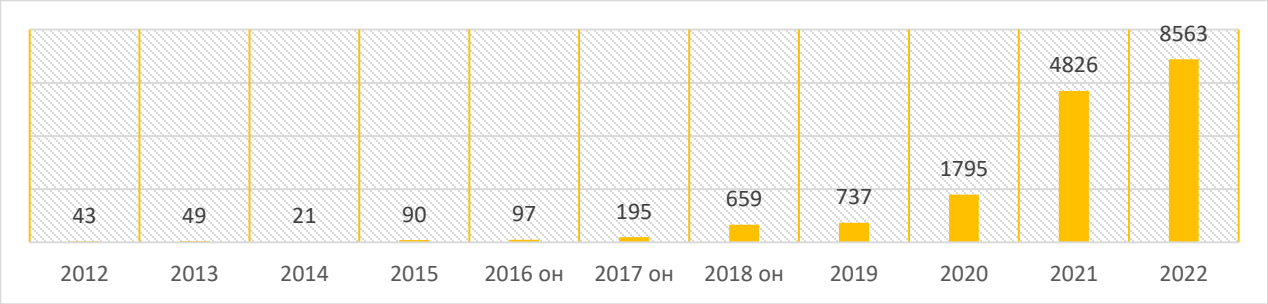
ХОЁРДУГААР БҮЛЭГ. КИБЕР ОРЧИНД ҮЙЛДЭГДСЭН ГЭМТ ХЭРЭГТ ХИЙСЭН ДҮН ШИНЖИЛГЭЭ

§2.1. Кибер орчинд үйлдэгдсэн гэмт хэргийн статистик мэдээлэлд хийсэн дүн шинжилгээ

Цагдаагийн байгууллагын гэмт хэргийн статистик мэдээгээр кибер орчинд үйлдэгдсэн гэмт хэрэг 2012 онд 43, 2013 онд 49, 2014 онд 21, 2015 онд 90, 2016 онд 97, 2017 онд 195, 2018 онд 659, 2019 онд 737, 2020 онд 1795, 2021 онд 4826, 2022 онд 8563 бүртгэгдэж, жил бүр 1-2 дахин өссөн байна[34].

Кибер орчинд үйлдэгдсэн гэмт хэрэг цагдаагийн байгууллагын хэмжээнд 2022 онд нийт 8563 бүртгэгдсэний 6865 буюу 80.2 хувь нь Улаанбаатар хотод, 1695 буюу 19.6 хувь нь орон нутагт, 3 буюу 0.04 хувь нь бусад газар /хилийн чанадад үйлдэгдсэн/ бүртгэгдсэн байна.

График 1. Кибер орчинд үйлдэгдсэн гэмт хэргийн тоон үзүүлэлт



"Кибер орчинд үйлдэгдсэн" гэмт хэрэг цагдаагийн байгууллагын хэмжээнд 2022 онд нийт 8563 бүртгэгдсэний 6865 буюу 80.2 хувь нь Улаанбаатар хотод, 1695 буюу 19.6 хувь нь орон нутагт, 3 буюу 0.04 хувь нь бусад газар /хилийн чанадад үйлдэгдсэн/ бүртгэгдсэн байна.

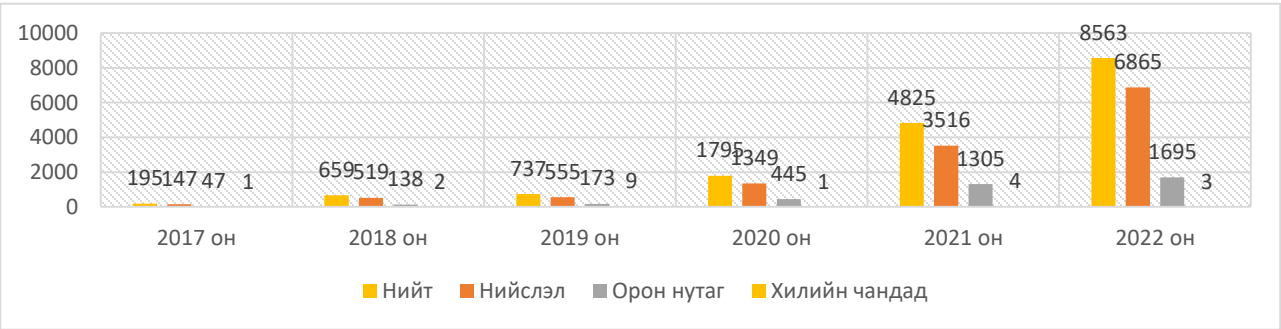


График 2. Кибер орчинд үйлдэгдсэн гэмт хэргийн бүртгэгдсэн газар, оноор

[34] Цагдаагийн ерөнхий газрын Мэдээлэл, дүн шинжилгээ, шуурхай удирдлагын албаны мэдээлэл.

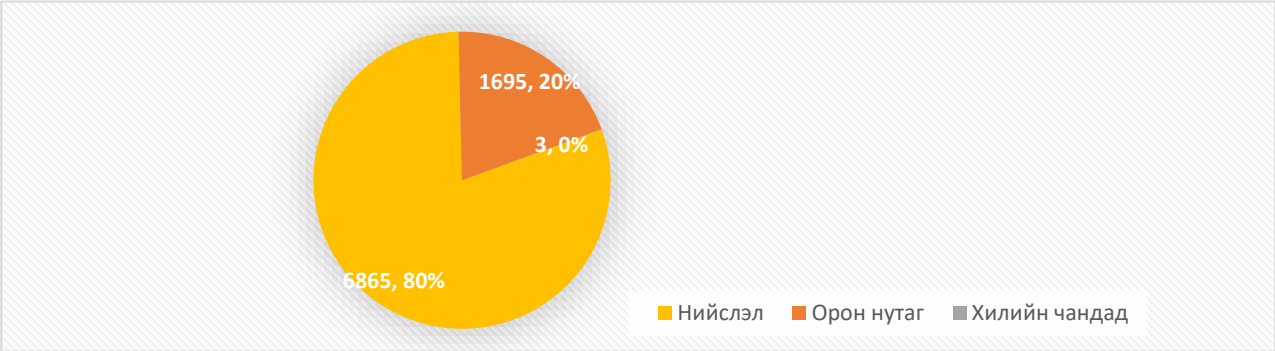


График 3. Кибер орчинд үйлдэгдсэн гэмт хэргийн бүртгэгдсэн газар, нийслэл, орон нутаг, гадаадад

Нийслэлд бүртгэгдсэн 2695 гэмт хэргийн 1042 буюу 38.7% нь Баянзүрх дүүрэгт, 405 буюу 15.0% нь Сүхбаатар дүүрэгт, 343 буюу 12.7% нь Баянгол дүүргийн нутаг дэвсгэрт үйлдэгдсэн байна.

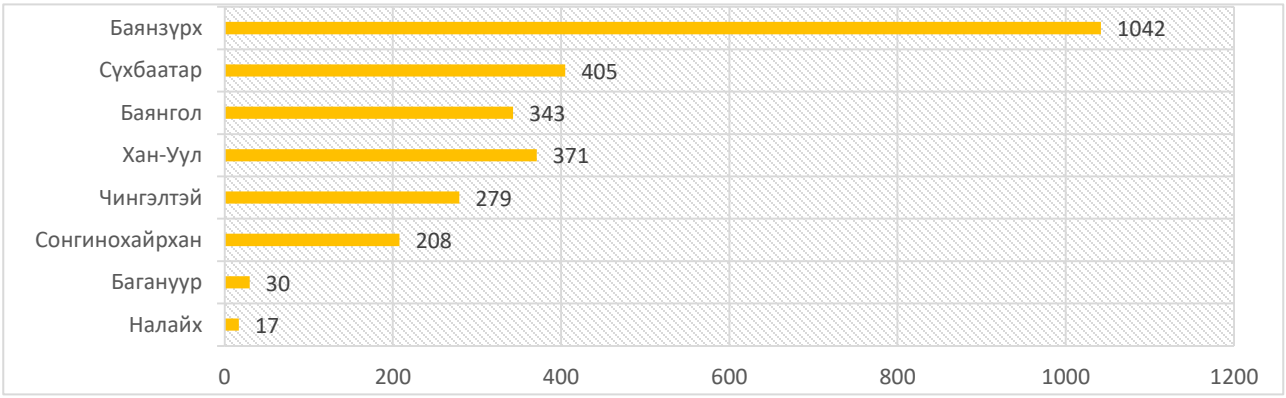


График 4. Нийслэлд бүртгэгдсэн гэмт хэрэг дүүргээр /2017-2022 он/

Орон нутгийн хэмжээнд бүртгэгдсэн гэмт хэргийн 123 буюу 14.8% нь Дархан-Уул, 93 буюу 11.2% нь Орхон, 64 буюу 7.7% нь Өмнөговь аймагт тус тус бүртгэгдсэн нь бусад аймгуудаас өндөр байна.

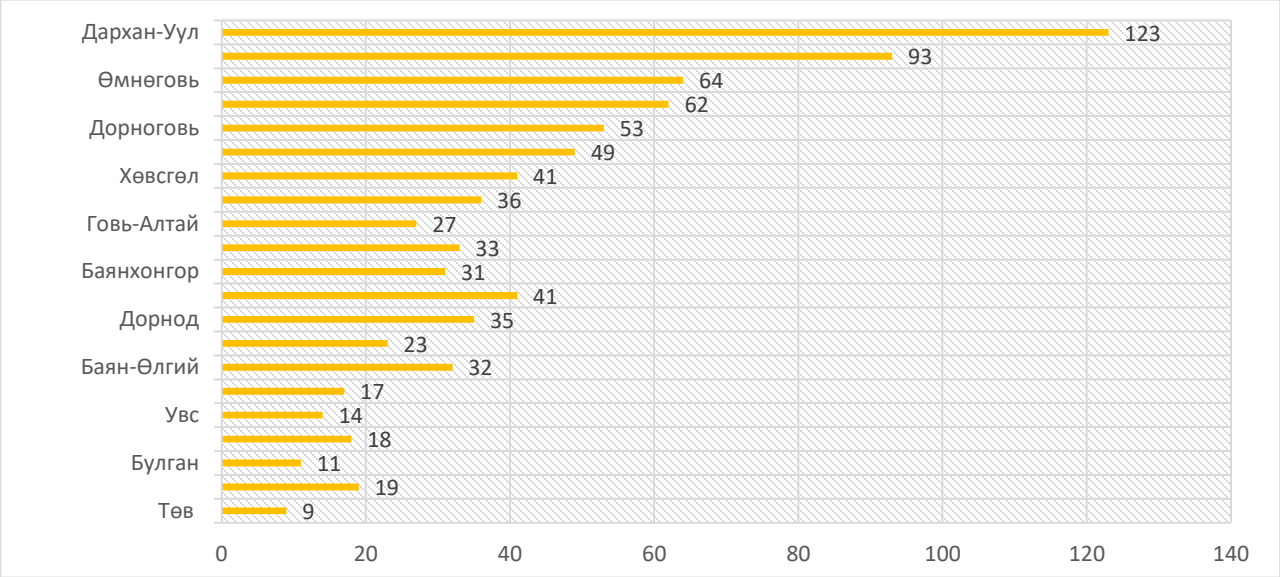


График 5. Орон нутагт бүртгэгдсэн гэмт хэрэг аймгаар /2017-2022 он/

Бүртгэгдсэн гэмт хэргийн зүйл заалтаар нь авч үзвэл, нийт 34 төрлийн гэмт хэрэг кибер орчинд үйлдэгдсэн байх бөгөөд нийт Кибер орчинд үйлдэгдсэн гэмт хэргийн 7708 буюу 90% нь залилах, 256 буюу 3% нь Кибер орчинд хууль бусаар халдах, 124 буюу 1.4% нь худал мэдээлэл тараах төрлийн гэмт хэрэг тус тус эзэлж байна.

Энэ хугацаанд бүртгэгдсэн гэмт хэргийн дийлэнх хувийг эзэлж буй залилах төрлийн гэмт хэрэг нь 2015 онд 17, 2016 онд 69, 2017 онд 136, 2018 онд 590, 2019 онд 641, 2020 онд 1281, 2021 онд 3858, 2022 онд 7708 тус тус бүртгэгдсэн байна.

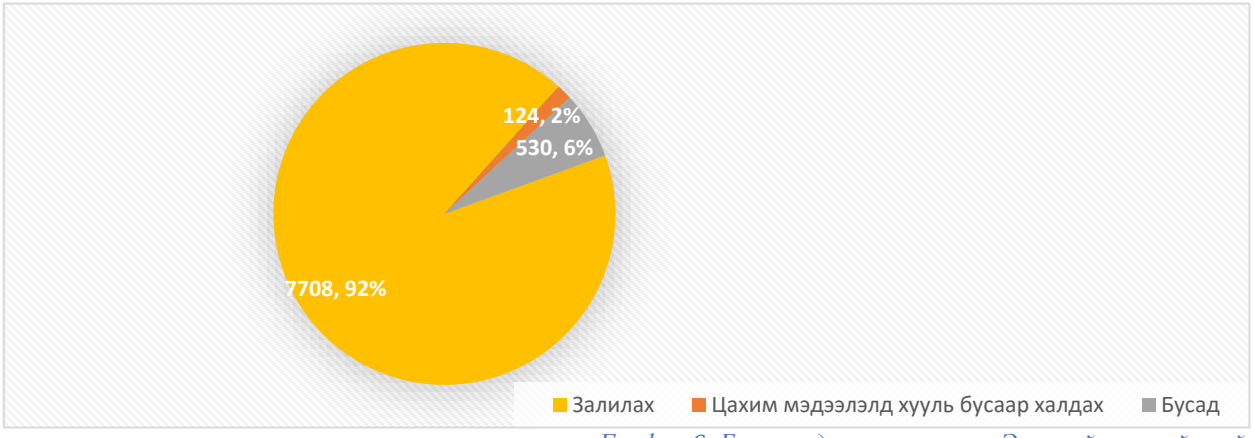


График 6. Бүртгэгдсэн гэмт хэрэг Эрүүгийн хуулийн зүйлээр

Хүснэгт 2. Бүртгэгдсэн гэмт хэрэг Эрүүгийн хуулийн зүйл, ангиар.

Д/Д	ТӨРӨЛ	2017	2018	2019	2020	2021	2022

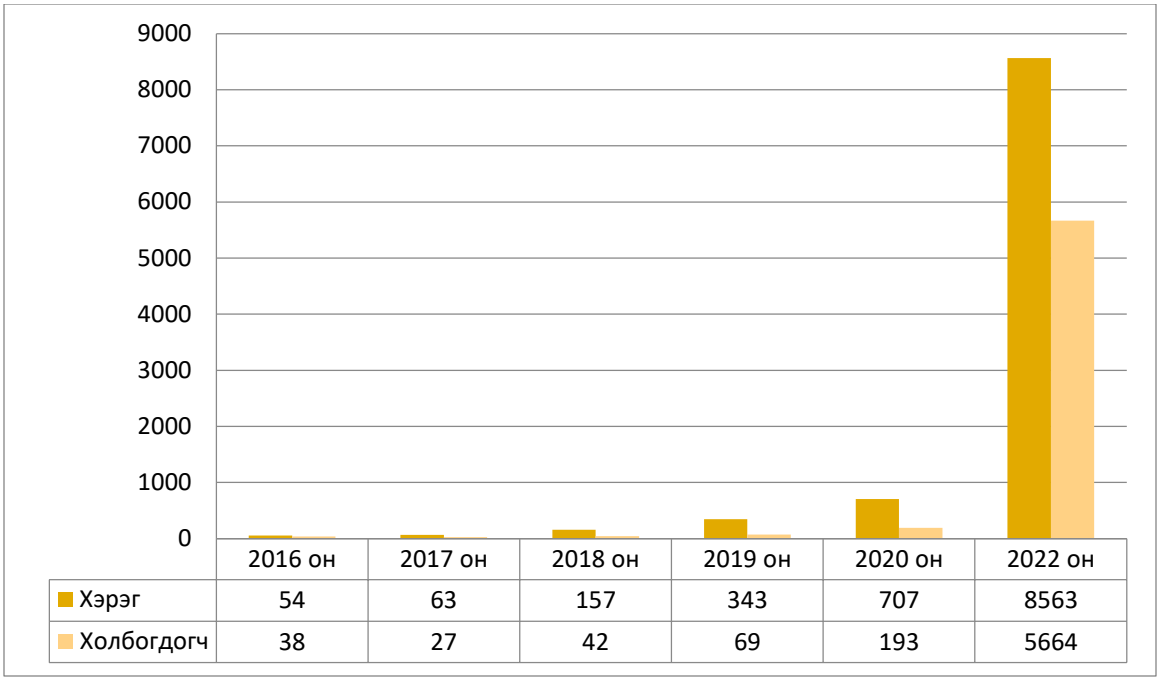
		ОН	ОН	ОН	ОН	ОН	ОН
1	Залилах	136	590	641	1281	3858	7708
2	Кибер орчинд хууль бусаар халдах	39	43	53	145	150	256
3	Гүтгэх	11					
4	Доромжлох	4					
5	Хувь хүний нууцад халдах		14	7	8	1	2
6	Компьютерын мэдээллийг хууль бусаар олж авах	3				1	
7	Хүүхдэд садар самууныг сурталчлах, уруу татах		5	7	4	2	37
8	Компьютерын мэдээлэл, программыг өөрчлөх, эвдэх, сүйтгэх	2					
9	Заналхийлэх			7	18	7	62
10	Хувь хүний нууцыг задруулах		5	1	2	1	2
11	Алдаатай гүйлгээ, андуурагдсан илгээмж, гээгдэл эд хөрөнгө, алдуул мал завших			4	17	21	41
12	Нянтай программ зохион бүтээх, ашиглах, тараах						
13	Зохиогчийн эрх болон түүнд хамаарах эрхийг зөрчих		2	1	1	1	3
14	Мөнгө угаах			3	1	7	
15	Садар самууныг сурталчлах					2	37
16	Бусдын бие махбодод хөнгөн гэмтэл санаатай учруулах						
17	Хуурамч баримт бичиг үйлдэх, ашиглах			2	3	11	3
18	Хүчиндэх			2	6	5	8
19	Арван зургаан насанд хүрээгүй хүнтэй бэлгийн харьцаанд орох			2	5	2	1
20	Бусдын эд хөрөнгийг авахаар заналхийлэх			2	5		
21	Иргэний захидал харилцааны нууцын халдашгүй байдлыг зөрчих						
22	Компьютерын мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай хэрэгсэл бэлтгэх, борлуулах				2	1	
23	Биеэ үнэлэхэд бусдыг татан оруулах, биеэ үнэлэхийг зохион байгуулах						
24	Хадгалуулсан буюу бусад зорилгоор итгэмжлэн өгсөн бусдын эд хөрөнгө завших						

25	Бэлгийн мөлжлөг	1		1	1
26	Хүн худалдаалах	1			
27	Ялгаварлан гадуурхах	1			
28	Бэлгийн дур хүслээ ёс бусаар хангах	1			
29	Хууль бусаар даатгалын нөхөн төлбөр авах	1			
30	Худал мэдээлэл тараах		173	126	124
31	Хулгайлах		67	92	126
32	Мөрийтэй тоглоом зохион байгуулах		18	487	69
33	Хөрөнгө завших		13	12	29
34	Бусад		26	17	32

Гэмт хэрэг үйлдэгдсэн шалтгаанаар нь авч үзвэл, нийт бүртгэгдсэн гэмт хэргийн 72.7% нь ашиг олох, шунахайн сэдэлтээр, 19.7% нь итгэл эвдэх, 2.4% нь цахим мэдээллийн аюулгүй байдал, нууцлал хангалтгүй, 2.1% нь хяналт, шалгалт сул байгаатай холбоотой байна.

Энэ төрлийн гэмт хэрэгт сүүлийн 6 жилийн байдлаар нийт 419 хүнийг 1377 хэрэгт холбогдуулан шалгасны 2015 онд 50 хүнийг 53 хэрэгт, 2016 онд 38 хүнийг 54 хэрэгт, 2017 онд 27 хүнийг 63 хэрэгт, 2018 онд 42 хүнийг 157 хэрэгт, 2019 онд 69 хүнийг 343 хэрэгт, 2020 онд 193 хүнийг 707 хэрэгт тус тус холбогдуулан шалгасан байна.

2016 онд сэжигтнээр татсан хүнийг 2015 онтой харьцуулбал 24.0 хувиар, 2017 оны сэжигтнийг 2016 онтой харьцуулбал 28.9 хувиар тус тус буурч, 2018 онд тухайн хэрэгт холбогдогчдыг 2017 оныхтой харьцуулбал 55.6 хувиар, 2019 оны холбогдогчдыг 2018 онтой харьцуулбал 64.3 хувиар тус тус өсөж, 2020 оны холбогдогчдыг 2019 онтой харьцуулбал 43.7 хувиар буурсан байна.



	2016 он	2017 он	2018 он	2019 он	2020 он	2022 он
Хэрэг	54	63	157	343	707	8563
Холбогдогч	38	27	42	69	193	5664

График 7. Гэмт хэрэг, холбогдогчийн тоо /2016-2022 он/

Холбогдогчдыг хүйсээр нь авч үзвэл, 2015 онд холбогдсон хүний 32 буюу 64.0% нь эрэгтэй, 18 буюу 36.0% нь эмэгтэй, 2016 онд холбогдсон хүний 27 буюу 71.1% нь эрэгтэй, 11 буюу 28.9% нь эмэгтэй, 2017 онд холбогдсон хүний 22 буюу 81.5% нь эрэгтэй, 5 буюу 18.5% нь эмэгтэй, 2018 онд холбогдсон хүний 37 буюу 88.1% нь эрэгтэй, 5 буюу 11.9% нь эмэгтэй, 2019 онд холбогдсон хүний 57 буюу 82.6% нь эрэгтэй, 12 буюу 17.4% нь эмэгтэй, 2020 онд холбогдсон хүний 139 буюу 72.0% эрэгтэй, 54 буюу 28.0% эмэгтэй хүн байсан.

Харин 2022 оны байдлаар нийт 8563 Кибер орчинд үйлдэгдсэн гэмт хэрэгт 5664 хүн холбогдон шалгагдаж, тэдний 3798 буюу 67.1 хувь нь эрэгтэй, 1866 буюу 32.9 хувь нь эмэгтэй, 402 буюу 7.1 хувь нь 14-17 насны хүүхэд байна. Өмнөх оны мөн үетэй харьцуулбал холбогдон шалгагдсан хүн 2805 буюу 98.1 хувиар, эмэгтэй хүн 1152 буюу 2.6 дахин, хүүхэд 298 буюу 3.9 дахин тус тус өссөн.

Гэмт хэргийн улмаас 8438 хүн хохирсны 3224 буюу 38.2 хувь нь эрэгтэй, 5214 буюу 61.8 хувь нь эмэгтэй, 83 буюу 1.0 хувь нь 11-17 насны хүүхэд байна. Өмнөх оны мөн үетэй харьцуулбал нийт хохирогч 4103 буюу 94.6 хувь, эрэгтэй хүн 1639 буюу 2.0 дахин, эмэгтэй хүн 2464 буюу 89.6 хувь, хүүхэд 39 буюу 88.6 хувиар тус тус өссөн байна.

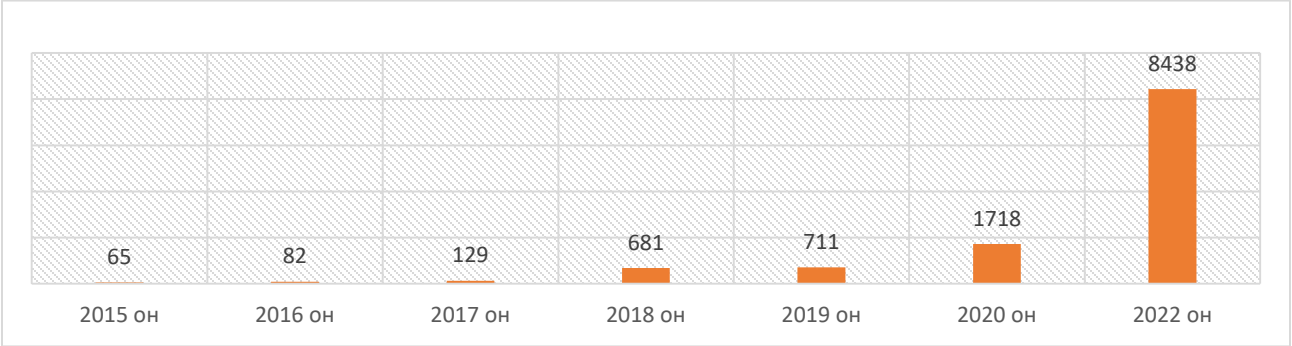
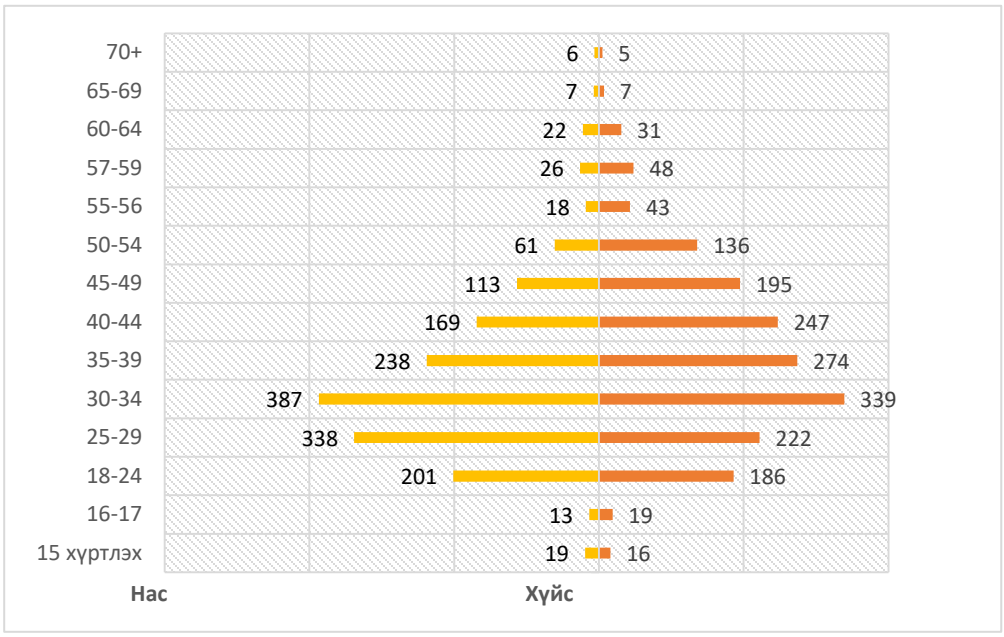


График 8. Кибер орчинд үйлдэгдсэн гэмт хэргийн хохирогч /2015-2022/

Насны ангиллаар нь авч үзвэл, нийт хохирогчдын 726 буюу 21.4% нь 30-34 насны, 560 буюу 16.5% нь 25-29 насны, 513 буюу 15.1% нь 35-39 насны иргэд эзэлж байна.

График 9. Хохирогчдын насны ангилал, хүйс /2017-2022/



Иргэн, хуулийн этгээдэд учирсан 32662.6 сая төгрөгийн хохирлын 10413.8 сая төгрөг буюу 31.9 хувийг нөхөн төлүүлж, 275.6 сая төгрөгийн хөрөнгө битүүмжилсэн нь өмнөх оны мөн үеэс хохирлын хэмжээ 14153.9 сая төгрөг буюу 76.5 хувиар, битүүмжилсэн хөрөнгө 241.3 сая төгрөг буюу 8.0 дахин, нөхөн төлүүлсэн хохирол 1185.0 сая төгрөг буюу 12.8 хувиар тус тус өссөн байна.

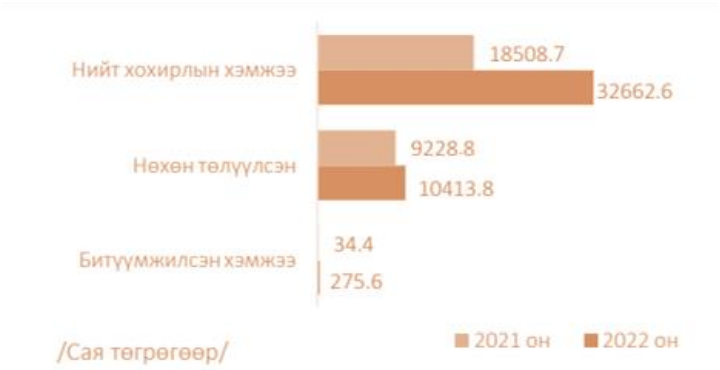


График 10. Кибер орчинд үйлдэгдсэн гэмт хэргийн улмаас учирсан хохирол /сая төгрөгөөр/

Кибер орчинд үйлдэгдсэн хүүхэд хохирсон гэмт хэргийн нөхцөл байдал:

Кибер орчинд бүртгэгддэг гэмт хэргийн 1.9% нь хүүхэд хохирсон гэмт хэрэг байдаг. Кибер орчинд хүүхэд хохирсон гэмт хэргийг бүртгэгдсэн оноор нь авч үзвэл, 2015 онд 2, 2016 онд 1, 2017 онд 1, 2018 онд 12, 2019 онд 27, 2020 онд 24, 2022 онд 84 бүртгэгджээ.

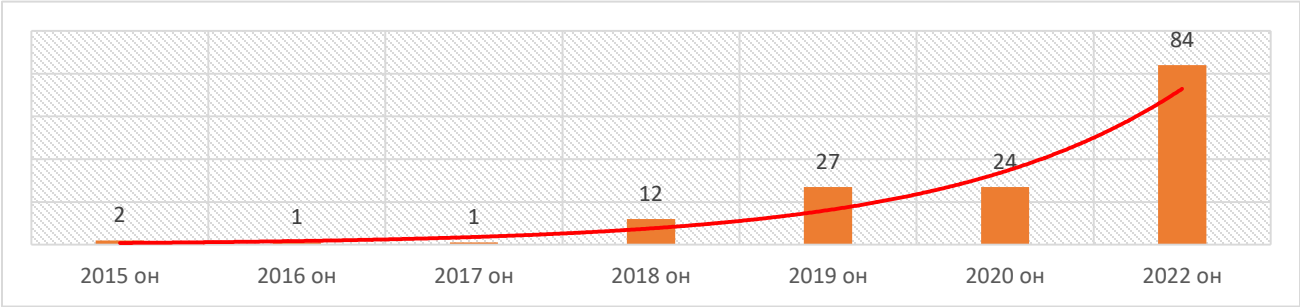


График 11. Кибер орчинд хүүхэд хохирсон гэмт хэрэг

Хэрэг үйлдэгдсэн газраар нь авч үзвэл, нийт бүртгэгдсэн энэ төрлийн гэмт хэргийн 58 буюу 86.6% нь Улаанбаатар хотод, 9 буюу 13.4% нь орон нутагт тус тус үйлдэгдсэн байна.

Бүртгэгдсэн гэмт хэргийн зүйл, ангиар нь авч үзвэл, нийт 13 төрлийн гэмт хэрэгт Кибер орчинд хүүхэд хохирсон байх бөгөөд нийт хэргийн 24 буюу 35.8% нь залилах, 18 буюу 26.9% нь хүүхдэд садар самууныг сурталчлах, уруу татах, 15 буюу 22.4% нь заналхийлэх, хүчиндэх, арван зургаан насанд хүрээгүй хүнтэй бэлгийн харьцаанд орох төрлийн гэмт хэргүүд эзэлж байгаа бол бэлгийн мөлжлөг, хүн худалдаалах, бэлгийн дур хүслээ ёс бусаар хангах, Кибер орчинд хууль бусаар халдах, хулгайлах, Алдаатай гүйлгээ, андуурагдсан илгээмж, гээгдэл эд хөрөнгө, алдуул мал завших төрлийн гэмт хэрэг тус бүр нэг үйлдэгдсэн байна.

1	Залилах	1	1	1	10	5	6	24
2	Кибер орчинд хууль бусаар халдах					1		1
3	Хүүхдэд садар самууныг сурталчлах, уруу татах				2	12	4	18
4	Заналхийлэх					2	1	3
5	Бэлгийн дур хүслээ ёс бусаар хангах					1		1
6	Хүн худалдаалах					1		1
7	Хүчиндэх					2	4	6
8	Арван зургаан насанд хүрээгүй хүнтэй бэлгийн харьцаанд орох					2	4	6
9	Бэлгийн мөлжлөг					1		1
10	Худал мэдээлэл тараах						2	2
11	Хулгайлах						1	1
12	Алдаатай гүйлгээ, андуурагдсан илгээмж, гээгдэл эд хөрөнгө, алдуул мал завших						1	1
13	Бусад	1					1	2
	Нийт	**2**	**1**	**1**	**12**	**27**	**24**	**67**

Дэлхийн эрүүл мэндийн байгууллагын судалгаагаар жил бүр 200 сая хүүхэд бэлгийн мөлжлөг, хүчирхийллийн золиос болдог байна. Үүний тодорхой хувь нь Кибер орчинд үйлдэгдэж, жилээс жилд хувь хэмжээ нь нэмэгдэж байгаа бөгөөд интернэт орчин нь мөлжлөг, хүчирхийллийн талбар болж байна[35]. Монгол Улсын хувьд ч гэсэн кибер орчин дахь хүүхдийн эсрэг бэлгийн эрх чөлөөний гэмт хэрэг өсөх хандлагатай байгаа тул хүүхэд хамгаллын асуудлыг бүхий л түвшинд авч үзэх шаардлагатай.

Мөн өдөр ирэх тусам өсөн нэмэгдэж буй цахим хэрэглээг дагаад компьютер, компьютерын сүлжээг ашиглан үйлдэгдэх гэмт хэргийн гаралт ихсэж байна. Олон нийтийн дунд кибер гэмт хэргийн тухай ойлголтгүй, хялбар аргаар мөнгө олох гэсэн хүний шунал, гэнэн итгэмтгий зангаас шалтгаалан уг төрлийн гэмт хэргийн гаралт ихсэх нэг том шалтгаан болж байгаа юм. Эрүүгийн хуулийн 26 дугаар бүлэгт кибер аюулгүй байдлын эсрэг гэмт хэргийн талаар хуульчилсан бөгөөд сүүлийн жилүүдэд залилах гэмт хэргийг кибер орчинд үйлдэх нь элбэг болоод байна.

[35] https://gia.gov.mn/12/item/709

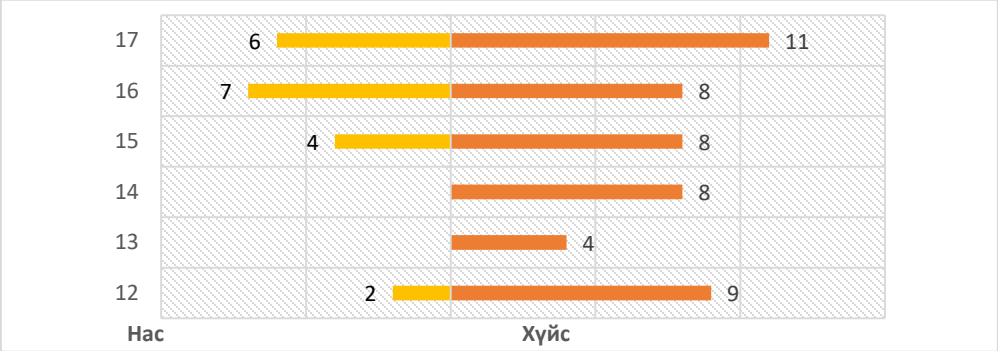
Кибер орчинд үйлдэгдэж буй гэмт хэргийн улмаас нийт 67 хүүхэд хохирсныг бүртгэгдсэн оноор нь авч үзвэл, 2015 онд 2, 2016 онд 1, 2017 онд 1, 2018 онд 12, 2019 онд 27, 2020 онд 24 хүүхэд хохирсон байна.

2020 онд хохирсон хүүхдийн тоог 2019 оныхтой харьцуулбал 11.1 хувиар буурсан, 2019 онд хохирсон хүүхдийг 2018 оныхтой харьцуулбал, 2.3 дахин өссөн байна.

Хохирсон хүүхдүүдийг хүйсээр нь авч үзвэл, энэ хугацаанд нийт хохирогчдын 18 буюу 26.9% нь эрэгтэй, 49 буюу 73.1% нь эмэгтэй хүүхэд байгаа нь 2015 онд хохирсон бүх хүүхэд эмэгтэй, 2016-2017 онд хохирсон бүх хүүхэд эрэгтэй байгаа бол 2018 онд хохирсон хүүхдийн 6 буюу 50.0% нь эмэгтэй, 6 буюу 50.0% нь эрэгтэй, 2019 онд хохирсон хүүхдийн 3 буюу 11.1% нь эрэгтэй, 24 буюу 88.9% нь эмэгтэй, 2020 онд хохирсон хүүхдийн 7 буюу 29.2% эрэгтэй, 17 буюу 70.8% эмэгтэй, 2022 он 63 буюу 69% эрэгтэй, 20 буюу 31% эмэгтэй хүүхэд байна.

Насны ангиллаар нь авч үзвэл, нийт хохирогч хүүхдүүдийн 19 буюу 28.3% нь 12 болон 15, 8 буюу 11.9% нь 13 болон 14, 23 буюу 34.3% нь 15 болон 16, 17 буюу 25.5% нь 17 насны хүүхдүүд байна.

График 22. Хохирогчдын насны ангилал, хүйс /2017-2022/



Прокурорын байгууллага 2019, 2021 он, 2021 оны III улирлын байдлаар Эрүүгийн хуулийн 26 дугаар бүлэгт заасан “кибер аюулгүй байдлын эсрэг” 453, кибер орчинд үйлдэгдсэн нийт 4593 хэрэгт хяналт тавьжээ. Дээрх хэргүүдийн 1028 буюу 22.4 хувийг давхар зүйлчлэгдсэн хэргүүд эзэлж байна.

Мөрдөн шалгах ажиллагаа явуулсан эрх бүхий байгууллагаар нь авч үзвэл хэрэг бүртгэлт, мөрдөн байцаалт явуулсан нийт хэргийн 6 буюу 0.1 хувийг Авлигатай тэмцэх газар, 19 буюу 0.4 хувийг Нийслэлийн цагдаагийн удирдах газрын Мөрдөн шалгах газар, 33 буюу 0.7 хувийг Цагдаагийн ерөнхий газрын Мөрдөн байцаах алба, 231 буюу 5.0 хувийг Эрүүгийн цагдаагийн албанаас шалгасан бол бусад 4304 хэрэг буюу 93.7 хувийг орон нутаг болон дүүрэг дэх Цагдаагийн газар, хэлтсүүдээс шалгажээ.

Хяналт тавьсан хэргийн талаар:

Прокуророос кибер аюулгүй байдлын эсрэг болон цахим сүлжээ, цахим хэрэгсэл ашиглаж үйлдсэн гэмт хэрэгт хяналт тавьсан байдлыг авч үзвэл, 2019 онд нийт 1014 хэрэгт хяналт тавьсны 614 буюу 60.6 хувь нь тухайн онд хэрэг бүртгэлтийн хэрэг нээсэн, 263 буюу 25.9 хувь нь тухайн онд эрүүгийн хэрэг үүсгэж яллагдагчаар татсан хэрэг, 2020 онд нийт 1267 хэрэгт хяналт тавьсны 559 буюу 44.1 хувь нь тухайн онд хэрэг бүртгэлтийн хэрэг нээсэн, 404 буюу 31.7 хувь нь тухайн онд эрүүгийн хэрэг үүсгэж яллагдагчаар татсан хэрэг, 2021 оны III улирлын байдлаар нийт 2312 хэрэгт хяналт тавьсны 794 буюу 69.6 хувь нь тухайн онд хэрэг бүртгэлтийн хэрэг нээсэн, 960 буюу 41.5 хувь нь тухайн онд эрүүгийн хэрэг үүсгэж яллагдагчаар татсан хэрэг тус тус эзэлж байна.

Хэрэг бүртгэлт, мөрдөн байцаалт явуулсан хэргийг гэмт хэргийн ангиллын хувьд авч үзвэл:

2019 онд нийт 1014 хэргийн 119 буюу 11.7 хувийг “Кибер орчинд хууль бусаар халдах”, 4 буюу 0.4 хувийг “Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах”, 2 буюу 0.2 хувийг “Хор хөнөөлт программ хангамж бүтээх, ашиглах, тараах”, 9 буюу 0.9 хувийг “хувь хүний нууцад халдах”, 880 буюу 86.8 хувийг “Цахим хэрэгсэл ашиглаж залилах” гэмт хэрэг;

2020 онд нийт 1267 хэргийн 153 буюу 12.0 хувийг “Кибер орчинд хууль бусаар халдах”, 5 буюу 0.4 хувийг “Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах”, 2 буюу 0.2 хувийг “Хор хөнөөлт программ хангамж бүтээх, ашиглах, тараах”, 8 буюу 0.6 хувийг “Цахим хэрэгсэл ашиглаж хувь хүний нууцад халдах”, 1099 буюу 86.7 хувийг “Цахим хэрэгсэл ашиглаж залилах” гэмт хэрэг;

2021 оны III улиралд 2312 хэргийн 163 буюу 7.0 хувийг “Кибер орчинд хууль бусаар халдах”, 1 хэрэг “Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах”, 4 буюу 0.2 хувийг “Хор хөнөөлт программ хангамж бүтээх, ашиглах, тараах”, 2 буюу 0.1 хувийг “Цахим хэрэгсэл ашиглаж хувь хүний нууцад халдах”, 2 буюу 0.1 хувийг “Цахим сүлжээ ашиглаж хүүхэд оролцуулж садар самууныг сурталчлах”, 2140 буюу 92.6 хувийг “Цахим хэрэгсэл ашиглаж залилах” гэмт хэрэг тус тус эзэлж байна.

Харин 2019, 2020 онуудад “Цахим сүлжээ ашиглан хүүхэд оролцуулж садар самууныг сурталчлах” гэмт хэрэг шалгагдаагүй байна.

Хэргийн шийдвэрлэлтийн талаар:

1.2019 онд хэрэг бүртгэлт явуулсан 939 хэрэгт хяналт тавьснаас 86 буюу 9.2 хувийг бусад хэрэгт нэгтгэж, 263 буюу 28.0 хувьд эрүүгийн хэрэг үүсгэн яллагдагчаар татаж, 286 хэрэг буюу 30.5 хувийг хааж шийдвэрлэсэн байна.

Хэрэг бүртгэлтийг хаасан хэргийн 279 буюу 97.6 хувийг гэмт хэргийн шинжгүй, 5 буюу 1.7 хувийг хэргийг хөөн хэлэлцэх хугацаа дууссан, 2 хэргийг яллагдагч, шүүгдэгч нас барсан үндэслэлээр тус тус хааж шийдвэрлэсэн байна.

Мөрдөн байцаалт явуулсан 338 хэрэгт хяналт тавьснаас 263 буюу 77.8 хувь нь тухайн онд шинээр эрүүгийн хэрэг үүсгэж яллагдагчаар татсан хэрэг байх бөгөөд 217 буюу 64.2 хувийг нэгтгэж, 2 буюу 0.6 хувийг хэрэгсэхгүй болгож, 62 буюу 18.3 хувьд яллах дүгнэлт үйлдэн шүүхэд шилжүүлсэн байна.

Хяналт тавьсан хэрэг бүртгэлтийн 1210 хэргийн 7 буюу 0.6 хувийг бусад хэрэгт нэгтгэж, 404 буюу 33.4 хувьд эрүүгийн хэрэг үүсгэн яллагдагчаар татаж, 308 хэрэг буюу 25.5 хувийг хааж шийдвэрлэсэн байна.

2020 онд Хэрэг бүртгэлтийг хаасан хэргийн 298 буюу 96.8 хувийг гэмт хэргийн шинжгүй, 6 буюу 1.9 хувийг хэргийг хөөн хэлэлцэх хугацаа дууссан, 4 хэрэг буюу 1.3 хувийг тухайн хэргийг урьд нь хэрэгсэхгүй болгосон тогтоол, магадлал хүчинтэй байгаа үндэслэлээр тус тус хаажээ.

Мөрдөн байцаалт явуулсан 461 хэрэгт хяналт тавьснаас 404 буюу 87.6 хувь нь тухайн онд шинээр эрүүгийн хэрэг үүсгэж, яллагдагчаар татсан хэрэг байна.

Хяналт тавьсан мөрдөн байцаалтын хэргийн 327 буюу 70.9 хувийг бусад хэрэгт нэгтгэж, 1 буюу 0.2 хувийг хэрэгсэхгүй болгож, 1 буюу 0.2 хэргийг түдгэлзүүлэн, 65 буюу 14.1 хувьд яллах дүгнэлт үйлдэж шүүхэд шилжүүлсэн байна.

2021 оны 3-р улирлын байдлаар хяналт тавьсан хэрэг бүртгэлтийн 1784 хэргээс 20 буюу 1.1 хувийг бусад хэрэгт нэгтгэн, 960 буюу 53.8 хувьд эрүүгийн хэрэг үүсгэн яллагдагчаар татаж, 221 буюу 12.4 хувийг хааж, 583 хэрэг буюу 32.7 хувь нь мөрдөн шалгах ажиллагаанд байгаагийн 266 буюу 45.6 хувьд хугацаа сунган шалгаж байна.

Хэрэг бүртгэлтийг хаасан хэргийн 189 буюу 85.5 хувийг гэмт хэргийн шинжгүй, 7 буюу 3.2 хувийг хэргийг хөөн хэлэлцэх хугацаа дууссан, 25 буюу 11.3 хувийг яллагдагч, шүүгдэгч нас барсан үндэслэлээр тус тус хааж шийдвэрлэсэн байна.

Мөрдөн байцаалт явуулсан 1027 хэрэгт хяналт тавьснаас 960 буюу 93.5 хувь нь тухайн онд шинээр эрүүгийн хэрэг үүсгэж яллагдагчаар татсан хэрэг байна.

Хяналт тавьсан мөрдөн байцаалтын хэргийн 829 буюу 80.7 хувийг бусад хэрэгт нэгтгэж, 6 буюу 0.6 хувийг хэрэгсэхгүй болгож, 1 хэргийг түдгэлзүүлэн, 70 буюу 6.8 хувьд яллах дүгнэлт үйлдэж шүүхэд шилжүүлж, үлдэгдэл 121 хэрэгт мөрдөн байцаалтын ажиллагаа явуулж байгаагийн 38 буюу 31.4 хувьд хугацаа сунган шалгаж байна.

Хэрэгсэхгүй болгосон 6 хэргээс 1 хэргийг сэжигтэн, яллагдагч барсан, 1 хэргийг ял оногдуулах насанд хүрээгүй үндэслэлээр, 4 хэргийг Өршөөл үзүүлэх тухай хуульд зааснаар тус тус хэрэгсэхгүй болгожээ.

2019, 2020 он, 2021 оны III улирлын байдлаар хяналт тавьж шийдвэрлэсэн хэргүүдийг нэгтгэн авч үзвэл, хэрэг бүртгэлтийн нийт 3933 /давхардсан тоогоор/ хэргээс 113 буюу 2.9 хувийг нэгтгэж, 1627 буюу 41.4 хувьд эрүүгийн хэрэг үүсгэн яллагдагчаар татаж, 815 хэрэг буюу 20.7 хувийг хааж шийдвэрлэсэн.

Хэрэг бүртгэлтийг хаасан хэргийн 766 буюу 94.0 хувийг гэмт хэргийн шинжгүй, 18 буюу 2.2 хувийг хэргийг хөөн хэлэлцэх хугацаа дууссан, 27 хэрэг буюу 3.3 хувийг яллагдагч, шүүгдэгч нас барсан, 4 хэргийг урьд нь хэрэгсэхгүй болгосон тогтоол, магадлал хүчинтэй байгаа үндэслэлээр шийдвэрлэсэн.

Мөрдөн байцаалт явуулсан 1826 хэргээс 1373 буюу 75.2 хувийг бусад хэрэгт нэгтгэж, 9 буюу 0.5 хувийг хэрэгсэхгүй болгож, 197 буюу 10.8 хувьд яллах дүгнэлт үйлдэж, шүүхэд шилжүүлсэн байна.

1/ Кибер орчинд болон цахим сүлжээ, цахим хэрэгсэл ашиглаж үйлдсэн гэмт хэргийг нийгмийн мэдээллийн сүлжээг ашиглаж үйлдсэн байдал

Хэрэг бүртгэлт, мөрдөн байцаалт явуулсан нийт 4593 хэргийн 1374 буюу 29.9 хувийг “Facebook”, 66 буюу 1.4 хувийг “e-mail” буюу цахим шуудан, 7 буюу 1.4 хувийг “Instagram”, 650 буюу 14.2 хувийг веб сайт болон бусад мэдээллийн сүлжээ ашиглаж үйлдсэн бол “Twitter”, “Tik tok” зэрэг бусад мэдээллийн сүлжээг ашиглаж үйлдэгдсэн гэмт хэрэг бүртгэгдээгүй байна.

“Facebook” мэдээллийн сүлжээг ашиглаж үйлдсэн гэмт хэрэг 2019 онд 305 шалгагдсан бол 2020 онд 308, 2021 оны III улирлын байдлаар 761 тус тус шалгагдсан. Үүнээс 54 хэрэг буюу 3.9 хувийг “Кибер орчинд хууль бусаар халдах”, 4 буюу 0.3 хувийг “Цахим хэрэгсэл ашиглаж Хувь хүний нууцад халдах”, 2 буюу 0.1 хувийг “Цахим сүлжээ ашиглаж Хүүхэд оролцуулж садар самууныг сурталчлах”, 1314 буюу 95.6 хувийг “Цахим хэрэгсэл ашиглаж Залилах” гэмт хэрэг;

“e-mail” цахим шуудан мэдээллийн сүлжээг ашиглаж үйлдсэн гэмт хэрэг 2019 онд 11 шалгагдсан бол 2020 онд 29, 2021 оны III улирлын байдлаар 26 хэрэг шалгагдсан. Үүнээс 13 буюу 19.7 хувийг “Кибер орчинд хууль бусаар халдах”, 53 буюу 80.3 хувийг “Цахим хэрэгсэл ашиглаж Залилах” гэмт хэрэг;

“Instagram” ашиглаж үйлдсэн гэмт хэрэг 2019 онд 1, 2020 онд 4, 2021 оны III улирлын байдлаар 2 хэрэг тус тус шалгагдсан. Үүнээс 1 буюу 14.3 хувийг “Кибер орчинд хууль бусаар халдах”, 6 буюу 85.7 хувийг “Цахим хэрэгсэл ашиглаж Залилах” гэмт хэрэг;

Бусад веб сайт, мэдээллийн сүлжээ ашиглаж үйлдсэн гэмт хэрэг 2019 онд 144, 2020 онд 167, 2021 оны III улирлын байдлаар 339 тус тус шалгагдсан. Үүнээс 52 хэрэг буюу 8.0 хувийг “Кибер орчинд хууль бусаар халдах”, 1 буюу 0.2 хувийг “Цахим хэрэгсэл ашиглаж Хувь хүний нууцад халдах”, 597 буюу 91.8 хувийг “Цахим хэрэгсэл ашиглаж Залилах” гэмт хэрэг тус тус эзэлж байна.

2/ Цахим мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг болон цахим сүлжээ, цахим хэрэгсэл ашиглаж үйлдэж буй гэмт хэргийн арга хэлбэр

Хэрэг бүртгэлт, мөрдөн байцаалт явуулсан нийт 4593 хэргийн 473 буюу 10.3 хувийг нийгмийн сүлжээ, хэрэглэгчийн нэвтрэх нэр, нууц үгийг хууль бусаар олж авах, 427 буюу 9.3 хувийг хэрэглэгчийн дансны болон зээлийн картын мэдээллийг хууль бусаар олж авах, 842 буюу 18.3 хувийг хувь хүнд сэдэл өгч, итгэл төрүүлэх замаар мэдээллийг олж авах, 18 буюу 0.4 хувийг компьютерын сүлжээнд вирус, хортой код тараах, спам халдлага үйлдэх аргаар үйлдэгдсэн байна. Дээрх хэргүүдийг Эрүүгийн хуулийн тусгай ангид заасан зүйлчлэлээр нь авч үзвэл:

Нийгмийн сүлжээ, хэрэглэгчийн нэвтрэх нэр, нууц үгийг хууль бусаар олж авах аргаар үйлдэгдсэн 473 хэргийн 40 буюу 8.5 хувийг Эрүүгийн хуулийн 26.1 дүгээр зүйлд заасан “Кибер орчинд хууль бусаар халдах”, 2 буюу 0.4 хувийг 13.10 дугаар зүйлийн 2 дахь хэсгийн 2.1-д заасан “Цахим хэрэгсэл ашиглаж хувь хүний нууцад халдах”, 1 буюу 0.2 хувийг 16.9 дүгээр зүйлийн 2 дахь хэсгийн 2.1-д заасан “Цахим сүлжээ ашиглаж хүүхэд оролцуулж садар самууныг сурталчлах”, 430 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 427 хэргийн 44 буюу 10.3 хувийг “Кибер орчинд хууль бусаар халдах”, 3 буюу 0.7 хувийг “Цахим хэрэгсэл ашиглаж хувь хүний нууцад халдах”, 380 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 842 хэргийн 19 буюу буюу 2.3 хувийг “Кибер орчинд хууль бусаар халдах”, 822 буюу 97.6 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 шалгагдсан байна.

Компьютерын сүлжээнд вирус, хортой код тараах, спам халдлага үйлдэх аргаар үйлдэгдсэн 18 хэргийн 15 буюу 83.3 хувийг “Кибер орчинд хууль бусаар халдах”, 3 буюу 16.7 хувийг “Цахим хэрэгсэл ашиглаж залилах” гэмт хэрэг эзэлжээ.

Мөн хэрэглэгчийн данс болон зээлийн картын мэдээлэлд хууль бусаар халдаж, иргэдийн данснаас мөнгө гуйвуулан авсан хэрэг 2019 онд 93 гарсан бол 2020 онд 99 болж 6-р буюу 6.5 хувиар, 2021 оны III улирлын байдлаар 188 болж 89-р буюу 89.9 хувиар тус тус өссөн бол хувь хүнд сэдэл өгч, итгэл төрүүлэх замаар мэдээллийг олж авах аргаар үйлдэгдсэн залилах гэмт хэрэг 2019 онд 197 гарсан бол 2020 онд 236 болж 39-р буюу 19.8 хувиар, 2021 оны III улирлын байдлаар 389 болж 153-р буюу 64.8 хувиар өссөн дүнтэй байна.

3/ Гэмт хэргийн улмаас учирсан хохирол, хор уршиг, нөхөн төлүүлэх, арилгуулах талаар авсан арга хэмжээний талаар

2019, 2020 он, 2021 оны III улирлын байдлаар Эрүүгийн хуулийн Хорин зургаадугаар бүлэгт заасан “Цахим мэдээллийн аюулгүй байдлын эсрэг” гэмт хэрэг 453, мөн хуулийн 17.3 дугаар зүйлийн 1 дэх хэсэгт заасан “Цахим хэрэгсэл ашиглаж залилах” 4119, нийт 4572 гэмт

хэргийн улмаас 1811 хүн, 8 хуулийн этгээдэд 12.781.765.586 төгрөг, 631.791 ам.доллар, 48.930 евро буюу нийт 14.7 тэрбум төгрөгийн хохирол учирсан байна.

Тодруулбал, “Цахим мэдээллийн аюулгүй байдлын эсрэг” гэмт хэргийн улмаас 231 хүн, 7 хуулийн этгээдэд 1.4 тэрбум төгрөг, 219.903,17 ам доллар буюу нийт 2.0 тэрбум төгрөгийн хохирол учирсан бол “Цахим хэрэгсэл ашиглаж залилах” гэмт хэргийн улмаас 1 хуулийн этгээд, 1580 хүнд 11.4 тэрбум төгрөг, 411.887,83 ам доллар, 48.930 евро буюу нийт 12.7 тэрбум төгрөгийн хохирол учирчээ.

Харин 2019, 2020 он, 2021 оны III улирлын байдлаар мөрдөн шалгах ажиллагааны явцад 177 хэргийн 279 хохирогч, 3 хуулийн этгээдэд нийт 539.369.241 төгрөг, 38.025 ам.доллар буюу нийт 645,7 сая төгрөгийн хохирол нөхөн төлөгдсөн байна.

4/ Гэмт хэрэг үйлдсэн этгээдийн нас, хүйс, боловсрол, мэргэжил, ажил эрхлэлт, ял шийтгэл болон хохирогчтой хамаарал бүхий байдлын талаар

Энэ төрлийн гэмт хэрэгт холбогдуулан 2019, 2020, 2021 оны III улирлын байдлаар мөрдөн байцаалт явуулсан нийт 1826 хэрэгт 526 хүн яллагдагчаар шалгагдсаны 354 буюу 67.3 хувь эрэгтэй, 172 буюу 32.7 хувь нь эмэгтэй хүн байна.

Яллагдагчаар татагдсан этгээдүүдийг насны байдлаар нь авч үзвэл 13 буюу 2.5 хувь нь 18-аас доош насны, 244 буюу 46.4 хувь нь 18-25 насны, 244 буюу 46.4 хувь нь 26-45 насны, 25 буюу 4.8 хувь нь 45-аас дээш насны хүн байна.

Эдгээр гэмт хэрэгт холбогдсон этгээдүүдийг боловсролын байдлаар авч үзвэл, 5 буюу 1.0 хувь нь боловсролгүй, 6 буюу 1.1 хувь нь бага боловсролтой, 399 буюу 75.9 хувь бүрэн дунд, 15 буюу 2.9 хувь нь тусгай дунд, 101 буюу 19.2 хувь дээд боловсролтой хүмүүс байна.

Мэргэжлийн байдлаар авч үзвэл нягтлан бодогч, эдийн засагч мэргэжилтэй 10, бизнес, санхүүгийн удирдлага 8, мэдээлэл, технологи, программ хангамжийн инженер 8, электрон систем, техник тоног төхөөрөмжийн инженер 7, барилгын инженер 6, уул уурхайн ашиглалтын инженер 6, авто, механикийн инженер 6, жолооч, автомашин засварчин 6, эрх зүйч 5, багш, дасгалжуулагч 5, тогооч 5, гагнуурчин 5, цахилгааны инженер 4, эмч 4, компьютерын операторч 3, кино зураглаач, жүжигчин 3, интерьер дизайнер 3, хэвлэлийн график дизайн, төрийн захиргааны менежмент 2, орчуулагч 3, аялал жуулчлалын менежер 2, гоо сайханч 2, гагнуурчин, мужаан 2, хүний нөөцийн менежер 2, маркетингийн менежер 2, холбооны инженер, түүхч, сэтгэл зүйч, архитектурч, хөгжмийн удирдаач, сувилагч, хивсчин мэргэжилтэй тус бүр 1 хүн байна.

Ажил эрхлэлтийн байдлыг авч үзвэл 415 буюу 78.9 хувь нь тодорхой эрхэлсэн ажилгүй, 111 буюу 21.1 хувь нь эрхэлсэн ажилтай. Үүнээс 42 буюу 37.8 хувь нь хувиараа хөдөлмөр эрхэлдэг, 62 буюу 55.9 хувь нь хувийн хэвшлийн байгууллагад ажилладаг бол 7 буюу 6.3 хувь нь төрийн байгууллагад ажилладаг байна.

Нийт яллагдагчаар татагдсан хүмүүсийн 50 буюу 9.5 хувь нь өмнө нь ял шийтгүүлж байсан байна. Эдгээр хүмүүсийн 6 буюу 12 хувь нь Кибер орчинд хууль бусаар халдах, 44 буюу 88.0 хувь нь Цахим хэрэгсэл ашиглаж Залилах гэмт хэрэгт тус тус яллагдагчаар татагджээ.

Хохирогчтой харилцаа хамаарлын тухайд, гэмт хэрэг үйлдсэн этгээдүүдийн 6 буюу 1.1 хувь нь хохирогчтой найз нөхдийн харилцаатай, 2 буюу 0.4 хувь нь хамаатан, 12 буюу 2.3 хувь нь таньдаг хүмүүс, харин 506 буюу дийлэнх 96.2 хувь нь хохирогчтой ямар нэгэн харилцаа хамааралгүй, таньж мэдэхгүй хүмүүс тухайн гэмт хэргийг үйлдсэн байна.

5/ Мэдээ, мэдээлэл, баримт бичгийг холбогдох байгууллага, албан тушаалтан, хүнээс гаргуулан авах ажиллагааг прокурорын зөвшөөрлөөр явуулсан талаар

Эрүүгийн хэрэг хянан шийдвэрлэх тухай хуулийн 24.5 дугаар зүйлийн 1 дэх хэсэгт “Мөрдөгч төрийн нууц, хувь хүний эрүүл мэнд, захидал харилцааны нууцтай холбоотой эрүүгийн хэрэгт ач холбогдол бүхий мэдээлэл, баримт бичгийг холбогдох байгууллага, албан тушаалтан, хүнээс прокурорын зөвшөөрлөөр гаргуулан авна” гэж заасны дагуу 2019, 2020 он, 2021 оны III улирлын байдлаар Цахим мэдээллийн аюулгүй байдлын эсрэг болон цахим сүлжээ, цахим хэрэгсэл ашиглаж үйлдсэн 498 хэрэгт хувь хүний захидал, харилцааны нууцтай холбоотой мэдээ, мэдээлэл, баримт бичгийг холбогдох байгууллага, албан тушаалтнаас гаргуулах тухай нийт 658 саналыг прокурорт гаргажээ.

Прокурор мөрдөгчийн саналыг хүлээн авч хянаад хэрэг хянан шийдвэрлэх ажиллагаанд ач холбогдолтой гэж үзэн, мөн хуулийн 22.1 дүгээр зүйлийн 3, 22.3 дугаар зүйлийн 2, 3, 24.5 дугаар зүйлийн 1 дэх хэсэгт заасны дагуу 2019 онд 92 хэрэгт 151, 2020 онд 117 хэрэгт 169, 2021 онд 286 хэрэгт 338 прокурорын зөвшөөрлийг тус тус олгосон байна.

§2.2. Кибер орчинд үйлдэгдсэн гэмт хэргийн шалтгаан нөхцөл, тулгамдаж буй асуудал

Монгол Улсад интернэт хэрэглэгчдийн тоо 2012 онд 695 мянга байсан бол уг тоо 2017 онд 3.5 сая, 2018 онд 4.1 сая, 2019 онд 5.4 сая болж 2012 онтой харьцуулахад 7.8 дахин нэмэгдсэн, фейсбүүк хэрэглэгчдийн тоогоор Ази тивд 1 дүгээрт /2.2 сая хэрэглэгч/, дэлхийд 10 дугаар байрт жагсах болсон ба цахим хэрэглээний хамрах хүрээ, хэрэглээ хурдацтай өсөж байгаа нь Үндэсний статистикийн хорооны мэдээллээс харагдаж байна. Цагдаагийн байгууллагаас 2020 онд хийсэн нөхцөл байдлын судалгаагаар гадаад улсад оршин суугаа Монгол Улсын иргэд олон нийтийн сүлжээн /фейсбүүк/-д мэдээлэл солилцох, худалдаа наймаа эрхлэх, ажлын зар түгээх, сонирхсон зүйлээр нэгдэх зэрэг чиглэлээр 35 оронд 619 фейсбүүк хаяг нээгдэж, давхардсан тоогоор 3.2 сая хэрэглэгч идэвхтэй ашигладаг.

Монгол Улсын хэмжээнд цахим халдлагыг илрүүлэх, хариу арга хэмжээ авах үйл ажиллагааг Тагнуулын ерөнхий газрын Мэдээллийн аюулгүй байдлын газар, “Үндэсний дата төв” УТҮГ, “MonCERT” ТББ зэрэг байгууллагууд явуулж байна. Эдгээр байгууллагуудаас ирүүлсэн тайлан мэдээллээс үзэхэд төрийн байгууллагуудын сүлжээнд гадаадын 40 орчим улсаас хоногт дунджаар 9900 орчим маш өндөр түвшний, 8000 орчим өндөр түвшний цахим халдлага бүртгэгдэж байгаа бол төрийн байгууллагуудын цахим хуудаст Монгол, БНХАУ, ОХУ, АНУ, ХБНГУ-аас халдлагууд хамгийн ихээр бүртгэгдэж байна. Төрийн байгууллагуудад чиглэж буй цахим халдлагуудад мэдээлэл хулгайлах зорилготой халдлага дийлэнх хувийг эзэлж байна.

Төрийн байгууллага, эрчим хүчний салбарын онц чухал дэд бүтэцтэй байгууллагуудад хийсэн цахим мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээнээс харахад тус байгууллагуудын удирдлагууд цахим мэдээллийн аюулгүй байдлын талаарх ойлголт муу, дэмжлэг сул, энэ чиглэлээр ажилладаг хүний нөөцийн чадвар дутмаг, мэдээллийн технологийн хэрэглээ өндөр хэдий ч энэ чиглэлд хэрэгжүүлсэн төсөл, хөтөлбөрүүдэд аюулгүй байдлын асуудлыг орхигдуулсан, мэдээллийн аюулгүй байдлын үндэсний стандартуудыг мөрддөггүй, сургалт, сурталчилгаа хийгддэггүй зэрэг нийтлэг дутагдал илэрч цахим халдлагад өртөх магадлал өндөр байна.[36]

Манай улс мэдээллийн аюулгүй байдалд төдийлөн анхаардаггүй, ойлголт болон мэдлэг, хяналт сул, энэ чиглэлээр мэргэшсэн мэргэжилтэн дутмаг, албан ёсны эрхтэй программ хангамж /үйлдлийн систем, хэрэглээний болон вирусийн эсрэг программ хангамж/-уудыг хэрэглэдэггүй, мэдээллийн аюулгүй байдлыг хангахад шаардагдах зардлыг төсөвт тусгадаггүй зэрэг нь халдлагад өртөх боломжийг бүрдүүлж байна.

Түүнчлэн төрийн болон төрийн бус байгууллага, бизнесийн үйл ажиллагаа эрхэлж байгаа аж ахуйн нэгж, байгууллага болон иргэд хоорондын харилцаа цахимжиж, дижитал шилжилт хийж буй өнөө үед Монгол Улсад хүчин төгөлдөр мөрдөгдөж буй төрийн болон

[36] Тагнуулын ерөнхий газрын Мэдээллийн аюулгүй байдлын газраас хийсэн эрсдэлийн үнэлгээ

албаны нууц, хувь хүний нууцын тухай хуулиар хамгаалагдсан мэдээлэл Кибер орчинд хамгаалалтгүй, алдагдах эрсдэл өндөр гэж үзэхээр байна.

Иргэдийн Кибер орчин дахь аюулгүй байдлын мэдлэг хангалтгүй, фейсбүүк, твиттер зэрэг гадаад улсад сервертэй шууд зохицуулалт хийх боломжгүй системүүдийг идэвхтэй ашиглаж байгаа нь гэмт хэрэгт өртөж хохирох, гэмт этгээдүүдэд хууль бус үйл ажиллагаагаа халхавчлах, ул мөрөө баллах, дүр төрхөө өөрчлөх боломжийг бүрдүүлдэг.

Улсын хэмжээнд сүүлийн гурван жилийн байдлаар Кибер орчинд үйлдэгдсэн 8253 гомдол, мэдээллийг Цагдаагийн байгууллага хүлээн авч шалгаж, шийдвэрлэсэн.

Кибер орчинд үйлдэгдсэн гэмт хэргийг оноор нь харьцуулбал 2015 онд 61, 2016 онд 97, 2017 онд 195, 2018 онд 659, 2019 онд 737, 2020 оны эхний 08 сард 1032 тус тус бүртгэгдэж өсөлтийн дундаж 92.4 хувьтай байна.

Гэмт бүлэглэлүүд хууль бус үйл ажиллагаагаа хөнгөвчлөх, богино хугацаанд ашиг олох зорилгоор интернэтийг өргөнөөр ашиглах болсонтой холбоотойгоор хулгайлах, залилах, хууль бус мөрийтэй тоглоом, мөнгө угаах зэрэг гэмт хэргүүд кибер орчинд үйлдэгдэх болсон тул хууль сахиулах байгууллагууд кибер орчинд үйлдэгдэж байгаа дээрх төрлийн гэмт хэрэгтэй тэмцэх чиглэлд анхаарах шаардлагатай байгааг Олон Улсын Эрүүгийн цагдаагийн байгууллага /Интерпол/-аас онцолсон.[37]

Мөн кибер орчин дахь хуурамч мэдээ, мэдээлэлтэй тэмцэх олон нийтийг төөрөгдөлд оруулахаас урьдчилан сэргийлэх, тогтвортой байдлыг хангах болон мэдээллийн дайнаас улс орны тусгаар тогтнол, аюулгүй байдлыг хамгаалах зорилгоор улс орнууд хуурамч мэдээ, мэдээлэлтэй тэмцэх тодорхой арга хувилбаруудыг хэрэгжүүлж байна.

АНУ, ОХУ, Украйн зэрэг улс орнууд иргэдээ хуурамч мэдээллээс хамгаалах, дархлаа тогтоох зорилгоор тухайн хуурамч мэдээлэлд дүн шинжилгээ хийх, албан ёсны эх сурвалжаас тодруулга авах, үр дүнг олон нийтэд мэдээлэх үүрэг бүхий төрийн болон төрийн бус байгууллагуудыг ажиллуулж байна.

Монгол Улсад кибер орчинд хуулиар хамгаалуулсан төр, хувийн хэвшил болон иргэний эрх, эрх чөлөөг хангах, хамгаалах, аюулгүй байдал зэрэгт хохирол учруулах, цаашлаад Үндэсний аюулгүй байдалд сөргөөр нөлөөлөхүйц мэдээлэл тархах сүлжээ, орчин бий болсон нь харагдаж байна.

Технологийн хувьсгал, дижитал шилжилтийн энэ үед төр, хувийн хэвшлийн байгууллага, иргэдийн эрх, эрх чөлөөг хамгаалах, аюулгүй байдлыг хангах, гэмт хэрэгт өртөж хохирохоос урьдчилан сэргийлэх, түүний хор уршгийг бууруулах, аюулгүй цахим орчныг бий болгох нь үндэсний аюулгүй байдлыг хамгаалах үүрэг бүхий төрийн тусгай албадын чиг үүрэгт хамаарах асуудал мөн бөгөөд тэдгээр байгууллагуудын хамтын ажиллагааг идэвхжүүлэх, хууль, эрх зүйн зохицуулалтыг боловсронгуй болгох, хүн хүч, технологийн чадавхыг

[37] https://www.interpol.int/

бэхжүүлэх зэрэгт төрийн нэгдсэн бодлого, шийдвэрээр дэмжлэг үзүүлэх шаардлага үүссэн гэж дүгнэж байна.

Тулгамдаж буй асуудал

1. Гадаад хамтын ажиллагаа:

Энэ төрлийн гэмт хэрэг нь үндэстэн дамнасан шинж чанартай байдаг бөгөөд тухайн улсын хууль сахиулах байгууллагаас шаардлагатай мэдээллээ гаргуулан авах асуудал хүндрэлтэй байдаг.

Жишээ нь: Кибер орчинд үйлдэгдэж байгаа гэмт хэрэг, зөрчилтэй тэмцэх ажлын хүрээнд АНУ-ын Фейсбүүк компанитай хамтран хууль бус үйл ажиллагаатай холбоотой контентыг устгах, хэрэглэгчийн талаарх холбогдох мэдээллийг гаргуулж авах ажиллагааг шат дараатай хэрэгжүүлж байна. /Тус компаниас хэрэглэгчийн мэдээллийг зөвхөн “терроризм”, “хүний амь нас хохирох нөхцөл байдал бий болсон”, “бага насны хүүхдийн садар самуун сурталчилсан контент”, “секс сүрдүүлэг” болон үндэстэн дамнасан, зохион байгуулалттай гэмт хэрэг зэрэгт мэдээлэл гаргаж өгнө гэж мэдэгдсэн/.

Гадаад улсад сервертэй олон нийтийн сүлжээ веб сайтууд нь тухайн улсын хууль тогтоомжийн хүрээнд үйл ажиллагаа явуулдаг тул манай улсаас хүргүүлж буй хүсэлт, албан бичгийг хүлээн авдаг ч тэр даруй хариу өгөхгүй, дийлэнх тохиолдолд хүсэлтийг хангахаас татгалзаж шийдвэрлэж байгаа нь энэ төрлийн гэмт хэрэг, зөрчилтэй тэмцэх ажилд хүндрэл учруулж байна.

2. Эрх зүйн зохицуулалт:

Дэлхийн улс орнууд мэдээллийн технологийн хөгжлийг хуулиар урьдчилан зохицуулах боломжгүй хэдий ч мэдээллийн технологийг түгээх, ашиглах, хуульд заасан үндэслэл журмын хүрээнд хянах, хязгаарлах үйл ажиллагааны үндэсний тогтолцоо, дэд бүтэц, нийтээр дагаж мөрдөх хэм хэмжээг бий болгож, цахим мэдээллийн аюулгүй байдлаа хангаж байна.

Эрүүгийн хуулийн тусгай ангийн 26 дугаар бүлэгт “Кибер орчинд хууль бусаар халдах, Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах**”** зэрэг үйлдлийг гэмт хэрэгт тооцож ял шийтгэхээр заасан нь өнөө цагийн мэдээллийн технологийн үсрэнгүй хөгжлийн үед дэлхий дахинаа ихээр үйлдэгдэж буй энэ төрлийн зарим гэмт хэргийг гэмт хэрэгт тооцоогүйн улмаас гэмт этгээд ял завших нөхцөлийг бүрдүүлж байна.

3. Интернэт орчны дэд бүтэц:

Манай улсын интернэтийн дэд бүтэц одоогоор “IP” хаягийн мэдээллийг дэлгэрэнгүй гаргах, эзэмшигчийг тогтоох, урсгалын хяналт хийх техникийн боломж хязгаарлагдмал байгаа нь кибер орчинд үйлдэгдэж буй гэмт хэрэгтэй тэмцэх ажилд хүндрэл учруулж байна. Тодруулбал нэг “IP” хаягийг олон хэрэглэгч дундаа хэрэглэдэг байдлаас шалтгаалан гэмт

этгээдүүдийн тухайн цаг хугацаанд, ямар “IP” хаяг ашигласан талаарх мэдээллийг гаргуулан авах боломж дутагдалтай байна.

4. Боловсон хүчин, хүний нөөцийн хүрээнд:

Кибер гэмт хэрэг мөрдөх ажиллагаа нь өөрөө хортой код болон мэдээллийн сүлжээний өргөн мэдлэг шаардах ажил тул цагдаагийн байгууллагад цахим гэмт хэрэгтэй тэмцэх мэдээлэл технологийн мэргэжилтэн дутмаг байгаа нь энэ төрлийн гэмт хэрэгтэй тэмцэх ажил удаашралтай явагдаж байна. Цаашид энэ төрлийн гэмт хэрэг мөрдөн шалгах мөрдөгч, боловсон хүчийг бэлтгэх боловсролын тогтолцоог бий болгох шаардлагатай.

§2.3. Кибер орчинд үйлдэгдсэн гэмт хэрэгт мөрдөх ажиллагаа явуулах асуудал

Кибер орчинд үйлдэгдсэн гэмт хэрэгт мөрдөн шалгах ажиллагааг мэдээллийн технологи, харилцаа холбооны талаар өндөр мэдлэг, мэргэшилтэй алба хаагч хийж гүйцэтгэх шаардлагатай. Учир нь кибер 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 мэдлэг шаардлагатай болдог. Хэрэв энэ төрлийн гэмт хэрэгтэй тэмцэх зохих мэдлэг, чадвар байхгүй бол Кибер аюулгүй байдлын эсрэг гэмт хэргийг таслан зогсоох, илрүүлэх, шийдвэрлэх боломжгүй болно.

Монгол Улсад facebook, instagram, twitter, likee, tiktok зэрэг шууд зохицуулалт хийх боломжгүй, гадаад улсад сервертэй олон нийтийн сүлжээг идэвхтэй ашигладаг.

Ялангуяа фейсбүүк 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 орж, хохирогч нартай харилцаа тогтоох, садар самуун агуулгатай зураг, дүрс бичлэг солилцох, биеэ үнэлэлт зохион байгуулах зэрэг хүүхдийн эсрэг гэмт хэрэг үйлдэж байна.

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

Манай улсад гэмт хэрэг үйлдэхэд ашиглагдсан IP хаяг, төхөөрөмжийн мэдээлэл, гар утасны дугаар, байршил, интернэт банкны лог зэрэг гэмт хэргийг илрүүлэхэд ач холбогдол бүхий мэдээллүүдийг холбогдох байгууллагуудаас гаргуулж авах процесс, шат дамжлага ихтэй, цаг хугацаа их зарцуулдаг. Үүний улмаас Эрүүгийн хэрэг хянан шийдвэрлэх ажиллагааны зорилт болох гэмт хэргийг шуурхай, бүрэн илрүүлэх, гэмт хэрэг үйлдсэн хүн, хуулийн

этгээдийг олж тогтоон шударгаар ял оногдуулах, хүний эрх, хууль ёсны ашиг сонирхлыг хамгаалах, зөрчигдсөн эрхийг сэргээх зорилт хэрэгжих нөхцөл боломжгүй байна[38].

Тухайлбал, тодорхой гэмт хэргийг real-time буюу гэмт хэрэг үйлдэгдэж буй тухайн мөчид нь илрүүлэх, таслан зогсоох боломж хязгаарлагдмал, тоон ул мөр устах эрсдэлийг бий болгодог. Тиймээс хүүхдийн эсрэг гэмт хэрэгт төрийн болон хувийн хэвшлийн байгууллагаас шуурхай мэдээлэл гаргуулан авах боломжийг нэмэгдүүлэхэд шаардлагатай бүхий л арга, зам, үйл ажиллагааг (мөрдөгч, прокурор, шүүгч, банк, оператор компани зэрэг хамтарсан баг ажиллах гэх мэт) судалж, нэвтрүүлэх шаардлагатай.

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.

Дээрх төрлийн гэмт хэргийг 2 хэсэгт хуваж үзэх ба Криминалистикийн болон Мэдээллийн 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 объектын 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.

Хэдий мэргэжилтэн зайлшгүй оролцуулах шаардлагатай ч хэрэгт мөрдөн шалгах ажиллагаа явуулах эрх бүхий алба хаагч доорх зүйлсийг зайлшгүй мэдэх шаардлагатай.

Мэдээллийн ул мөр нь шууд компьютер /тодорхой техник хэрэгсэл дээр/ болон шууд бус төхөөрөмж[39]үүд дээр хадгалагдсан байж болдог. Дээрх тохиолдолд дараах арга хэмжээг авна. Үүнд:

1. Интернэт холболтыг ямар компанийн хаяг, IP хаяг ашиглан холбогдсон болох

2. Уг хаягаар тухайн хэрэглэгчийн сүлжээнд тухайн Log файлаар нэвтэрсэн цаг хугацаа, хэдий хугацаанд байрласан зэргийг тодруулах

[38] Монгол Улсын Эрүүгийн хэрэг хянан шийдвэрлэх тухай хууль. 2017 он.

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

3. Интернэт сүлжээнд нэвтэрсэн үйлдлийг компьютер автоматаар хадгалдаг бөгөөд тухайн Log файл нь интернэттэй хамт тухайн төхөөрөмжид холбогдсон байх юм бол тухайн компьютер /төхөөрөмж, сүлжээ, систем/-д халдсан гэдэг нотлох баримт болдог.

4. Windows үйлдлийн системтэй компьютерууд программын үйлдлийн талаарх мэдээллийг үүсгэн, түүний хуулбарыг бий болгон автоматаар хадгалж байдаг. Тодорхой жишээ дурдахад:

-/Windows/Temporary Internet Files/ - Интернэтэд байрласан мэдээлэл,

-Windows/History – 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 – Интернэтэд орох үед мэдээлэл солилцсон талаарх түүх хадгалагддаг.

-/Windows/Downloaded Programm Files – тухайн үйлдлийн системд гаднаас ачаалагдсан файлуудын талаарх түүхийг харуулдаг. Нэг үгээр хэлэх юм бол вирус болон бусад байдлаар тухайн үйлдлийн системд нөлөөлөх программууд ачаалагдсан байдлыг харуулдаг.

-/Windows/Application Data/ - цахим шуудангаар явуулсан, хүлээн авсан талаарх мэдээллийг харуулдаг.

-/Windows/Application Data/ Identities/Microsoft/Outlook – цахим шуудангаар явуулсан, хүлээн авсан талаарх мэдээллийг харуулдаг.

-/Windows/Application Data/Microsoft/Adress book – тухайн эзэмшигчийн хаягуудыг харуулдаг.

-/Windows/SchedLog.txt/ - тухайн үйлдлийн системийн төлөвлөлтийг харуулдаг.

Сүлжээнд холбогдсон компьютерыг хураан авах ажиллагаанд цагдаагийн алба хаагч тухайн хэрэгт хувийн сонирхолгүй компьютерын мэргэжилтнийг урьж оролцуулна. Энэ үедээ тухайн байгууллага, газар дээр нь үзлэг хийж, компьютерыг эсхүл түүний хард драйверыг салган авч болно.

Компьютер, түүний хард драйверт үзлэг хийх, шинжээч томилж, шинжилгээ хийлгэх журмыг энэ журмын 3 дугаар зүйлээр, дараах маягаар тодорхойлж өгсөн.

1. Гэмт хэрэгт ач холбогдол бүхий байдлыг тодруулах зорилгоор компьютерын хард драйвер, флоппи диск, компакт диск, бусад мэдээлэл хадгалах төхөөрөмжид үзлэг хийж, шаардлагатай гэж үзвэл шинжээч томилж, дүгнэлт гаргуулна.

2. Шинжилгээ хийлгэх бол шинжээч томилсон тогтоолын хамт тухайн эд мөрийн баримтаас гадна дор дурдсан зүйлсийг хүргүүлнэ:

а/ хураан авсан тэмдэглэлийн хуулбар;

б/ шинжилгээгээр олж тогтоох зүйлийн жагсаалт /фото зураг, санхүүгийн бүртгэл, мэйл,

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.

а/ тухайн хэрэгсэл нь хуулбарлан авахаас сэргийлсэн унтраагууртай бол түүнийг идэвхжүүлнэ;

б/ шинжилгээнд хүргэж өгөхөөс өмнө дижитал файлыг нээх, үзэхийг хориглоно;

в/ мэдээлэл шаардлагатай болсон үед тухайн хураан авсан цахим хэрэгсэлд байгаа мэдээллийг зохих хэрэгсэлд хуулбарлан авах хүсэлт тавина;

г/ 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 хадгална;

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

е/ эвдэрч, гэмтэхээс урьдчилан сэргийлсэн зориулалтын битүүмжлэл бүхий хайрцаг, савand хадгалах ёстой.

Судлаач Ц.Болор-Эрдэнэ “Мөн журмын 5 дугаар зүйлд холбооны хэрэгсэл хураан авах журмыг зааж өгсөн ба үүрэн болон суурин телефон, эсхүл бусад төхөөрөмжүүдийг хураан авахдаа түүний дотор хадгалагдаж байгаа бүх төрлийн мэдээллийг арилгах, устгах, гэмтэхээс сэргийлэх зорилгоор дор дурдсан журмыг баримтална гэжээ. Үүнд:

а/ 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;

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

в/ 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.

Энэ кодын 7 дугаар зүйлд цахим мэдээлэл хадгалах хэрэгслийг тодорхойлж өгсөн ба дүрс,

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

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

б/ мемори болон бусад картыг шалгах болон хуулбарлаж болохгүй. Зөвхөн компьютерын мэргэжилтний тусламжтайгаар картад байгаа мэдээллийг боломжтой хэлбэрээр бэхжүүлнэ;

в/ 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;

г/ мэргэжилтний тусламжтайгаар хадгалах төхөөрөмж ашиглан мемори болон бусад карт дээрх мэдээллийг хуулбарлан авна;

д/ 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.

Тоон технологийн шинжилгээ (*Digital forensic) гэж юу вэ?*

Тоон технологийн шинжилгээ гэдэг нь ихэвчлэн 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.

Тоон технологийн шинжилгээ гэдэг ухагдахууныг саяхан болтол шүүх компьютер-техникийн шинжилгээ гэж ойлгож ирсэн бөгөөд компьютертой холбоотой бүх шинжилгээг үүнд хамруулж үздэг байв. Энэ нь тоон технологийн шинжилгээг тооллын системд ба программчлалын хэлний хөрвүүлэгчийн мэдээлэлд үндэслэн, санах ойд орсон өөрчлөлтөд их төлөв хийж, өөрчилсөн мэдээллийг өмнө ямар байсныг тогтоох зорилго агуулдаг байсантай холбоотой. Тоон технологи дээр суурилсан төхөөрөмжүүд, тоон технологийн хөгжлийн явцад энэ хандлага өөрчлөгдөж,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 орчинд хийх шинжилгээ, онлайн хост үйлчилгээнд хийх шүүх шинжилгээ.

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 шинжилгээ.

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 төхөөрөмжүүдэд (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 адилтгал хийх шүүх шинжилгээ.

Тоон(digital) нотлох баримтын хэлбэр:

Тоон нотлох баримт гэдэг нь компьютер болон дижитал мэдээлэл хадгалагч төхөөрөмжид хадгалагдаж байгаа болон компьютерын сүлжээгээр дамжиж буй цахим мэдээллээс гэмт хэрэг мөрдөх, нотлох ажиллагаанд шаардлагатай нотлох баримт болохуйц мэдээллийг хуульд заасан үндэслэл, журмын дагуу тусгаарлан авч, шинжлэх ухааны үндэслэлтэй аргачлал дээр суурилан дүн шинжилгээ хийж байгаа мэдээллийг хэлнэ. Тоон нотлох баримтыг тоон мэдээлэл үүссэн нөхцөл байдлаар хэд хэд ангилдаг.

Эх тоон нотлох баримт** (Original Digital Evidence)**:

Анхдагч тоон мэдээлэл үүсгэгдэн хадгалагдаж байгаа биет төхөөрөмжийг эх тоон нотлох баримт гэж нэрлэнэ. Анхдагч тоон мэдээлэл гэж аливаа төхөөрөмжийн санах ойд анх үүсгэсэн тэр хэвээр, ямар нэг өөрчлөлт оруулаагүй хадгалж байгаа мэдээллийг хэлнэ.

Хувилж авсан тоон нотлох баримт *(Duplicate Digital Evidence)**:***

Анхдагч тоон мэдээлэл үүсгэгдсэн биет төхөөрөмжид агуулагдаж байгаа бүх мэдээллийг тусгай зориулалтын төхөөрөмж болон программ хангамжийн тусламжтайгаар хувилж авсан мэдээллийг хэлнэ. Техникийн үзүүлэлтийн хувьд энэ хувь эх хувьтайгаа яг адил.

Хуулбарлаж авсан тоон нотлох баримт *(Copy Digital evidence):*

Анхдагч тоон мэдээлэл үүсгэгдсэн төхөөрөмжид агуулагдаж байсан мэдээллийг бүхэлд нь болон түүнээс хэсэгчлэн хуулбарлаж авсан, анхдагч тоон мэдээлэл үүсгэгдсэн төхөөрөмжөөс тусдаа /ангид, бие даасан г.м/ мэдээллийг хэлнэ. Техник үзүүлэлтийн хувьд энэ хувь эх хувьтайгаа яг адил боловч хэсэгчлэн хуулбарлах үед хэрэгцээгүйг орхиж, зөвхөн шаардлагатай гэж сонгож авсан мэдээллийг оруулснаараа ялгагдана.

<u>Тоон нотлох баримтын онцлог[40]:</u>

Хэврэг: Компьютерын сүлжээгээр боловсруулсан зарим цахим өгөгдөл маш хэврэг бөгөөд амархан устаж өөрчлөгддөг. Үүнийг цахим нотлох баримтыг цуглуулах үед онцгой анхаарах нь зүйтэй. Өгөгдөл зөвхөн RAM, сүлжээний санах ойд хадгалагдах бөгөөд урьдчилан сэргийлэх техникийн тусгай арга хэмжээ аваагүй бол сүлжээ гэмтэх буюу унтрах аюултай сүлжээний санах ойд хадгалагдсан мэдээлэл мөрдөн шалгах үйл ажиллагаанд маш чухал бөгөөд ийм нотлох баримтыг цуглуулах технологи нь уламжлалт нотлох баримтыг цуглуулах ажиллагаанаас ялгаатай.

Хувиргахад амархан: Цахим өгөгдлийг хувиргах буюу өөрчлөхөд амархан байдаг. Компьютерын шинжилгээний хамгийн суурь зарчмын нэг бол цахим нотлох баримтын бүрэн бүтэн байдлыг хадгалах юм. Компьютерын өгөгдлийг бүрэн бүтэн байдлыг хадгалах аргыг хэрэглэх, зохих бичиг баримтыг бүрдүүлэх нь мөрдөн байцаагчийн хувьд нотлох баримтыг цуглуулах, бэхжүүлэх талаар хуульд заасан журмыг баримтлаагүй буюу зөрчсөн гэх асуудлаар сэжигтний зүгээс гомдол гаргахаас зайлсхийхэд чухал юм.

Тархан байршсан: Өргөн зурвасын хүртээмж, серверт зайнаас хадгалах боломж нь мэдээлэл хадгалах арга замд нөлөөлсөн. Өмнө нь мөрдөн байцаагчдын хувьд сэжигтний орон байранд төвлөрч компьютерын өгөгдлийг хайж болдог байсан бол одоо цагт тэдний хувьд тоон мэдээллийг хилийн чанадад хадгалагдаж, шаардлагатай бол сэжигтэн зөвхөн алсаас хандаж болно гэдгийг анхаарч үзэх шаардлагатай болсон.

Техникийн дэвшлийн хурд: Техникийн дэвшлийн хурд асар хурдацтай хөгжиж байна. Энэ нь криминалистикийн шинжилгээнд шинэ сорилтыг бий болгож байна. Ийм хөгжил нь

[40] Marco Gercke, Project on Cybercrime, Council of Europe. Cybercrime training for judges: Training manual (draft). 2010. p.67

нотлох баримт цуглуулах үүрэгтэй хүмүүсийг сургах, түүнчлэн одоогийн криминалистикийн шинжилгээний багаж, хэрэгслийг шинэчлэхийг шаардаж байна. Үйлдлийн систем болон бусад программ хангамжийн бүтээгдэхүүн шинэ хувилбарууд мөрдөн шалгах үйл ажиллагаанд холбоотой янз бүрийн мэдээлэл, өгөгдөл бий болгож байна. Иймд дэвшил программ хангамжаас гадна техник хангамж хамаарах болов.

Мэдээллийн технологитой холбоотой хэрэгт криминалистикийн мөр судлал, гарын мөрний зэрэг уламжлалт шинжилгээнээс гадна компьютер техникийн шинжилгээ томилдог.

Тоон систем дээр суурилсан төхөөрөмжид шинжилгээ хийхтэй холбоотой харилцааг Шүүхийн шинжилгээний тухай хуулийн холбогдох зүйлүүдээр зохицуулж байгаа ба харин энэ төрлийн шинжилгээнд нотлох баримт бүрдүүлэхдээ ШШҮХ-ийн захирлын 2017 оны 02 дугаар сарын 08-ны өдрийн А/02 тоот тушаалаар баталсан “Хэргийн газрын үзлэгээр илрүүлж, бэхжүүлсэн ул мөр, эд мөрийн баримтыг савлах, битүүмжлэх, хаягжуулах, бүртгэх журам”, Улсын прокурорын газрын 2017 оны 07 дугаар сарын 16-ны өдрийн №А/80 дугаар тушаалаар баталсан “Эрүүгийн хэрэгт хөрөнгө, орлого, барьцааны мөнгө, эд мөрийн баримт, эд зүйлийг хураан авах, бэхжүүлэх, хүлээн авах, хадгалах, хамгаалах, шилжүүлэх, шийдвэрлэх журам, ЦЕГ-ын даргын 2010 оны 9 дүгээр сарын 29-ний өдөр баталсан үйл ажиллагааны журмын код №225, “Компьютерын болон цахим эд мөрийн баримтыг хураан авах” зэрэг эрх зүйн актаар зохицуулж байна.

Кибер гэмт хэргийг мөрдөн шалгах ажиллагааны тактик арга зүй

Кибер гэмт хэргийг мөрдөн шалгах анхан шатны ажиллагаанд 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 хойшлуулшгүй тохиолдолд 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.

Үзлэгийн 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[41] ангилсан байдаг.

Мөн үүн дээр гэмт хэрэг үйлдэхэд ашигласан компьютер, тусгай төхөөрөмжүүд хамаарч болно.

Үзлэг эхлэхийн өмнө бэлтгэл ажлыг сайтар хангасан байх хэрэгтэй. Тухайн ажиллагаанд оролцох мэргэжилтэн, техник хэрэгсэл, үзлэг хийх объектын 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 мөрдөгч, шинжээч криминалист, дүрс бичлэг хийх алба хаагчийг зайлшгүй бэлтгэн үзлэгийн онцлогийг тайлбарлан өгнө.

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 оролттой 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;

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 программ хангамж, тоног төхөөрөмж.

5. Тухайн компьютер, төхөөрөмжтэй холбож мэдээлэл авахад хэрэглэх холбогч кабель утаснууд, зөөвөрлөхөд шаардлагатай уут, цаасан хайрцаг г.м.

Үзлэгийг эхлэхийн өмнө дараах зүйлийг анхаарна. Үүнд:

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

[41] Дворкин А.И и др. Тактика следсвенних дейсвий. Москва. 2011 г, С502.

2. Тухайн үзлэг хийх компьютер, мэдээллийг хадгалж байгаа төхөөрөмжид шаардлагатай нууц үгийг хийхгүй байх, эсвэл тодорхой хугацааны дотор нууц товчлуур дарах, эсвэл 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 суурилуулсан эсэхийг эхлээд нарийвчлан шалгах,

4. Төхөөрөмжид гадны биет /зөөврийн санах ой, холбогч утас г.м/ холбогдсон байгаа эсэх, тийм бол түүний шинж байдлыг тодорхойлох зэрэг болно.

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 программ хангамжийг суулгасан эсэхийг шалгаж, суулгасан тохиолдолд тухайн төхөөрөмжийг сүлжээнээс салгаж, тоон ул мөрийг хамгаалах арга хэмжээг тухайн нөхцөл байдалдаа уялдуулан зайлшгүй авах хэрэгтэй. Нөгөөтээгүүр гэмт этгээдэд дээрх төрлийн программ хангамжийг ашиглах нөхцөл боломжийг зориудаар хэвээр үлдээн мөрдлөгийн ажиллагааг үргэлжлүүлэх нь зарим тохиолдолд илүү үр дүнтэй байхыг үгүйсгэх учир тухайн нөхцөл байдалдаа үнэлэлт дүгнэлт өгч зөв шийдвэр гаргах шаардлагатай.

Үзлэгээр тогтоох нөхцөл байдал:

- Компьютерыг нүүрэн ба ар талаас нь, ялангуяа бусад төхөөрөмжтэй холбогдсон холболтын зургийг авах. Интернэт 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 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;

- 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 унтраалгын 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 шалгаснаас тухайн этгээд “USB” төхөөрөмж ашиглан давхар үйлдлийн систем ашиглаж байгаа эсэхэд үнэлэлт дүгнэлт хийх боломжтой. Түүнчлэн /live boot/ тухайн төхөөрөмж дээр давхар Кибер компьютер суулгасан эсэхийг нягтлан /VMWARE/ үзсэний эцэст тэмдэглэлийг энэхүү дарааллаар үйлдэнэ.

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 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 компьютерын 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 мэдээллүүдийг хуулбарлуулан авч тухайн хэргийн онцлогт тохирсон үзлэгийг явуулна. Боломжтой бол тухайн үзлэгийг дүрс бичлэгийн төхөөрөмжөөр 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 бичин, 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 интернэт сайтуудаар орсон, ямар шинэ программ татаж суулгасан,

ямар сүлжээ ашигладаг болох[42], 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 оффис, албан байгууллагын хамгаалалт зэргийг тодруулан дэлгэрэнгүй мэдүүлэг авна.

Мөн тухайн гэрч, хохирогчийн хувийн байдлыг, ялангуяа техникийн мэдлэгийн талаарх мэдээллийг дэлгэрэнгүй судлан үзэж, гэмт хэрэг 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 объектын талаарх дэлгэрэнгүй мэдээлэл, уг газар телефон болон интернэт 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[43].

Шинжээч томилох. Тоон технологийн шинжилгээ гэдэг нь ихэвчлэн кибер гэмт хэрэг мөрдөх явцтай холбоотойгоор, тоон технологи дээр суурилсан төхөөрөмжийн санах ойд

[42] О.А. Егерева “Некоторые вопросы методики расследования киберпреступлений” журнал «Государство и право. Юридические науки»
[43] Будилов А.М. “Киберпреступления: криминалистическая характеристика и особенности расследования” Вологда – 2016г. С57.

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 орчинд хийх шинжилгээ, онлайн хост үйлчилгээнд хийх шүүх шинжилгээ.

- 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 адилтгал хийх шүүх шинжилгээ[44].

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, мэйл, 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 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[45].

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

[44] Ц.Болор-Эрдэнэ. “Тоон технологийн шинжилгээ”. Уб., 2019 он. 45 дахь тал.
[45] ЦБҮАЖ КОД-226

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 битүүмжилж хүргүүлнэ[46].

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?

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

5. Тухайн компьютерын хүчин чадал нь өөрт нь суулгасан программ хангамжуудыг ачаалан 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 XXX 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

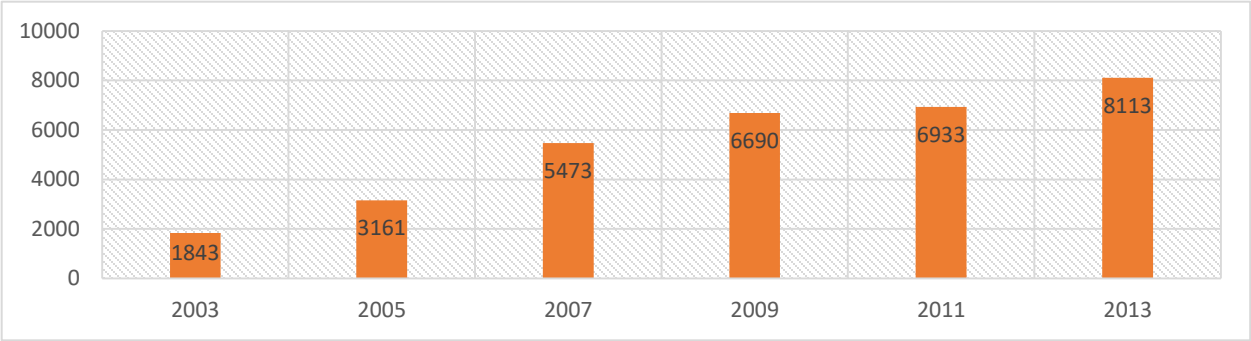
Шинжээчид тавих асуултыг тухайн хэргийн онцлогоос шалтгаалан сонгож тавих нь хурдан шуурхай шинжилгээ явуулах ач холбогдолтой байдаг.

ГУРАВДУГААР БҮЛЭГ. КИБЕР ОРЧИНД ҮЙЛДЭГДЭЖ БАЙГАА ГЭМТ ХЭРГЭЭС УРЬДЧИЛАН СЭРГИЙЛЭХ АРГА ЗАМ

§3.1. Гадаадын зарим улс, орны кибер аюулгүй байдлыг хангах, гэмт хэргээс урьдчилан сэргийлж буй туршлага

Дэлхий дахинд уламжлалт гэмт хэргүүд интернэт орчинд идэвхтэй шилжих чиг хандлага бий болж интернэт гэмт хэргийн төрөл, хэлбэрүүд хэдийн бий болж даяарчлагдаж эхэлсэн.

Зураг.4 Япон улсын Кибер аюулгүй байдлын эсрэг гэмт хэргийн тоон үзүүлэлт



Япон улсад үйлдэгдсэн гэмт хэрэг 2013 оны байдлаар цахим луйвар 12%, хүүхдийн порнограф 14%, хүүхдийн биеийг онлайнаар үнэлүүлсэн 6%, зохиогчийн эрх зөрчсөн 9%, онлайн болзооны хууль зөрчсөн 9%, онлайн худалдааны хууль зөрчсөн 2%, компьютерын мэдээллийн санд халдсан 6% тус тус эзэлж байна.

Америкийн Нэгдсэн Улс

Америкийн Нэгдсэн Улс нь 2003 онд нийтэлсэн анхны үндэсний кибер аюулгүй байдлын стратеги болох "Аюулгүй кибер орон зай" баримт бичгээрээ интернэт, компьютерын салбарт технологийн олон хөгжлийг тэргүүлж, түүнийг хөгжүүлэхэд шаардлагатай суурийг бэлтгэж байна.

2003 онд хэвлэгдсэн энэхүү баримт бичгээс гадна кибер аюулгүй байдлын бодлогын талаарх бусад баримт бичгүүдийг 2011, 2013, 2015 онуудад нийтэлсэн. 2011 онд хэвлэгдсэн кибер аюулгүй байдлын стратегийн баримт бичиг нь стратегийн таван тэргүүлэх чиглэлээс бүрдэнэ. Үүнд: Батлан хамгаалах салбарын зохион байгуулалтын хөгжил, батлан хамгаалахын шинэ агуулгатай болох, төр, хувийн хэвшлийн хамтын ажиллагаа, бусад улс оронтой бат бэх харилцаа тогтоох, бүтээлч байдлыг нэмэгдүүлэх зэрэг багтана.

АНУ-ын кибер аюулгүй байдлын стратегийг чухал дэд бүтцийн эсрэг кибер халдлагаас урьдчилан сэргийлэх, кибер халдлагын эсрэг үндэсний аюулгүй байдлын эмзэг байдлыг бууруулах, кибер халдлагаас учирч болох хохирлыг багасгах гэсэн гурван үндсэн сэдвийн дор үнэлж болно.

Кибер аюулгүй байдал, дэд бүтцийн аюулгүй байдлын агентлаг (CISA)-ийн дэргэдэх Үндэсний Эрсдэлийн Удирдлагын Төв (NRMC) нь улс орны чухал дэд бүтцэд учирч болох хамгийн чухал эрсдэлүүдийг тодорхойлж, эдгээр эрсдэлийн менежментийг удирдан чиглүүлдэг. CISA нь кибер довтолгооноос хамгаалах, чадавхыг сайжруулах, нийтлэг оролцогч талууд болон байгууллагуудын үндсэн чиг үүргийг дэмждэг ".gov" сүлжээг хамгаалахын тулд кибер аюулгүй байдлын хэрэгсэл, ослын хариу үйлчилгээ, үнэлгээний чадавхыг хангах зорилгоор холбооны засгийн газартай хамтран ажилладаг.

Холбооны Бүгд Найрамдах Герман Улс

2005 оноос хойш Германы засгийн газар кибер аюулгүй байдлын стратегиа байнга шинэчилж ирсэн. 2018 оны хамтарсан Засгийн газрын хэлэлцээр нь судалгаа, боловсруулалт, мэдээллийн технологийн бүтээгдэхүүний аюулгүй байдлыг сайжруулах чиглэлээр одоо байгаа үйл ажиллагааны чиглэлийг нөхөх хэд хэдэн үйл ажиллагааны чиглэлийг үндсэндээ тодорхойлсон.

Мэдээллийн технологийн аюулгүй байдлын чиглэлээр судалгаа, хөгжүүлэлтийг хөгжүүлэх, чадамжийн төвүүдийг бий болгох, аюулгүй цахим үнэмлэх, төгсгөл хүртэлх шифрлэлтийн шийдлүүдийг иргэдэд илүү хялбар хүртээмжтэй болгохыг хичээж байгаа юм.

Байгууллагын үүднээс авч үзвэл, энэ нь кибер аюулгүй байдал дахь аж үйлдвэр болон төрийн байгууллагуудын найдвартай хамтын ажиллагааг дэмжихийн тулд аж үйлдвэртэй шинэ кибер холбоо байгуулах зорилготой юм.

Франц Улс

Франц улс 2008 онд тус улсад тулгарч буй аюул заналыг тодорхойлж, энэ аюулыг даван туулахын тулд батлан хамгаалах, үндэсний аюулгүй байдалд шаардлагатай чадавхыг тодорхойлоход туслах Цагаан ном хэрэгтэй гэж шийдсэн. Үндэсний дэд бүтцэд кибер халдлагад өртөх эрсдэл нь ойрын арван таван жилийн хамгийн том аюул заналхийллийн нэг гэдгийг онцлон 2008 оны Цагаан номд ийм халдлагын тус улсад үзүүлэх нөлөөллийн цар хүрээг анхаарч тусгаж эхэлжээ. Мэдээллийн нийгэм хөгжиж, төр, нийгмийн мэдээллийн технологийг өргөнөөр ашиглахын хэрээр бидний хараат байдал байнга нэмэгдэж байгааг Цагаан номд онцлон тэмдэглэжээ.

2008 онд хэвлэгдсэн “Цагаан ном”-д улсыг кибер халдлагаас урьдчилан сэргийлэх, хариу арга хэмжээ авах чадавхыг хөгжүүлж, үүнийг үндэсний аюулгүй байдлын агентлагийн нэн тэргүүний зорилт болгохыг уриалсан. Тодруулбал, кибер хамгаалалтын салбарт кибер халдлагыг эрт илрүүлж, аливаа байгууллага хамгийн энгийнээс эхлээд өргөн цар хүрээтэй олон төрлийн халдлагыг эсэргүүцэх чадварыг онцлон тэмдэглэв.

Францын Үндэсний Кибер Аюулгүй байдлын Агентлаг (ANSSI) нь батлан хамгаалах, үндэсний аюулгүй байдлын талаарх Цагаан номд гарсан зөвлөмжийн дагуу байгуулагдсан.

ANSSI-г үүсгэн байгуулах зарлигаар кибер аюулгүй байдлын стратегийн хороог үндэсний кибер аюулгүй байдлын стратегийг санал болгох зорилгоор байгуулсан.

2017 оны 12-р сарын 15-нд Гадаад хэргийн сайдын танилцуулсан Францын олон улсын дижитал стратеги нь засаглал, эдийн засаг, аюулгүй байдал гэсэн гурван үндсэн чиглэлд төвлөрч байна. Энэхүү загвар нь өнөөгийн хэрэглээний талбарт бидний харж буй сегментчилэл, сүлжээг хянах, тогтворгүйжүүлэх чиг хандлагыг эсэргүүцдэг. Мөн Америк, Хятадын томоохон технологийн фирмүүдийн хэрэгжүүлж буй загвараас ялгаатай нь үндсэн эрхийг хүндэтгэх, шударга өрсөлдөөн, татварыг дэмжих замаар илүү хамгаалалтыг хангах зорилготой юм.

Англи Улс

2011-2015 оныг хамарсан Их Британид кибер аюулгүй байдлын үндэсний стратеги анх удаа 2011 онд хэвлэгдсэн. Энэхүү стратегийн баримт бичгийг улс орны дөрвөн үндсэн зорилтод нийцүүлэн боловсруулсан. Энэ нь кибер гэмт хэрэгтэй тэмцэх, кибер довтолгоонд илүү тэсвэртэй байх замаар цахим ертөнц дэх улс орны эрх ашгийг хамгаалах, олон нийт итгэлтэйгээр ашиглах нээлттэй, тогтвортой, эрч хүчтэй цахим орон зайг бүрдүүлэхэд тус дөхөм үзүүлэх замаар Их Британи улсыг кибер орон зайд ажиллах дэлхийн хамгийн аюулгүй газруудын нэг болгох мөн нээлттэй нийгмийг дэмжиж, кибер аюулгүй байдлын бүх зорилгыг хэрэгжүүлэхэд шаардлагатай нийтлэг мэдлэг, ур чадвар, чадвартай байхыг дэмждэг байна.

Энэхүү стратеги нь чухал дэд бүтцэд, ялангуяа харилцаа холбооны салбарт илүү их анхаарал хандуулдаг. Энэ салбарын зорилго нь юуны түрүүнд аж үйлдвэр, ялангуяа Харилцаа холбооны үйлчилгээ үзүүлэгч нартай хамтран ажиллаж, Их Британийн интернэтийн үйлчилгээ, хэрэглэгчдэд халдлага үйлдэхээс урьдчилан сэргийлж, тус улсад удаан хугацаагаар нөлөөлөх халдлагын магадлалыг эрс бууруулахад чиглэгддэг.

Үүний нэгэн адил бусад зорилтуудад төрийн систем, сүлжээний хамгаалалтыг сайжруулах, үндэсний чухал дэд бүтцийн хангамжийн сүлжээнд илүү аюулгүй байдлыг бий болгоход туслах, программ хангамжийн экосистемийг илүү найдвартай болгох, төрийн онлайн үйлчилгээг иргэдэд автоматжуулсан хамгаалалтаар хангах зэрэг орно.

Япон Улс

2000 оны 1-р сард Японы засгийн газар кибер аюулгүй байдлыг бодлогын чиглэл болгон тодорхойлж, эхний алхамдаа "Мэдээллийн системийг кибер халдлагаас хамгаалах үйл ажиллагааны төлөвлөгөө"-г нийтэлсэн. 2000 оны дунд үеэс кибер аюулгүй байдлын асуудлыг стратегийн хувьд нарийвчлан шийдвэрлэх хоёр чиглэлтэй бодлогын арга барилыг эхлүүлж, эхний ээлжид засгийн газрын дотоод мэдээллийн технологийн аюулгүй байдлыг хангах, хоёр дахь шатанд зөвхөн чухал дэд бүтцийн хамгаалалтыг хангах зорилготой байв.

Энэхүү давхар төвлөрсөн стратегийг тасралтгүй хөгжүүлж, шинэ институцуудыг бий болгож, мэдээлэл солилцох шинэ арга замууд, мэдээллийн аюулгүй байдлын шинэ стратеги, зохицуулалтаар дэмжигдсэн.

2014 онд Японд анх удаа Кибер аюулгүй байдлын хуулиар "кибер аюулгүй байдал" гэсэн нэр томьёог хуульчилсан. Тус хуулиар мэдээлэл алдагдах, гэмтэх аюулаас урьдчилан сэргийлэх, мэдээллийг найдвартай хадгалах, гэмт хэргээс урьдчилан сэргийлэх арга хэмжээ авах зэрэг үйл ажиллагааг зохицуулжээ.

Япон дахь кибер аюулгүй байдал нь хувийн мэдээллийг хамгаалахтай салшгүй холбоотой юм. 2019 онд Европын холбооны Комисс Япон улсын талаар зохих шийдвэр гаргаж, "хүчтэй хамгаалалтын баталгааны үндсэн дээр хоёр улсын эдийн засгийн хооронд хувийн мэдээлэл чөлөөтэй шилжих" боломжийг олгосон. Энэхүү шийдвэрийн дагуу дэлхийн хамгийн том аюулгүй мэдээллийн урсгалын домэйн бий болсон.

Бүгд Найрамдах Хятад Ард Улс

1980-аад оны сүүлээр БНХАУ-д кибер аюулгүй байдлын талаарх албан ёсны төлөвлөгөө олны анхаарлыг татсан. Мэдээллийн технологийн талаарх үндэсний хэмжээний анхны албан ёсны санаачилгыг 1986 онд "Улсын эдийн засгийн мэдээллийн удирдлагын тэргүүлэгч жижиг бүлэг"-ийг үүсгэн байгуулж байжээ. 1999, 2001 онуудад гарсан шийдвэрүүдээр “Төрийн мэдээлэл зүйн манлайллын бүлэг”-ийг байгуулсан. Дараа нь 2003 оноос “Засгийн газрын сүлжээ, мэдээллийн аюулгүй байдлыг зохицуулах жижиг бүлэг” ажиллаж эхэлсэн.

Эдгээр бүлгүүдийн гол зорилго нь Хятадын мэдээллийн технологийн салбарын хөгжил, Хятадын засгийн газрын дэлхийн өрсөлдөх чадварыг нэмэгдүүлэхэд богино болон дунд хугацаанд мэдээлэл, сүлжээний технологийн гүйцэтгэх үүргийг тодорхойлох явдал байв.

Сансрын технологиос үүссэн шинжлэх ухааны дэвшлийг кибер аюулгүй байдлын салбарт шинэ санаачилга гаргаснаар цэргийн хүчин чадлаа сайжруулах шинэ боломж гэж үзэж буй Хятадын засгийн газар сансрын технологийн салбарт кибер чадавхыг хөгжүүлэх алхмуудыг хийжээ. Энэ хүрээнд 2016 оны 12 дугаар сарын 27-ны өдөр Хятадын Кибер орон зайн албанаас нийтэлсэн “Үндэсний кибер аюулгүй байдлын стратеги” баримт бичигт кибер орон зай нь улс орны аюулгүй байдалд шинэ аюул занал учруулж болзошгүй бүс нутаг гэдгийг онцолжээ.

Бүгд Найрамдах Турк Улс

Цахим гэмт хэрэг, өөрөөр хэлбэл кибер гэмт хэрэгтэй тэмцэх нь бусад гэмт хэргүүдтэй тэмцэхээс ялгаатай. Учир нь кибер гэмт хэргийн тухай ойлголт нь нэлээд шинэ үзэгдэл бөгөөд гэмт хэрэг үйлдэх загваруудыг тогтоох маш хэцүү байдаг. Байнга хөгжиж, өөрчлөгддөг Кибер орчинд эрх зөрчигдсөн, гэмт хэргийн эсрэг шийтгэл ногдуулахад хориг арга хэмжээний тасралтгүй байдал, өөрчлөлтөд дасан зохицох шаардлагатай байна.

Энэ бүхнээс гадна гэмт хэргийг тодорхойлоход хүндрэлтэй бөгөөд гэмт хэрэг үйлдэгч, хохирогч хоёрын хооронд цаг хугацаа, орон зайн хувьд зайг тодорхойлох боломжгүй.

Техникийн хувьд кибер гэмт хэрэгтэй тэмцэх бодлого, стратегийн үндсэн элементүүд нь; Цахим гэмт хэрэгтэй тэмцэх чиглэлээр урьдчилан сэргийлэх арга хэмжээ авах, хууль тогтоомжийг тогтоох, хууль сахиулах тусгай алба, прокурорын тусгай алба байгуулах,

байгууллага хоорондын хамтын ажиллагааг хангах, хууль сахиулах, шүүхийн ажилтнуудыг сургах, төр, хувийн хэвшлийн хамтын ажиллагаа, олон улсын үр дүнтэй хамтын ажиллагаа, санхүүгийн мөрдөн байцаалт мөнгө угаах, залилан мэхлэх гэмт хэргээс урьдчилан сэргийлэх, хүүхдийг бэлгийн хүчирхийллээс хамгаалахад гол анхаарал хандуулж байна.

Эдгээр элементүүд нь цахим гэмт хэрэгтэй тэмцэх бодлогыг тодорхойлох, хэрэгжүүлэхэд нэгээс олон оролцогч харилцан уялдаатай үүрэг гүйцэтгэдэг болохыг харуулж байна.

§3.2. Кибер гэмт хэрэгтэй тэмцэх арга зүй

Кибер гэмт хэрэгтэй тэмцэхийн тулд эрх зүйн орчноос гадна, ёс зүй, соёлын дархлааг суулгах, мэргэшсэн хүний нөөцийг бэлтгэх, чадваржуулах хэрэгцээ, шаардлага бий болж байна.

Тухайлбал, хувь хүний болон хуулийн этгээдийн кибер аюулгүй байдлыг хууль, тогтоомжийн дагуу хамгаалах, зөрчигдсөн тохиолдолд гэмт хэргийг таслан зогсоох, хохирлыг барагдуулах, найдвартай хамгаалалтыг бүрдүүлэх зэрэг нь нэн тулгамдсан асуудал юм. Үүний зэрэгцээ хувь хүний урьдчилан сэргийлэх арга хэмжээг авах буюу цахим соёл, ёс зүйг түгээх, хувь хүн болгон кибр аюулгүй байдлаа хангахад анхаарах шаардлагатай.

Мөн кибер аюулгүй байдлын эсрэг гэмт хэргийг илрүүлэх, нотлох арга хэмжээг авахад энэ төрлийн гэмт хэргийг шалган шийдвэрлэх эрх бүхий албан тушаалтан, шинжээчдийг чадваржуулах шаардлага бий болж байна.

Компьютерын болон цахим эд мөрийн баримтыг шинжлэх шинжээч нар нь гол ач холбогдолтой субъект болох юм. Цахим шинжилгээ гэдэг нь хатуу диск, зөөврийн санах ой зэрэг цахим материал дахь кибер өгөгдлийг шалгаж, бодит ертөнц болон эдгээр мэдээллийн хоорондын хамаарлыг тогтоох замаар аливаа гэмт хэргийг нотлох тоон өгөгдлийг илрүүлэх үйл явц юм. Эндээс олж авсан гэмт хэргийг нотлох тоон мэдээллийг дижитал нотлох баримт гэж нэрлэдэг.

Кибер аюулгүй байдлын эсрэг гэмт хэргийн талаарх хамгийн үр дүнтэй эрх зүйн зохицуулалт бол 2001 оны 11 дүгээр сарын 23-нд Европын Зөвлөлийн Кибер гэмт хэргийн тухай конвенц гэж хэлж болно. Энэхүү конвенцын зорилго нь “Эрүүгийн нэгдсэн бодлого бүрдүүлэх, нийгмийг Кибер аюулгүй байдлын эсрэг гэмт хэргээс хамгаалах, ялангуяа шаардлагатай хууль тогтоомжийг батлах”, олон улсын хамтын ажиллагааг хөгжүүлэхэд чиглэж байна.

Ёс суртахууны үзэл баримтлалыг бүх нийтийн үнэт зүйлсийг илэрхийлэхэд ашигладаг. Ёс суртахууны зорилго нь хувь хүнийг нийгэмд бусадтай хамт амьдрахдаа ёс суртахууны үндэслэлтэй шийдвэр гаргах, бие даан оршин тогтнох чадвартай байхыг заах явдал юм. Энэ нь өнөөгийн нийгэмд кибер орчинд хамгийн их зөрчигдөж буй нөхцөл байдал болж байна.

Сошиал медиа дахь үйл ажиллагааг кибер ёс зүйн хүрээнд авч үзэх юм бол хүмүүс эдгээр нийгмийн сүлжээгээр дамжуулан дуу хоолойгоо хүргэж байна.

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 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[47]/ гэдэг нь мэдээллийн агуулгыг нуух, өөрчлөлт хийх, бусад этгээдүүд зөвшөөрөлгүй хандалт хийхээс сэргийлэх зорилгоор үндсэн өгөгдлийг хувиргах аргыг ашиглан “кибер 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

[47] ru.wikipedia.org

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 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 цэсээс ачааллаж болох ба мөн сонгогдсон файл, хавтасны 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[48]. Мөн уг программыг ШШҮХ-ийн Дүр зураг, дүрс бичлэгийн лабораториос хуулбарлан авах боломжтой талаар дурджээ.

Кибер гэмт хэргийг мөрдөн шалгах ажиллагаанд тулгамдаж буй асуудал

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

1. Дээрх төрлийн хэргийг мөрдөн шалгах ажиллагаа явуулах, хяналт тавих, шүүхээр эцэслэн шийдвэрлэх туршлага байхгүй,

2. Энэ хэрэгт мөрдөн шалгах ажиллагаа явуулах цахим мэдээллийн чиглэлээр өндөр мэргэшсэн эрүүгийн процессын мэдлэгтэй, чадамжтай мөрдөгчид дутмаг,

3. Цахим мэдээллийн хэрэгт хийх шинжилгээг бүрэн дүүрэн явуулах боломжгүй байдал,

[48] Ц.Болор-Эрдэнэ. "Тоон технологийн шинжилгээ". Уб.,2019 он. 63 дахь тал.

4. Цахим мэдээллийн хэрэгт мөрдөн шалгах ажиллагаа явуулах нэгдсэн стандарт байхгүй[49]

5. Олон улсын хамтын ажиллагаа дутмаг г.м.

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 орчныг ашиглан үйлдсэн залилах, далайлган сүрдүүлэх гэмт хэргийг л шийдвэрлэж байна.

Монгол Улсад үйлдэгдэж байгаа Кибер аюулгүй байдлын эсрэг 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 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[50] 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[51]. Тухайн гэмт хэргийг гадаад улсаас

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

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

[51] “Зууны мэдээ” сонин №165 /5872/

үйлдсэн тул “Эрх зүйн харилцан туслалцаа үзүүлэх” эрх зүйн орчныг бүрдүүлэх, тухайн улстай байгуулаагүй байгаа нь мөрдөн шалгах ажиллагааг явуулах боломжгүй болгодог.

ДҮГНЭЛТ

Өнөөгийн техник технологи нь хувь хүмүүсийн амьдралыг хөнгөвчлөхөөс гадна хянах, ажиглахад чиглэгддэг бөгөөд сошиал медиа соёл нь дижитал орчинд хяналтаа үргэлж нээлттэй байлгадаг. Нөгөөтээгүүр, олон нийтийн мэдээллийн хэрэгслээр хүмүүс өөрсдийн дагалдагчидтайгаа өдөр тутмын үйл ажиллагаагаа хуваалцсаны үр дүнд харилцаж, энэ мэдээллийн хэрэгсэлд интерактив функцийг нэмж өгдөг. Энэ байдал нь хүн хүссэнээрээ санаа бодлоо илэрхийлэх бодит орчин байхаас гадна хэлсэн үгэндээ хариуцлага хүлээх боломжгүй кибер орчинтой байдгаараа онцлог юм.

Судалгааны үр дүнгээс харахад сошиал медиа хэрэгслүүд хөгжиж, олшрохын хэрээр кибер гэмт хэргийн гаралт нэмэгдсээр байна. Энэ байдал нь олон нийтийн мэдээллийн хэрэгсэлд тавих хяналтыг хүндрүүлж, үүнтэй зэрэгцэн цахим ертөнцөд ёс зүйн зөрчил гарах нөхцөлийг бүрдүүлж байна. Олон нийтийн мэдээллийн хэрэгслээр харагдах байдал, хүртээмжийг нэмэгдүүлснээр хэрэглэгчдийг гэмт хэргийн шинэ аюул заналхийлэлд өртөмтгий болгож, гэмт хэргийн хохирогч болох боломжийг бий болгож байна.

Кибер гэмт хэргийн сөрөг үр дагаврыг бууруулах, таслан зогсоохын тулд тэдгээрийн мөн чанар, динамикийг ойлгох нь чухал юм. Энэ хүрээнд дижитал технологи хөгжихийн хэрээр сошиал медиа платформууд өргөжин тэлж, аюулыг эрсдлийг нэмэгдүүлж байна. Хэдийгээр дижитал ертөнцийг хамарсан эрх зүйн зохицуулалтууд өдрөөс өдөрт боловсронгуй болж байгаа ч кибер салбарт хурдацтай өөрчлөлт гарч байгаа нь эрх зүйн зохицуулалтыг хангалтгүй болгож байна.

Энэ тохиолдолд сошиал медиа хэрэглэгчдийн соёл, нийгмийн ухамсрын түвшнээс хамаарч өөр өөр ёс зүйн үнэлэмж гарч ирдэг бөгөөд өөрийгөө хянах нь "бичмэл" бус зохицуулалтаар хангагддаг. Харин интернэтэд нэвтрэхэд хялбар болсон өнөө үед ёс зүйн дүрмээр өөрийгөө хянах механизмыг бий болгох эдгээр дүрмийг нийгэмд сануулах зорилгоор олон нийтийн мэдээллийн хэрэгслээр сургалт явуулах шаардлагатай байна.

Энэ бүхний үр дүнд сошиал медиа хэрэглэгчдийн хуваалцсан мэдээлэл болон интернэтэд түгээж буй бусад мэдээлэл нууц биш гэдгийг харгалзан дижитал ертөнцөд хариуцлагатай байх нь чухал байна.

1. Кибер гэмт хэргийн гаралт нэмэгдэж байгаа нь Монгол Улсад кибер аюулгүй байдлыг хангах хууль эрх зүйн орчин хангалттай бүрдээгүй, энэ төрлийн гэмт хэрэг шалгаж шийдвэрлэх нэгдсэн арга зүй, ойлголтгүй зэрэгтэй шууд холбоотой.

2. Кибер орчинд үйлдэгдсэн гэмт хэргийг шалгах чадамж бүхий боловсон хүчин орон нутагт дутмаг байдагтай холбоотойгоор илрүүлэлт орон нутагт өсөөгүй байгаагаар тодорхойлогдож байна.

3. Мэдээллийн технологийн салбарын мэргэжилтний эдийн засгийн орлогын байдал төрийн албан хаагчийн цалингаас хэд дахин илүү байдаг. Ийм учраас салбарын мэргэшсэн мэргэжилтнүүд төрийн албанд орж ажиллах сонирхолгүй байдагтай холбоотойгоор мэргэшсэн албан хаагч дутагдалтай байгаа нь энэ төрлийн гэмт хэрэгтэй тэмцэхэд тулгамдаж буй үндсэн асуудлуудын нэг болжээ.

4. Манай улсын иргэдийн дийлэнх нь хэрэглэдэг төдийгүй бүртгэгдэж буй талбар болох Фейсбүүк /Facebook/ компани нь терроризм, хүний амь нас хохирох нөхцөл байдал бий болсон, хүүхдийн садар самуун, секс сүрдүүлэг, үндэстэн дамнасан зохион байгуулалттай гэмт хэрэг /хар тамхи, хүн худалдаалах, мөнгө угаах/ зэрэг тодорхой төрлийн цөөн хэргээс бусад хэрэгт мэдээлэл гарган өгдөггүй нь кибер орчинд үйлдэгдэж буй бусад гэмт хэргийг таслан зогсооход хүндрэл учруулдаг аж.

5. Энэ төрлийн гэмт хэрэгтэй тэмцэх дагнасан нэгж зөвхөн төвийн албадад байгуулагдсан нь улсын хэмжээнд чиг үүрэг хэрэгжүүлэхэд хүрэлцээ муу, дутагдалтай зохион байгуулалт болжээ.

6. Монгол Улсын баталсан кибер аюулгүй байдлын тухай хуульд дүн шинжилгээ хийж үзэхэд Үндэсний аюулгүй байдлын тухай хууль, “Монгол Улсын Үндэсний аюулгүй байдлын үзэл баримтлал”-д мэдээллийн аюулгүй байдлыг үндэсний аюулгүй байдлын нэг бүрэлдэхүүн хэмээн тодорхойлсон. Гэсэн хэдий ч кибер аюулгүй байдлын индексийн гол үзүүлэлт болох хууль эрх зүйн орчин бүрдээгүй, үндэсний кибер халдлага, зөрчлөөс сэргийлэх, хариу үйлдэл үзүүлэх чиг үүрэг бүхий байгууллага байхгүй, хамтын ажиллагаа дутмаг байсныг өөрчилж өгчээ.

7. Кибер аюулгүй байдлын эсрэг гэмт хэргийг ихэвчлэн мэдээллийн технологийн өндөр мэдлэг, чадвартай этгээд үйлддэг нь энэ төрлийн гэмт хэргийг илрүүлэхэд шаардлагатай боловсон хүчин дутмаг байдагтай холбоотойгоор илрүүлэх, шалгаж тогтоох ажиллагаанд сөрөг үр дагавар бий болгосоор байна.

8. Олон улсын гэрээ, конвенцод нэгдэн ороогүй учир салбарын нэр томъёог олон улсын түвшинд хэрэглэх бодит нөхцөл бүрдээгүй. Кибер орчинд үйл ажиллагаа явуулдаг иргэн, байгууллага бүрийн дотоод бүтэц хүний нөөцийн бүтэц нэг мөр төлөвшөөгүй. Мөн энэ төрлийн гэмт хэрэг, зөрчилтэй тэмцэх байгууллагын тогтолцоо, хүний нөөцийн асуудал, сургалт, урьдчилан сэргийлэх ажиллагаа, техникийн зэрэг асуудлууд бүрэн шийдвэрлэгдээгүй өдийг хүрчээ.

САНАЛ

Судалгааны үр дүн, түүний эцэст хийсэн дүгнэлтэд түшиглэн цаашид кибер гэмт хэргийн ойлголтыг тодорхой болгох, шалтгаан нөхцлийг тогтоох, урьдчилан сэргийлэх арга замыг тогтоох үүднээс тодорхой саналыг дараах байдлаар боловсруулаа.

1. Кибер аюулгүй байдлын эсрэг болон кибер орчинд үйлдэгдэж буй гэмт хэрэгтэй тэмцэх чиглэлээр эрх зүйн орчныг боловсронгуй болгох;
2. Энэ хүрээнд салбарын мэргэжилтнүүдийг оролцуулсан эрдэм шинжилгээний хурлуудыг тогтмол зохион байгуулж, тухай бүр практикт үүсэж буй хүндрэл бэрхшээлүүдийг шийдвэрлэх арга хэмжээ авах, шийдлийг боловсруулж хэвших;
3. Кибер аюулгүй байдлын эсрэг гэмт хэргийг мөрдөн шалгах, хянан шийдвэрлэхэд шаардлагатай нэгдсэн ойлголт, тусгай дэс дараалал бүхий процесс ажиллагааны стандарт боловсруулж мөрдүүлэх;
4. Энэ төрлийн гэмт хэрэгтэй тэмцэх боловсон хүчний цалин хангамжийг нэмэгдүүлэх замаар мэргэшсэн иргэдийг цагдаагийн байгууллагад урьж ажиллуулах боломжийг бий болгох арга хэмжээ авах;
5. Мэдээллийн технологийн салбар хурдацтай хөгждөгтэй уялдуулж алба хаагчдад сургалтыг тогтмол явуулах;
6. Гэмт хэрэгтэй тэмцэх чиг үүрэг бүхий албан хаагчдын энэ чиглэлийн сургалтын төлбөрөөс чөлөөлөх замаар боловсрол эзэмшүүлж, мэргэшүүлэх, мэргэшсэн албан хаагчдын тогтвор суурьшилтай ажиллах нөхцөлийг бүрдүүлэх арга хэмжээ авах. Энэ үйл ажиллагааг орон нутгийн гэмт хэрэгтэй тэмцэх чиг үүргийн алба хаагчдыг түлхүү хамруулах;
7. Олон улсын хамтын ажиллагааг нэмэгдүүлэхийн тул олон улсад баримтлагдаж буй хэм хэмжээний акт, гэрээ, конвенцуудад зохих журмын дагуу нэгдэн орох;
8. Үндэсний хэмжээнд кибер орчинд зохистой хэрэглээг төлөвшүүлэх, сошиал орчин дахь хүний эрхийн зөрчил болоод гэмт хэргийг таних чадамж олгох, түүнээс урьдчилан сэргийлэх, авч хэрэгжүүлэх арга хэмжээний талаар сургалтыг байнга тогтмол явуулж байх зэрэг болно.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

Нэг. Хууль тогтоомж.

1. Кибер аюулгүй байдлын эсрэг гэмт хэргийн тухай конвенц, Будапешт хот, 2001 он,

2. Монгол Улсын Эрүүгийн хууль /Шинэчилсэн найруулга/, 2015 он,

3. Монгол Улсын Эрүүгийн байцаан шийтгэх хууль, 2002 он,

4. Монгол Улсын Шүүхийн шинжилгээний тухай хууль, 2010 он,

5. Криминалистикийн шинжилгээ хийх журам, 2010 он,

6. Монгол Улсын Ерөнхий прокурорын 2017.07.16-ны өдөр А/80 тушаал,

7. Цагдаагийн байгууллагын үйл ажиллагааны журам-226.

Хоёр. Сурах бичиг, гарын авлага.

1. Батзориг.Ч. Кибер орчин дахь гэмт хэргээс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох эрх зүйн зохицуулалт /харьцуулсан судалгаа/, Уб., 2018 он,

2. Өсвөр үеийнхний цахим хэрэглээний өнөөгийн байдал" судалгааны тайлан, 2018 он,

3. С.Жанцан. "Монгол улсын Эрүүгийн эрх зүй" УБ, 2004 он,

4. OCED, Computer-Related Crime: Analysis of Legal Policy. Paris, 1986 он,

5. Хүрэл-Очир.Ц. Эрх зүй. No15. УБ.,2007он,

6. Галбаатар.Л. "Цахим эрх зүй"., УБ., 2010,

7. Галбаатар.Л. "Кибер аюулгүй байдлын эсрэг гэмт хэргийг шүүхэд хянан шийдвэрлэх"., УБ., 2015,

8. Баатархуяг.Н. "Мэдээлэл түүнийг олж цуглуулах шинжлэх"., УБ., 2013,

9. Жаргал.О. "Хакер"., УБ., 2006,

10. Хишигтогтох Б., Цогтбаяр Л; Сумъяацэрэн Д., "Цахим мэдээллийн орчинд үйлдэгдэх гэмт хэргийг мөрдөн шинжлэхүйн онол, арга зүйн үндэс" /Сурах бичиг/., УБ.,2015.

Гурав. Гадаад хэл дээрх эх сурвалж.

1. Akamai (2012). The state of the internet. Erişim tarihi: 20.04.2013, http://www.akamai.com/

2. Akdoğan, H. (2005). Çocuğun cinsel istismarı ve Türkiye'de çocuk cinsel istismarını önlemeye yönelik çalışmalar. Polis Bilimleri Dergisi, 7(1), 1-15.

3. Ballard, J. D., Hornik, J. G., &McKenzie, D. (2002). Technological facilitation of terrorism: Definitional, legal and policy issues. American Behavioral Scientist, 45(6), 989-1016.

4. Chen, T. ve Walsh, P. J. (2009). Guarding against network intrusions. Vacca, J. R. (Ed.)
5. Computer and Information Security Handbook (ss. 53-66). Morgan Kaufmann Publishers
6. Dimensional Research (2011). The risk of social engineering on information security: A survey of IT professionals. Erişim tarihi: 16.04.2013, http://www.checkpoint.com/ press/downloads/social-engineering-survey.pdf
7. Easttom, C. ve Taylor, J. (2011). Computer crime investigation and the law. Course Technology.
8. Goodrich, M. ve Tamassio, R. (2010). Introduction to computer security. Addison-Wesley.
9. Host Exploit (2013). World hosts report. Erişim tarihi: 23.04.2013, http:// www.hostexploit.com
10. Identity Theft Resource Center (2012). Knowing less and less about less and less. 23.04.2013,
11. Karagülmez, A. (2011). Bilişim suçları ve soruşturma-kovuşturma evreleri, Seçkin.
12. Kleiner, A., Nicholas, P. and Sullivan, K. (2013). Linking cybersecurity policy and performance, Microsoft Corporation, Measuring the Impact of Policy on Global Cybersecurity. Erişim tarihi: 03.04.2013, http://www.microsoft.com/en-us/ download/details.aspx?id=36523

Дөрөв. Интернэт орчин дахь эх сурвалжууд

1.https://prokuror.mn,

2. https://legalinfo.mn,

3. https://www.itgovernance.co.uk,

4. https://nli.gov.mn,

5. www.nifs.gov.mn,

6. www.police.gov.mn,

7. www.legalinfo.mн,

8. www.arnnet.com.au,

9. www.mongoltoli.mn,

10. www.slideshare.net,

11. www.mn.wikipedia.org,

12. www.e-book.must.edu.mn,

13. www.Bolor-toli.com.