Компьютерийн гэмт хэргээс үүдэлтэй эрсдэл, түүнээс сэргийлэх арга замууд

П.Оюунбилэг
МУИС-ийн ЭЗС-ийн багш, доктор (Ph.D), дэд профессор

Компьютерийг хүмүүс баримт бичиг боловсруулах, тооцоо тайлан гаргах зэрэг наад захын үйлдэл гүйцэтгэхэд ашиглахаас эхлээд хүний гараар бүтээгдэжгүй хамгийн нарийн зүйлүүдийг бүтээж, хамгийн эрсдэлтэй үйл ажиллагаануудыг ч компьютерийн системээр удирдаж байна. Иймээс компьютер гэмт хэрэгт ашиглагдах өндөр магадлалтай.

Компьютерийн гэмт хэрэг гэдэг нэр томьёо анх 1960 аад онд АНУ д гарсан бөгөөд «хэн нэг нь компьютерийг гэмт хэргийн зориулгоор ашиглах үйлдэл юм. Компьютерийн гэмт хэргээс үүдэлтэй дараах эрсдэлүүд гарч болно. Үүнд: компьютерт хор учруулах программуудаас үүдэх эрсдэл, хакер (Hacker), кракер (Cracker) уудын үйлдлээс үүдэх эрсдэл, садар самуун, хүчирхийллийг сурталчлахаас үүдэх эрсдэл, кибер терроризмийн ажиллагаанаас үүдэх эрсдэл гэх мэт.

Манай оронд компьютерийн гэмт хэрэг хэдийнээ бодит зүйл болжээ. Тухайлбал, 2005 онд нэр бүхий банкин дахь компаний данснаас программ зохиогч мэргэжилтэй хүмүүс их хэмжээний мөнгө сулжээний технологи ашиглан авсан явдал юм. Үүнтэй холбоотойгоор «Мэдээллийн аюулгүй байдлын үзэл баримтлал, эрх зүйн зохицуулалт» бага хурлыг Монгол Улсын Үндэсний аюулгүй байдлын зөвлөлийн ажлын албанаас санаачлан хуралдуулж зохих зөвлөмж гаргасан явдал юм. Энэ зөвлөмжинд олон асуудлыг авч үзсний дотор компьютерийн мэдээллийн аюулгүй байдлын чиглэлээр дагнан ажилладаг мэргэжлийн байгууллагатай болох саналыг гаргасан байна.

Компьютерийн гэмт хэргийн эрсдлээс сэргийлэх арга замууд:

Вирусийн эсрэг программ хангамжийг байнга ашиглах, шинээр гарч буй вирус, түүний хор хөнөөл ,хэрхэн сэргийлэх талаар байгууллага хүн бүрийг мэдээллээр хангах, хэвлэл мэдээллийн хэрэгслээр сурталчилгаа хийх;

Хууль бус программ хангамж аль болох ашиглахгүй байх, компьютерийн эрсдлийн менежментийн чиглэлээр нарийн мэргэшсэн мэргэжилтэн бэлтгэх,

Бага насны хүүхдүүдийг интернэт орчинд хяналттай, зөв сургах, хууль эрх зүйн заалтыг шинэлэг, дорвитой болгон өөрчлөх;

Улс оронд гарч буй компьютерийн гэмт хэргийн чанартай үйл явдлуудыг мэргэжлийн хүрээнд шүүн хэлэлцэж үнэлэлт дүгнэлт өгдөг нарийн мэргэшсэн комисстой болох, олон улсын түвшинд компьютерийн гэмт хэрэгтэй тэмцдэг арга туршлагаас байнга суралцах;

Байгууллага бүр сулжээний найдвартай аюулгүй байдлыг ханган, нөөц сулжээний шугамтай болох, сулжээний администраторааар мэргэжлийн өндөр түвшний хакерийн хэмжээний мэдлэгтэй хүмүүсийг ажиллуулж байх шаардлагатай байна.

Эрсдэл - энэ үг зах зээлийн харилцаанд орохоос өмнө бидэнд тийм ч чухал бус, ерөнхийдөө бидний үйл ажиллагаанд огт хамаагүй мэт санагддаг байсан. Хэн нэгэн, эсвэл аль нэг аж ахуйн байгууллага ямар нэгэн эрсдэлд орлоо гэж дуулддаггүй байсан юм. Гадаадын улс орнуудын, тэр дундаа ЗХУ-ын ном, сэтгүүлээс зарим нэг зүйл уншвал сонин болгож ярих төдийгээр өнгөрдөг байлаа.

Харин 80 аад оны сүүлчээс Монгол Улс зах зээлийн эдийн засагт шилжих шилжилтийн үе эхэлж, ардчилал, ил тод байдал, өөрчлөн байгуулалт зэрэг үг хэллэг бидний амьдралд орж ирсэнтэй эн зэрэгцэн эрсдэл (risk) гэдэг цоо шинэ бодит зүйл бидний үйл ажиллагаанд түрэн орж ирсэн билээ. Энэ үеэс хүмүүс эрсдлийн тухай ойлголтыг дуртай дургүй ч хүлээн авч, зарим нэг нь «шатах» гэдэг үгээр төлөөлүүлэн ойлгож, томъёолж байсан.

Тэгвэл тэр хүмүүст төдийлөн таатай бус санагддаг, нэг үгээр хэлбэл бидний айдаг «эрсдэл» нь чухам юу юм бол. Хамгийн

энгийн үгээр, ойлгомжтой илэрхийлбэл «Эрсдэл нь хүмүүс ямар нэг зүйлд хандахад, эсвэл түүнийг ашиглахад учирч болох аюул занал юм. »Эндээс үзэхэд эрсдэл маш өргөн хүрээтэй бөгөөд ер нь «хүн байж» байгаа цагт байж л байдаг ойлголт юм байна. Гэхдээ хүний хийж гүйцэтгэж байгаа аливаа үйлдэл, үйл ажиллагаа нь өөрийн мөн чанараас хамааран эрсдлийг их, бага хэмжээгээр дагуулдаг нь мэдээж хэрэг.

Эрсдлийн энэ өргөн хүрээтэй ойлголтоос бид энэ удаад компьютер, компьютерийн гэмт хэргээс үүдэх болон интернэтийн сүлжээ ашигласнаар үүсэх «аюул занал»-ын тухай ярилцах болно. Энэ «аюул занал» нь мэдээлэл, компьютер, интернэтийн глобал сүлжээний мөн чанараас хамааран үлэмж өндөр байдаг онцлогтой. Өөрөөр хэлбэл, хүмүүс компьютер болон интернэтийг өөрийн үйл ажиллагаанд өдөр бүр ашигласанаар эрсдлийг их хэмжээгээр дагуулж байдаг гэсэн үг юм.

Орчин үед компьютер, мэдээлэл, мэдээллийнсүлжээашиглахгүйбайгууллага, хамт олон гэж бараг үгүй болжээ. Тэрч бүү хэл Монгол Улсын засгийн газраас явуулж буй мэдээлэл, харилцаа холбооны технологийг дэмжих хөтөлбөрийн үр дүнд ойрын ирээдүйд айл өрх, хувь хүн бүрт тэдгээрийг ашиглах боломж илүү ойртох нь тодорхой болж байна. Энэ утгаараа эрсдэл нь хүн бүрт хамааралтай асуудал болох нь ээ.

Компьютерийн гэмт хэргийн эрсдэл

Хүн төрөлхтний агуу суут бүтээлүүдийн тоонд компьютерийг зохион бүтээсэн явдал зүй ёсоор ордог билээ. Компьютерийг хүмүүс баримт бичиг боловсруулах, тооцоо тайлан гаргах зэрэг наад захын үйлдэл гүйцэтгэхэд ашиглахаас эхлээд хүний гараар бүтээгдэшгүй агуу, хамгийн нарийн зүйлүүдийг бүтээж удирдахад ч ашиглах болжээ. Мөн компьютер дээр хамгийн нууц мэдээлэл боловсруулж, хадгалж, дамжуулж, хамгийн эрсдэлтэй үйл ажиллагаануудыг ч компьютерийн системээр удирдаж байна. Иймээс компьютер нь гэмт хэрэгт ашиглагдах өндөр магадлалтай.

Компьютерийн гэмт хэрэг гэдэг нэр томъёо анх 1960 аад онд АНУ д гарчээ. Энэ үеэс л дэлхий нийт компьютертай холбоотой гэмт хэрэг байж болохыг мэдэрч, энэ асуудлыг анхаарлын төвдөө байлгах болжээ. Компьютерийн гэмт хэргийн тодорхойлолтыг эрдэмтэн судлаачид олон янзаар өгсөн байдаг. Тухайлбал, Оросын эрдэмтэн А.Н.Караханьян «Компьютер нь хууль зөрчсөн үйлдлийн арга хэрэгсэл болсон байвал компьютерийн гэмт хэрэг гэнэ» гэсэн бол АНУ-ын судлаач Рональд Стэндлэр «Компьютерийн гэмт хэрэг нь хууль зөрчсөн санамсаргүй, эсвэл урьдчилан төлөвлөсөн үйлдэл байдаг» гэжээ. Эдгээрээс үзвэл компьютерийн гэмт хэрэг гэдэг нь «хэн нэг нь компьютерийг гэмт хэргийн зорилгоор ашиглах үйлдэл юм. »Үүнээс улбаалан компьютерийн гэмт хэргээс үүдэлтэй эрсдэл гарч болох юм. Энэ эрсдлийг доорхи байдлаар ангилан авч үзье. Үүнд:

* Компьютерт хор учруулах программуудаас үүдэх эрсдэл
* Хакер (Haker), кракер (Cracker) уудын үйлдлээс үүдэх эрсдэл
* Садар самуун, хүчирхийллийг сурталчлахаас үүдэх эрсдэл
* Кибер терроризмийн ажиллагаанаас үүдэх эрсдэл

Компьютерт хор учруулах программуудаас үүдэх эрсдэл

Компьютерийн программ нь түүний үйл ажиллагааг зориудаар зогсоох, хор хөнөөл учруулах зорилгоор бичигдсэн бол түүнийг хорлон сүйтгэгч программ гэнэ. Ийм төрлийн программуудад вирус (virus), ворм (worm), трожан хорс (trojan horse), системийн бөмбөг (logic bomb) зэрэг багтана.

Вирус - Компьютерийн анхны вирус 1970-аад оны эхэн үеэс бүтээгдэн тархсан байна. Эхэн үедээ хүмүүс дэлгэцэн дээрээ тэмдэгтүүд «явж» байхыг хараад дэлгэцээ эвдэрсэнд тооцож байсан бол зарим мэргэжилтнүүд компьютерийг хүн шиг

өвчилдөг юм байна гэсэн төөрөгдөлд ч орж байсан гэдэг. Гэвч энэ нь вирус гэгч, компьютерийг санаатайгаар «өвчлүүлдэг» гэмт хэргийн эхлэл байсан юм. Энэ үеэс эхлэн компьютерийн санах ой, удирдлагын программуудад нэвтэрч файлыг гэмтээх хангалттүй болгох, устгах, диск форматлах, дискний төхөөрөмжүүдийг ажиллагаагүй болгох, хатуу дискийг эвдэх зэрэг хор хохирол учруулагч вирусууд шил шилээ даран гарах болжээ.

Компьютерийн вирус гэдэг нь программ байдлаар дуудагдан ажилладаг, файлын эхлэл юмуу төгсгөл хэсэгт залгагддаг идэвхитэй код юм. Өвчилсөн файлаас эрүүл файлд дамжих замаар цааш түгдэг. Анх үүссэн үедээ вирус нь зөвхөн уян дискээр дамжин халдварлаж байсан бол орчин үед бүх төрлийн диск, сүлжээ, интернэт гэзд маш олон замаар тархаж байна.

Дэлхий дахинаа одоо 70 мянга орчим вирус бүртгэгдээд байгаа юм. Вирусийн эсрэг программ үйлдвэрлэгч томоохон компаниудын судалгаагаар вирусийн программууд нь дэлхий дахинд 2001 онд 13 тэрбум ам. доллар, 2002 онд 30 тэрбум ам доллар, 2003 онд 55 тэрбум ам долларын хохирол учруулжээ. Эндээс үзэхэд вирусийн хор хөнөөл жилээс жилд асар хурдацтай өсч байна. Ганцхан жишээ дурдахад 2000 оны 5 сард электрон шуудангаар дамжин халдварладаг 'I love you' нэртэй вирус Европ, Ази, Америкийн 20 гаруй оронд тархаж зөвхөн 5 сарын 6-ны өдөр л гэхэд 10 тэрбум долларын хохирол учруулсан байжээ. Тэр үедээ дэлхийг шуугиулсан энэ вирусын тухай мэдээллийн томоохон агентлагууд сэрэмжлүүлэг гаргаж Холбооны мөрдөх товчоо вирусыг тараасан Филиппин улсын иргэдийг илрүүлснээр уг гэмт хэргийг зогсоосон юм.

Ворм нь компьютерийн ажиллагааг удаашруулж, өгөгдөл дамжуулах хурдыг сааруулдаг, өт шиг хурдан үржиж хатуу дискний багтаамжийг дүүргэн ажиллах боломжгүй болгодог, сүлжээнд байнга оршин, түүгээр дамжин компьютерт халдварлаж байдаг онцгой төрлийн вирус юм. Ворм нь ихэвчлэн E-Mail-ээр дамжин тарж байгаа тухай 2004 онд дэлхий нийтэд мэдээлж байсан. Вормын хамгийн гол аюул нь өөрөө өөрийгөө хувилдаг, мөн вирусийн эсрэг программуудыг унтрааж чаддагт оршино. 90-ээд оны эхээр АНУ-ын нэгэн их сургуулийн оюутан Роберт Моррис анхны вормыг интернэтэд оруулсан байна.

Трожан хорс нь хэрэглэгчийн компьютерт нууц байдлаар суугаад, хэрэглэгч мэдэлгүйгээр түүнийг идэвхжүүлэх үед уг программ нь түүнийг бүтээсэн хууль бус үйлдэл хийгчийн компьютертэй холбогдон таны компьютерийг түүний гарт оруулдаг байна. Ингэснээр таны компьютер ямар ч хамгаалалтгүй болно. Трожан хорс нь вирус болон ворм шиг хувилагддаггүйгээрээ онцлогтой.

Системийн бөмбөг нь тодорхой хугацаа, эсвэл нөхцөл бүрдсэн үед вирусийг идэвхжүүлэх, компьютерийн эд ангийг эвдэх, файлуудыг устгах зэргээр хорлон сүйтгэх зориулалттай бүтээгдсэн програмууд юм. Ийм програмуудын нэг нь бидний сайн мэдэх Чернобыль нэртэй 4 сарын 26-нд идэвхждэг программ билээ.

Хакер (Haker), Кракер (Cracker) уудын үйлдлээс үүдэх эрсдэл

Орчин үед хакердах, кракердах гэдэг нэр томъёо дэлгэрч үүний цаана тэдгээр үйлдлийг хийж гүйцэтгэдэг өндөр мэргэшсэн хүмүүс байдаг болжээ. Хакерууд нь ихэнхдээ системийн найдвартай байдлыг шалгадаг, системийн цоорхой, логик алдааг олж чаддаг, учир шалтгааныг нь хялбархан илрүүлдэг байдлаараа өндөр мэргэшсэн программ зохиогчид байдаг. Тэдний гол зорилго нь эвдэх, сүйтгэх, хорлох явдал биш, харин өөрийнхөө чадварыг шалгах, мэдлэг туршлагаа үргэлж дээшлүүлж байхыг эрмэлздэг, системд юу нээснээ бусадтай хуваалцаж, түүнийг сайжруулахад тэмүүлэх явдал юм.

Харин кракерууд бол өөр. Тэдний зорилго бол программыг засах, өөрийн зорилгод нийцүүлэн өөрчлөх, ингэснээрээ ямар нэг байдлаар ашиг хонжоо олох, гэмт хэргийн чанартай үйлдлүүдийг хийж байдагт оршино. Гэхдээ хакерууд өөрийн мэдлэгийг

өөр зорилгоор ашиглахыг үгүйсгэх аргагүй юм. Учир нь тухайн системийг хамгийн сайн мэдэж байгаа хүн түүнийг хамгийн сайн хамгаалж, эсвэл түүнд хамгийн их аюул учруулж ч болзошгүй.

Дэлхий дахинд хакер, кракеруудын үйл ажиллагаа улам өргөжсөөр байна. АНУ ын хамгаалалтын албаны систем л гэхэд сүүлийн жилүүдэд 250000 удаа халдлагад өртсөн байдаг байна. MicroSoft корпорацийн нэгэн вэб хуудасны Солонгос дахь салбарын программ хангамжид тус вэбэд хандагчдын нууц үгийг мэдэх зорилготой программ суулгасан байсныг илрүүлж үйл ажиллагааг нь нэг өдөр зогсоож засварлаж байжээ. Ер нь хакер, кракеруудын үйл ажиллагаа ихэнхдээ амар хялбар аргаар мөнгө олоход чиглэгддэг. Энэ нь банкны дансны, эсвэл кредит картны дугаар болон нууц үгийг хулгайлах, хууль эрхийн холбогдолтой бичиг баримт, хувийн нууцтай холбоотой мэдээлэл хулгайлах зэргээр хохирол учруулдаг. Мөн сүүлийн жилүүдэд вэб сайтуудын агуулгыг өөрчлөх эрсдлүүд нэлээд гарах хандлагатай болжээ. Ялангуяа хөгжингүй орнуудын Засгийн Газрын, шүүх эрх мэдлийн байгууллагуудын вэб болон мэдээллийн системүүдэд байнгын аюул занал учруулахаар завддаг тухай судалгаанууд их байдаг байна.

Садар самуун, хүчирхийллийг сурталчлахаас үүдэх эрсдэл

Хэдийгээр компьютерийг олон сайн зүйлд ашиглаж байдаг ч бас тодорхой хэмжээгээр буруу зорилгоор ашиглах явдал байсаар байгаа юм.

XX зууны шилдэг технологиудын нэг интернэтийг ашиглахтай холбоотой сөрөг үзэгдлүүдийн нэг нь садар самуун, хүчирхийллийг сурталчлах явдал юм. Энэ нь нэгэн төрлийн гэмт хэрэг бөгөөд үүнтэй дэлхий дахин олон арга замаар тэмцэж байна. Интернэтийн хамгийн өргөн ашиглагддаг Yahoo сайтын чат өрөөнүүдийн дор хэрэглэгчдийн үүсгэсэн чатаар энэ төрлийн сурталчилгаа нэг хэсэг нэлээд хийгдэж байсныг мэдээд хэрэглэгчийн чат өрөө үүсгэх боломжийг хаажээ. Хэдийгээр энэ нь Yahood хамааралгүй үйлдэл байсан ч гэлээ сайтдаа тавих хяналт сул байсан гэдэг утгаар тодорхой хэмжээнд буруутгагдсан юм.

Интернэтээр хүний нэр төрийг гутаан доромжлох, айлган сүрдүүлэх, заналхийлэх оролдлогууд нэлээд гардаг. Энэ нь хүний сэтгэл санаанд хүчтэй цочрол өгч, дарамт үзүүлдэг. Гэсэн ч энэ төрлийн гэмт хэргийг шүүх цагдаагаар шийдүүлэхэд төвөгтэй, хууль эрх зүйн орчин бүрдээгүй, эзэн холбогдогчийг нь тогтооход бэрхшээлтэй байдгаас хохирогчдод хүндрэл учруулдаг болно. Ихэнхдээ нэртэй дуучид, алдартай хүмүүс, томоохон бизнесмэн болон улс төрчдөд ийм дарамт ирэх нь олонтой.

Кибер терроризмийн ажиллагаанаас үүдэх эрсдэл

Өнөө үед компьютерийн гэмт хэрэг нь улам бүр өсөх хандлагатай болоод байна. Интернэт нь дэлхий даяар аалзны тор мэт хэрсэн асар том сүлжээ боловч хууль эрхийн болон хамгаалалтын нарийн тогтсон дүрэм байхгүй байгаагаас түүнийг ямар ч зорилгоор хэн ч ашиглаж болдогт аюулын гол нь оршиж байгаа юм.

Кибер терроризм гэдэг нь дэвшилтэт технологи ашиглан террорист үйл ажиллагаа явуулахыг хэлэх бөгөөд үүнд өртөж болох дэд бүтцүүдэд агаарын болон бусад тээврийн удирдлага, атомын болон усан цахилгаан станц, эрчим хүчний байгууламж, цэнэгтэй сумнаас хамгаалах систем, цахилгаан сүлжээ, холбооны системүүд ба мөнгөн гуйвуулга хийх электрон системүүд багтана.

Кибер терроризм нь компьютер, компьютерийн систем болон сүлжээнд санаатайгаар байрлуулсан улс, нийгмийн аюулгүй байдал, тусгаар тогтнол, хүний амь нас, эрүүл мэндэд шууд заналхийлэх зорилготой, хууль зүйн сөрөг үр дагавар бүхий аливаа халдлагаар илэрч байдаг. Гэмт хэргийн бүлэглэлүүд нь мэдээллийн технологийг ашиглан улс үндэстэн, хил хязгаар дамнасан гэмт үйлдэл, үйл ажиллагаа эрчимтэй явуулж буйг мэдээллийн технологи өндөр хөгжсөн

дэлхийн улс орнуудын практик, бусад эх сурвалж баримтаар нотолж байна.

WWW ийг террорист бүлэглэлүүд суртал нэвтрүүлэг, харилцаа холбооныхоо гол хэрэгсэл болгож байна. Тэдний үйл ажиллагаандаа ашиглаж байгаа арга барилууд байнга өөрчлөгдөж байдаг нь тэднийг мөрдөгч, судлагчдаас үргэлж түрүүлж байдаг. Тэгэхдээ тэд заримдаа алдаа гаргадаг гэж интернэтийн терроризмыг судлагч Нейл Дойль хэлсэн байдаг байна. Эндээс үзэхэд дэлхий дахинд болж буй сайн муу бүх л үйл явдлуудын гол хэрэгсэл нь Интернэт гэдгийг бид ямагт санаж байх хэрэгтэй юм.

Авч үзэж буй асуудал Манай улсад ...

Нэгэн үе компьютерийн гэмт хэрэг гэж юу болох талаар бид огт мэддэггүй байлаа. Энэ үед манай улсын компьютерийн хэрэглээ өндөр биш, хүмүүсийн мэдлэг дулимаг, сүлжээний технологи сайн хөгжөөгүй, интернэт бидний хэрэглээ болж чадаагүй байсан юм. Харин сүүлийн 10 аад жилд байдал эрс өөр болжээ. Монголчууд өөрсдийн сүлжээтэй болж, интернэтэд холбогддог гарцуудтай болсноор дэлхий дахины гэмт хэргийн халдлагад өртөх зам нээгдсэн гэж хэлж болно.

Манай улсын ихэнх байгууллагуудын дотоод сүлжээнд «байнгын зочин» вирусууд байж л байдаг. Зарим хүмүүсийн компьютер маш олон төрлийн вирусуудыг тээгээд л явж байдаг. Манай интернэт үйлчилгээ үзүүлэгч байгууллагууд болон харилцаа холбооны компаниудын вэб сайтууд, банкны байгууллагуудын сүлжээнд нэвтрэх оролдлого удаа дараа гарч байгаа тухай хэвлэл мэдээллийн хэрэгслээр дурдагддаг болжээ.

2005 онд манай нэгэн нэртэй том банкин дахь компаний данснаас программ зохиогч мэргэжилтэй хүмүүс их хэмжээний мөнгө сүлжээний технологи ашиглан авсан явдал нь биднээс хол ангид юм шиг бодож явдаг эрсдэл биднийг үргэлж дагаж мөрдөж байгааг сануулж байх шиг. Харамсалтай нь халдлагад өртсөн болон өртөх магадлалтай байгууллагууд байгууллагынхаа нэр төр, эрх ашгийг хамгаалах нэрийдлээр болж буй үйл явдлыг нууж, ялимгүй зүйл мэтээр өнгөрөөдгөөс ийм явдал бусдад сэрэмж болох нь бага байх шиг санагддаг.

Манай оронд компьютерийн гэмт хэрэг хэдийнээ бодит зүйл болжээ. Үүнийг манай мэргэжлийн хүмүүс ч нэгэн дуугаар хүлээн зөвшөөрдөг юм. Үүний тод жишээ нь «Мэдээллийн аюулгүй байдлын үзэл баримтлал, эрх зүйн зохицуулалт» бага хурлыг Монгол Улсын Үндэсний аюулгүй байдлын зөвлөлийн ажлын албанаас санаачлан хуралдуулж зохих зөвлөмж гаргасан явдал юм. Энэ зөвлөмжинд олон асуудлыг авч үзсэний дотор компьютерийн мэдээллийн аюулгүй байдлын чиглэлээр дагнан ажилладаг мэргэжлийн байгууллагатай болох саналыг гаргасан байна.

Компьютерийн гэмт хэргийн эрсдлээс сэргийлэх арга замууд:

1. Аль болох олон төрлийн вирус илрүүлдэг, түүнийгээ компьютерт нөлөөлөхгүйгээр устгаж чаддаг, программуудаа байнга шинэчилж, түгээх ажлыг хялбаршуулсан, дэлхий нийтэд нэрд гарч чадсан компаний вирусийн эсрэг программ хангамжийг ашиглах нь зүйтэй юм. Тухайлбал: Norton Anti Virus, Kaspersky Anti Virus, McAfee, V3pro, F-Prot зэргийг дурдаж болох юм.

2. Шинээр гарч буй вирус, ялангуяа хор хөнөөл ихтэй вирусээс хэрхэн сэргийлэх талаар байгууллага хүн бүрийг мэдээллээр хангах, энэ зорилгоор хэвлэл мэдээллийн хэрэгслээр сурталчилгаа хийдэг болох шаардлагатай.

3. Хууль бус программ хангамж аль болох ашиглахгүй байх хэрэгтэй. Учир нь ийм төрлийн программууд нь ихэвчлэн хакер, кракерын замаар тархсан байх магадлалтай байдаг. Иймээс бид хууль бус программ ашиглах нь эрсдлээ өндөрсгөж байгаа хэрэг юм.

4. Компьютерийн эрсдлийн менежментийн чиглэлээр нарийн мэргэшсэн мэргэжилтэн бэлтгэх хэрэгтэй.

5. Бага насны хүүхдүүдийг интернэт орчинд хяналттай, зөв сургах хэрэгтэй.

6. Манайд компьютерийн гэмт хэрэг, мэдээллийн аюулгүй байдалтай холбоотой хууль эрх зүйн орчин төгс утгаараа бүрдээгүй зөвхөн эхлэлийн төдий,тодорхойгүй,ядмагзаалтуудтай байгаагаас энэ төрлийн гэмт хэрэг гарах нэг нөхцөл болж байж магадгүй юм. Иймээс энэ чиглэлээр хууль эрх зүйн заалтыг шинэлэг, дорвитой болгон өөрчлөх шаардлагатай байна.

7. Улс оронд гарч буй компьютерийн гэмт хэргийн чанартай үйл явдлуудыг мэргэжлийн хүрээнд шүүн хэлэлцэж үнэлэлт дүгнэлт өгдөг нарийн мэргэшсэн комисстой болох шаардлагатай юм.

8. Олон улсын түвшинд компьютерийн гэмт хэрэгтэй тэмцдэг арга туршлагаас байнга суралцах хэрэгтэй.

9. Байгууллага бүр сүлжээний найдвартай аюулгүй байдлыг ханган, нөөц сүлжээний шугамтай болох, сүлжээний администраторааар мэргэжлийн өндөр түвшиний хакерийн хэмжээний мэдлэгтэй хүмүүсийг ажиллуулж байх шаардлагатай.