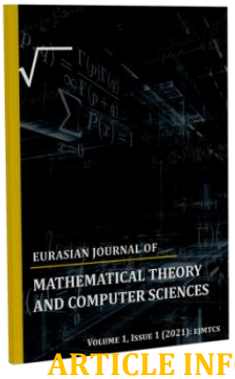
EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
IF = 7.906 www.in-academy.uz



MALICIOUS SOFTWARE

Saidullaev Dilshod
Kurbanbaev Azamat
Abdulazizova Umida,
Shukurov Muhammadolim
(Samarkand State Medical University)
Scientific Advisor: **A.E. Kubaev**
https://doi.org/10.5281/zenodo.15504151

ARTICLE INFO

Received: 19th May 2025
Accepted: 23rd May 2025
Online: 24th May 2025

KEYWORDS

Trojan horses, Adware, Spyware, Backdoors, Triggers, Logic bombs, Authentication request logging, "Semi-resident" viruses.

ABSTRACT

This article discusses various types of malicious software that have become well-known on a global scale, their classifications, and the methods they use to operate or cause damage to computer systems.

ЗАРАРЛИ ДАСТУРИЙ ТАМИНОТЛАР

Саъдуллоев Дилшод
Курбанбаев Азамат
Абдулазизова Умида
Шукуров Мухаммадолим
(Самарқанд давлат тиббиёт университети)
Илмий рахбар: **А.Э.Кубаев**
https://doi.org/10.5281/zenodo.15504151

ARTICLE INFO

Received: 19th May 2025
Accepted: 23rd May 2025
Online: 24th May 2025

KEYWORDS

Троян отлари, Adware, Spyware, Backdoors Триггер, мантиқий бомбалар, аутентификация сўровларини қайд этиш, ярим резидентли вируслар.

ABSTRACT

Ушбу маколада бугунги кунда дунё микиёсида таникли булишга улгурган зараркунанда дастурий таъминотлар, турлари ва уларнинг компютер дастурларидаги харакалари ёки зарар келтириш усуллари хакида баён килинади.

Зарарли дастурий воситалар фойдаланувчини рухсатисиз ҳужумчи каби ғаразли амалларни бажаришни мақсад қилган восита ҳисобланиб, улар юкланувчи код (.exe),

актив контент, скрипт ёки бошқа кўринишда бўлиши мумкин. Ҳужумчи зарарли дастурий воситалардан фойдаланган ҳолда тизим хафсизлигини обрўсизлантириши, компьютер амалларини бузиши, махфий ахборотни тўплаши, веб сайтдаги контентларни модификациялаши, ўчириши ёки қўшиши, фойдаланувчи комптютерини бошқарувини қўлга киритиши мумкин. Бундан ташқари зарарли дастурлар, ҳукумат ташкилотлардан ва корпоратив ташкилотлардан катта ҳажмдаги махфий ахборотни олиш учун ҳам фойдаланилиши мумкин.

Зарарли дастурлар турлари:

- *вируслар:* ўзини ўзи кўпайтирадиган программа бўлиб, ўзини бошқа программа ичига, компьютернинг юкланувчи секторига ёки ҳужжат ичига бириктиради.

- *троян отлари:* бир қарашда яхши ва фойдали каби кўринувчи дастурий восита сифатида кўринсада, яширинган зарарли коддан иборат бўлади.

- *Adware:* маркетинг мақсадида ёки рекламани намойиш қилиш учун фойдаланувчини кўриш режимини кузутиб борувчи дастурий таъминот.

- *Spyware:* фойдаланувчи маълумотларини қўлга киритувчи ва уни ҳужумчига юборувчи дастурий код.

- *Rootkits:* ушбу зарарли дастурий восита операцион тизим томонидан аниқланмаслиги учун маълум ҳаракатларини яширади.

- *Backdoors:* зарарли дастурий кодлар бўлиб, ҳужумчига аутентификацияни амалга оширмасдан айланиб ўтиб тизимга кириш имконини беради, маслан, администратор паролисиз имтиёзга эга бўлиш.

- *мантиқий бомбалар:* зарарли дастурий восита бўлиб, бирор мантиқий шарт қаноатлантирилган вақтда ўз ҳаракатини амалга оширади.

- *Ботнет:* Интернет тармоғидаги обрўсизлантирилган компьютерлар бўлиб, тақсимланган ҳужумларни амалга ошириш учун ҳужумчи томонидан фойдаланилади.

- *Ransomware:* мазкур зарарли дастурий таъминот қурбон компьютерида мавжуд қимматли файлларни шифрлайди ёки қулфлаб қўйиб, тўлов амалга оширилишини талаб қилади.

Мантиқий бомба

Ўзидан кўпайиш йўқ

Сонини ошиб бориши: ноль

Юқумлилиги: мумкин

Мантиқий бомба икки қисмдан иборат код ҳисобланади:

1. Фойдали юклама қисми бажарилиш учун ҳаракат қисми ҳисобланади. Фойдали юклама қисми ҳоҳлаган кўринишда бўлиши мумкин, лекин зарар келтирувчи эффект маъносига эга бўлади.

2. Триггер, мантиқий шарт бўлиб фойдали юклама қисмини бажарилишини назоратга олади ва баҳоланади. Триггернинг аниқ шарти тасаввур билан чегараланган бўлади ва сана, фойдаланувчининг тизимга кириши ёки операцион тизим версияси каби маҳаллий шартларга асосланади. Шу тарзда триггерлар масофадан тўриб ўрнатилувчи кўринишда лойиҳаланиши мумкин ёки бўлмаса қандайдир ҳолатни мавжуд эмаслигига кўра.

Мантиқий бомбалар мавжуд коднинг ичига киритилиши ёки бўлмаса автоном тарзда бўлиши мумкин. Оддий паразитик (юқумли) намуна қуйида кўрсатилган бўлиб, триггер сифатида аниқ сана ишлатилганда компьютерни бузилишига олиб келиши мумкин:

legitimate code
if date is Friday the 13th:
crash_computer( )
legitimate code

Троян оти

Ўзидан кўпайиш : йўқ
Сонини ошиб бориши: ноль
Юқумлилиги: Ҳа

Ушбу турдаги зарар келтирувчи дастурлар Греклар ва Трояликлар ўртасидаги уруш даврида ишлатилган найрангга асосланади ва шу учун шунақа ном олган.

Ахборот коммуникация технологияларида троян оти бу дастур бўлиб, қандайдир содда вазифани бажаришга мўлжалланган бўлади. Бироқ қўшимча тарзда зарар келтирувчи вазифани хуфиёна бажаради. Классик намунаси сифатида тизимга киришда паролни ушлаб олиш дастурини келтириш

мумкин, у «username» и «password» каби аутентификация сўровларини қайд этади ва фойдаланувчи томонидан ахборот киритилишини кутиб туради. Ушбу ҳолат юз берганда ўзининг яратувчиси учун паролларни ушлаб олувчи дастур ўзига ёзиб қуяди, сўнгра эса “нотўғри парол” деган хабарни тизимга реал кириш олдидан чиқаради. Ҳеч нимадан шубҳаланмаган фойдаланувчи хато қилгандек бўлади.

Backdoors (орқа эшик)

Ўзидан кўпайиш: йўқ
Сонини ошиб бориши: ноль
Юқумлилиги: мавжуд

Backdoor (туйнук) бу оддий хавфсизлик текширувидан ўта оладиган ҳар қандай механизмдир. Дастурчилар баъзида орқа эшикни (туйнук) қонуний асосларга кўра ҳосил қилишади.

Мантиқий бомбалар каби орқа эшик (туйнук) дастурлари ҳам дастур кодида ёки автоном дастурларда бўлиши мумкин. Орқа эшик (туйнук) намунаси қуйидаги кодда кўрсатилган бўлиб, у тизимга киришда аутентификация жараёнини айланиб ўтади.
username = read_username ( )
password = read_password ( )
if username is “133t h4ck0r”:
return ALLOW_LOGIN
if username and password are valid:
return ALLOW_LOGIN
else:
return DENY_LOGIN

Вирус

Ўзидан кўпайиш: ҳа

Сонини ошиб бориши: ижобий

Юқумлилиги: ҳа

Компьютер вируси – зарарли дастурларнинг бир тури бўлиб, бажарилган вақтида бошқа компьютер дастурларини ўзгартириш ва ўз кодини киритиш орқали ўзини кўпайтиради. Ушбу жараён муваффақиятли амалга ошилган тақдирда, таъсирланган соҳа компьютер вируси билан “зарарланган” деб айтилади.

Вирус яратувчилар тизимларни дастлабки зараралаш ва унда вирусни тарқатиш учун социал инжинерия алдовлари ва хавфсизлик заифликлари тўғрисидаги батафсил маълумотлардан фойдаланади. Компьютер вирусларининг аксарияти Microsoft Windows ОТда ишловчи тизимларда қаратилган бўлиб, янги хостларни зараралашда кўплаб механизмлардан ва кўп

ҳолларда антивирус воситаларини алдаб ўтиш учун анти-аниқлаш/ яширин стратегиялардан фойдаланади.

Ҳозирги кунда компьютер вирусларининг ягона тизимли таснифи мавжуд эмас ва турли манбаларда уларни турлича омиллар асосида таснифлари келтирилган. Маколамизда хусусан, компьютер вирусларини қуйидаги омиллар бўйича таснифланишини айтиб утамиз:

1. Ресурслардан фойдаланиш усулига кўра. Ҳозирги кунда компьютер вирусларини ресурсдан фойдаланиш усулига кўра *вирус-паразитлар* (ёки шунчаки *вирус*) ва *вирус-червлар* (ёки шунчаки *червлар*) га ажратиш мақсадга мувофиқ бўлади.

Ресурслардан фойдаланиб кўпайишнинг биринчиси бу – бошқа дастурга мансуб бўлишдир. Масалан, улар бошқа дастурлар ичида жорий қилинади ва ушбу дастур юкланиши билан активлашади.

Иккинчиси одатда фақат ҳисоблаш тизими ресурсидан (тезкор ва доимий хотира, дастурий бўлмаган файллар) фойдаланиб, тармоқ орқали ўз нусхаларини тарқатади, ахборот элтувчилари, хотира буфери ва бегона архивлар ёрдамида барчага тақсимланади. Червлар автоном бўлиб, улар бошқа дастурларга бириктирилмайди.

2. Зарарланган объектлар турига кўра. Ушбу таснифга кўра вирусларни *дастурий*, *юкланувчи, макровируслар* ва *кўп платформали* вирусларга ажратиш мумкин.

Дастурий вируслар бошқа дастурларнинг файлларини зараралайди. Масалан, *Win9X.CIH* вируси Windows 95/98/ME ОТ дастурлари учун паразит ҳисобланади.

Юкланувчи вируслар юкланган қаттиқ дискдаги, дискета ёки флешка секторларида жойлашган кичик программаларни зараралайди ёки уни алмаштиради. Бунга мисол сифатида BIOS сатҳида ишловчи *Michelangelo* вирусини келтириш мумкин.

Макровируслар учун шароит яратувчи восита сифатида маълум дастурлаш тилида ёзилган ва турли офис иловалари – MS Word ҳужжати, MS Excel электрон жадвали, Corel Draw тасвири, файлларида жойлашган “макрослар” ёки “скриптлар” хизмат қилади. Бунга мисол қилиб, MS Word ҳужжатларини зарарловчи *Concept* вируси, Excel жадвалларини зарарловчи *Laroux* вирусларини келтириш мумкин.

Кўп платформали вируслар бир вақтнинг ўзида турли хилдаги объектларни зарарлайди. Масалан, *OneHalf.3544* вируси ҳам MS-DOS дастурлари ҳам қаттиқ дискнинг юкланувчи секторларини зарарласа, *Anarchy* оиласига тегишли вируслар MS-DOS ва Windows дастурларидан ташқари, MS Word ҳужжатларини ҳам зарарлай олади.

3. Фаоллашиш принципига кўра. Вирусларни ушбу хусусиятига кўра *резидент* ва *норезидент* турларга ажратиш тавсия этилади. Резидент вируслар доимо компьютер хотирасида актив ҳолатда жойлашади, жабрланувчига бошқа дастур ёки операцион тизим орқали мурожаатларни кузатиб боради ва шундан сўнг унга юқади. Масалан, бажарилувчи дастурлар юкланиш вақтида, ишни тугатиш вақтида ёки уларнинг файлларини кўчириш вақтида зарарланади. Буларга мисол қилиб, *OneHalf.3544* (MS-DOS муҳитида) ва *Win9X.CIH* (Windows 95/98/ME муҳитида) вирусларини мумкин.

Норезидент вируслар зарарланган ташиб юрувчиларни ишга тушириш вақтида ишга тушади ва уларнинг фаолият вақти чекланган бўлади. Масалан, *Vienna.648* вируси зарарланган дастур ишга тушгандан сўнг дарҳол ишга тушади. Бироқ, ушбу вақтда дискдан кўплаб қурбонларни топишга ва уларни бириктиришга улгуради. Шундан сўнг, бошқарувни ўзининг сақловчисига узатади ва ўзи кейинги юкланишга қадар "*ухлайди*".

Кўп вазифали операцион тизимларда "*ярим резидентли*" вируслар мавжуд бўлиб, улар худди норезидент вируслар каби юкланади. Алоҳида оқимли юкланган дастурлар каби ташкил қилиб, ушбу дастурларнинг бутун ишлаш давомида ўзини резидент каби тўтади ва ўз ишини сақловчи-дастури билан биргаликда тугатади. Масалан, *Win32.Funlove.4070* бунга мисол бўла олади.

4. Дастур кодини ташкил қилиш ёндашувига кўра. Мазкур таксаномик белгилар вирусларни *шифрланган, шифрланмаган* ва *полиморф*ларга ажратишга имкон беради.

Шифрланмаган вируслар ўзини оддий дастурлар каби кўрсатади ва бунда дастур кодида ҳеч қандай қўшимча ишлашлар мавжуд бўлмайди. Бундай вирусларни (масалан, **Vienna.648**) дастурларда осонлик билан аниқлаш ҳамда дизассамберлар ва декомпиляторлар орқали тадқиқ қилиш ва ўчириб ташлаш мумкин.

Шифрланган вируслар кодида бир қанча ўзгаришлар мавжуд бўлади. Шифрланган вирус ҳисоблаш қурилмасининг хотирасида дастлаб дешифрланади ва шундан сўнг зарарлашни бошлайди. Шунинг учун мазкур вирусларни аниқлаш, ўрганиш ва ўчириш мураккаб бўлиб, бу мураккаблик камида ундаги қайтариш амали – кодни дешифрлаш билан характерланади. Одатда вирусни шифрлаш коддаги махсус антидебаггерлаш усулидан фойдаланиш орқали амалга оширилади. Бундай вируслар сирасига *Sayha.Diehard* вирусини киритиш мумкин.

Полиморф вируслар турли кўринишдаги шифрланган вируслар бўлиб, ўзининг иккилик шаклини нусхадан-нусхага ўзгартириб боради. Мазкур синфдаги вирусларга *OneHalf* оиласи вирусларини киритиш мумкин. Хусусий ҳолларда полиморфлик *метаморфик вируслар* бўлиб, ўзининг иккилик танасини шифрламасдан, фақат уларни ўзгартириш орқали ўз нусхаларини яратади. Бундай вирусларга мисол қилиб, *Win32.Zmyst* вирусини келтириш мумкин.

1. ***Вирус-червларнинг таснифи.*** Вирус-червларни классификациялашда уларни тарқалиш йўлларига асосланилади. Масалан, *почта червлари (*масалан,*E-*

Worm.Win32.Aliz) электрон почта орқали тарқалса, *тармоқ червлари* (одатда улар *Интернет червлари* деб ҳам юритилади) тармоқ протоколлари ёрдамида тарқалади ва маълумот пакетлари ичида я ширинган ҳолда узатилади (масалан, *Net-Worm.Win32.Lovesan*). *"Телефон"* ёки *"мобил"* червлар (масалан, *Cabir*) эса турли "тармоқ" лар орқали тарқалади. Масалан, симсиз ахборот узатиш тармоғи ҳисобланган *BlueTooth* орқали. Бундан ташқари 1980 йилларда тарқалган *файл червлари* деб номланган тури (масалан, *Mkworm.715*) эса, ўзи мустақил равишда тарқалмайди. Балки, ўзини турли ташиб юрувчилар ва каталогларда, ҳаттоки, ZIP, RAR файлларда, нусхалайди ҳамда шу тартибда тарқалади.

6. Компьютер вирусларининг бошқа омиллар бўйича таснифи. Компьютер вирусларининг юқорида келтирилган омиллардан ташқари қуйидаги омиллар асосида ҳам таснифлаш мумкин:

– зарарлайдиган операцион тизими ва платформасига кўра (DOS, Windows, Unix, Linux, Android);

– компьютер вируси ёзилган дастурлаш тили бўйича (ассемблер, юқори дастурлаш тили, ценарий тили ва ҳ.);

– қўшимча зарарли функцияларига кўра (бекдорлар, кейлоггерлар, шпионлар, ботнетлар ва ҳ.).

Албатта, юқорида келтирилган компьютер вирусларининг таснифи якуний эмас ва ҳар бир муаллиф танлаб олган омиллари асосида уларни таҳлил қилиши мумкин. Кейинги бўлимда эса ҳисоблаш тармоқларида кўп зарар келтирилган ва машҳур зарарли дастурий воситалар билан танишиб чиқилади.

Вирус тарихи

Илк бора 1983-йил 11-ноябр куни Жанубий Калифорния университети талабаси, америкалик Фред Коен 5 дақиқадан 1 соатгача бўлган тезликда кўпая оладиган компьютер вируси тақдимотини ўтказган.

Шундан сўнг, орадан бир йил ўтиб, Коен компьютер тармоқлари бўйлаб вирусларнинг тарқалиш хавфи ва антивирус дастурларини яратиш имкониятлари ҳақида китоб ёзади.

Биринчи яратилган вирус (1986 йилда яратилган) "Brain" деб номланган бўлиб, у фақат компьютер дискетлари орқали тарқалган. Биринчи антивирус дастури эса 1988-йилда ишлаб чиқилган.

Барча вақтларнинг энг кучли 4 вируси

1. ILOVE YOU

ILOVEYOU ҳозирги кунга қадар яратилган энг кучли зарарли вируслардан бири ҳисобланади. У бутун дунё бўйлаб компьютер тизимларига вайронагарчиликларни келтириб чиқарди ва тахминан 10 миллиард доллар зарар келтирди. Дунё компьютерларининг 10 фоизи зарарланган деб ҳисобланган. Ҳукуматлар ва йирик корпорациялар инфекцияни олдини олиш учун почта тизимларини офлайн режимга ўтказганлар.

Вирус икки филипинлик дастурчи Реонел Рамонес ва Онел де Гузман томонидан яратилган. Бу вирус социал инжинериядан фойдаланиб, одамларни "қўшимча ҳаволани" босишга мажбур қилди. Бу ҳолда севгини тан олиш сўрови бўлган. Илова аслида TXT

файл сифатида шаклланадиган скрипт бўлган. Чунки ўша пайтда Windows ушбу файлнинг ҳақиқий кенгайтмасини яширган еди.

Босиш тугмачасини босгандан сўнг, у фойдаланувчини юбориш рўйхатидаги ҳар бир кишига ўзини юборади ва файлларни қайта ёзишни давом еттиради. Бу эса компьютерни ўчириб бўлмайдиган ҳолатга туширади.

2. Code Red

Code Red биринчи марта 2001 йилда пайдо бўлган ва eEye Digital Security ташкилотининг икки ходими томонидан топилган. Бу кашфиёт пайтида жуфтликлар Code Red Mountain Dew номли ичимликни ичганлиги сабабли Code Red деб номланган.

Тизимда буфер тошиб кетиш муаммосидан фойдаланиб, Microsoft IIS веб-сервери ўрнатилган компьютерларни нишон қилиб олган. У қаттиқ хотирада жуда оз из қолдиради. Чунки у тўлиқ хотирада ишлай олади, ҳажми 3569 байтга тенг.

Инфекцияни юқтирганида, у юз нусхани яратишга киришади, лекин дастурлашдаги хато туфайли у яна кўпаяди ва кўплаб тизим ресурсларига зарар килиб улгурди.

Энг эсда қоларли аломат бу таъсирланган веб-саҳифаларда “Хитойликлар томонидан ҳужум қилинди” деб қолдирган хабар булди. Кейинчалик вакцина чиқарилди ва кейинчалик 2 миллиард долларгача зарар келтиргани ҳисобланган. Жами 1-2 миллион серверларга таъсир кўрсатди. Шу даврда 6 миллион IIS серверлар мавжуд бўлган.

3. Melissa

Флорида штатидаги екзотик раққос номи билан 1999 йилда Девид Л. Смит томонидан яратилган. Бу вирус билан зарарланган Word ҳужжати, alt.sex номи билан марказлашмаган тармоқ гуруҳига жойлаштирилган ва порнографик сайтлар учун пароллар рўйхати деб даъво қилинган. Бу нарса одамларни қизиқтирди ва юклаб олиб очганда ишга тушади.

Вирус ўзини электрон почта манзиллар китобидаги 50 та одамга юборади ва бу электрон почта трафикининг кўпайишига олиб келади. Бу ҳукумат ва корпорацияларнинг электрон почта хизматларини бузган. Бундан ташқари, баъзан

уларга Simpsons (Америка анимация жанри) маълумотномасини қўшиш орқали ҳужжатларни бузади.

Охир оқибат Смит Word ҳужжатини унга топширишганида қўлга олинди. Файл ўғирланган AOL аккаунтидан фойдаланиб юкланган ва уларнинг ёрдами билан ҳуқуқни муҳофаза қилиш идоралари уни авж олганидан бир ҳафтадан камроқ вақт ичида ҳибсга олишга муваффақ бўлишган.

У ФҚБ билан Анна Коурникова вирусини яратувчиси сифатида танилган бошқа вирус яратувчиларини ушлашда ҳамкорлик қилди. Ҳамкорлиги учун у бор-йўғи 20 ой хизмат қилди ва белгиланган 10 йиллик қамоқ жазоси учун уша пайтда 5000 доллар миқдорида жарима тўлади. Маълум қилинишича, вирус 80 миллион доллар зарар етказган.

4. Sasser

Windows ОТ қурти биринчи марта 2004 йилда кашф етилган бўлиб, уни Netsky қурти яратган талаба Свен Жасчан яратган. Ушбу чувалчанг Local Security Authority Subsystem Service (LSASS) тизимида буфер тўлиб тошиши мумкин бўлган заифликдан фойдаланди. Бу эса компьютернинг бузилишига сабаб бўлувчи локал қайд ёзуви хавфсизлик сиёсатини назоратлаш имконини берган. Бундан ташқари, у тизим манбаларини Интернет орқали бошқа машиналарга тарқатиш ва бошқаларга автоматик равишда юқтириш учун фойдаланади.

Бу вирус авиакомпаниялар, ахборот агентликлари, жамоат транспорти, касалхоналар ва бошқа кўплаб муҳим инфратузилмаларга таъсир қилиб, миллиондан ортиқ инфекцияланиш ҳолатини қайд қилди. Умуман, зарар 18 миллиард долларга тушди. Жасчен балоғат ёшига етмаганликда айбланиб, 21 ой шартли қамоқ жазосига ҳукм қилинди.

Натижа: Дастурлаштирилган вируслардан химояланиш учун Антивирус дастурини ўрнатиш ва мунтазам равишда янгилаб туриш талаб этилади.

Norton, McAfee, Kaspersky каби дастурларнинг тўловли версиялари юқори даражадаги ҳимояни таъминлайди.

Антивирус дастурини ўрнатиб бўлгандан сўнг, уни мунтазам равишда янгилаб туриш жуда муҳим. Чунки янги вируслар ҳар куни яратилиб, тарқалади ва антивирус дастурининг янгиланган версияси уларни аниқлай олади. Шу билан биргаликда шубхали электрон почта ва хабарларга эътиборли бўлиш керак, яъни нотаниш

манзиллардан келган электрон почталар ва хабарлардаги ҳаволаларни (ссылкаларни) босманг ва шубҳали электрон почталар ва хабарлардаги файлларни юклаб олманг.

Банк, тўлов тизимлари ва бошқа муҳим ташкилотлардан келганлиги айтилган электрон почталарга эътиборли бўлинг. Уларнинг ҳақиқийлигига ишонч ҳосил қилмагунча, шахсий маълумотларингизни киритманг.

Операцион тизим ва дастурларни мунтазам равишда янгилаб туриш асносида кучли пароллардан фойдаланиш курилмамизни вирусли дастурлардан химоя килишда яхши натижага эришамиз.

Хулоса: Ўзбекистон Республикаси қонунчилигига кўра, вирус дастурларни яратиш, тарқатиш ёки улардан фойдаланиш жиноий жавобгарликка сабаб бўлади. Жиноят кодексининг 278-моддаси ("Компьютер ахборотидан қонунга хилоф равишда фойдаланиш")га кўра, компьютер тизимига, компьютер тармоғига ёки сақлаш воситасига қонунга хилоф равишда кириш, шунингдек компьютер вирусларини яратиш, тарқатиш ёки улардан фойдаланиш, агар бу ҳаракатлар фуқароларнинг ҳуқуқларига ёки қонуний манфаатларига ёхуд ташкилотларнинг ёки давлатнинг қонун билан қўриқланадиган манфаатларига жиддий зарар етказса, базавий ҳисоблаш миқдорининг уч юздан беш юз бараваригача миқдорда жарима ёки уч йилгача ахлоқ тузатиш ишлари ёхуд бир йилдан уч йилгача озодликни чеклаш ёки уч йилгача озодликдан маҳрум қилиш билан жазоланиши мумкин.

Вирус дастурлардан фойдаланиш жуда хавфли ва қонунга хилофдир. Бундай фаолият билан шуғулланиш жиддий оқибатларга ва жиноий жавобгарликка олиб келиши мумкин. Шунинг учун, компьютерингизни вируслардан ҳимоя қилиш ва ҳеч қачон вирус дастурларини яратиш, тарқатиш ёки улардан фойдаланиш билан шуғулланмаслик керак.

References:

1. Бабаш, А. В. Криптографические методы защиты информ.: Уч.пос.: Т.1/А.В.Бабаш-2изд.-ИЦ РИОР,НИЦ ИНФРА-М,2016-413с(/ А.В. Бабаш. - Москва: **Мир**, 2016. - **597** с.
2. Баранова, Е. К. Информационная безопасность и защита. Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: РИОР, Инфра-М, 2016. - 324 с.
3. Борисов, М. А. Основы организационно-правовой защиты информации / М.А. Борисов, О.А. Романов. - М.: Ленанд, 2014. - 248 с.
4. Борисов, М. А. Основы программно-аппаратной защиты информации / М.А. Борисов, И.В. Заводцев, И.В. Чижов. - М.: Либроком, 2013. - 376 с.
5. Варлатая, С. К. Криптографические методы и средства обеспечения информационной безопасности. Учебное пособие / С.К. Варлатая, М.В. Шаханова. - М.: Проспект, 2015. - 152 с.
6. Academic Research, Uzbekistan www.ares.uz formation of students ’ skills in using the internet and hit the digital technologies. Kubaev A.E, Abdullaeva S. B
7. Galaxy International Interdisciplinary Research Journal, 10(2), 748–751
8. https://internationaljournals.co.in/index.php/giirj/article/view/1374
9. Ахборот хавфсизлиги: асосий тушунчалар.Таҳдидлар ва уларнинг турлари. Ахборот хавфсизлиги сиёсати мавзусидаги маруза дарсни модул тизимида онлайн утиш.

10. Kubayev A.E, Ne'matov N.И. Хоразм Маъмун академияси ахборотномаси: илмий журнал.-№1 (85) 2022-2, Стр. – 290-300. http://mamun.uz/uz/page/56.
11. Kubaev A. TIBBIYOTDA MATEMATIK MODELLASHTIRISH VA NANOTEXNOLOGIYALAR //Евразийский журнал математической теории и компьютерных наук. – 2023. – Т. 3. – №. 9. – С. 17-26.
12. Esirgapovich K. A. RULES OF USING MATHEMATICAL MODELING IN THE FIELD OF MEDICINE //ENG YAXSHI XIZMATLARI UCHUN. – 2023. – Т. 1. – №. 6. – С. 582-584.
13. Esirgapovich K. A. MODELING BASED ON DIFFERENTIAL EQUATIONS //TA'LIM VA RIVOJLANISH TAHLILI ONLAYN ILMIY JURNALI. – 2023. – Т. 3. – №. 11. – С. 72-75.
14. Ulug'bekovna M. S. et al. EUROPEAN JOURNAL OF MODERN MEDICINE AND PRACTICE.
15. Khozhievich B. E. et al. STUDY OF CARDIOVASCULAR SYSTEM REGULATION MECHANISMS //JOURNAL OF THEORY, MATHEMATICS AND PHYSICS. – 2023. – Т. 2. – №. 11. – С. 1-13.
16. Khozhievich B. E. et al. STUDY OF CARDIOVASCULAR SYSTEM REGULATION MECHANISMS //JOURNAL OF THEORY, MATHEMATICS AND PHYSICS. – 2023. – Т. 2. – №. 11. – С. 1-13.
17. Khojievich B. E. et al. MATHEMATICAL MODELING IN MEDICINE. ADVANTAGES AND DISADVANTAGES OF THE MAIN METHODS OF MODELING //JOURNAL OF SCIENCE, RESEARCH AND TEACHING. – 2023. – Т. 2. – №. 11. – С. 1-11.
18. Esirgapovich K. A. RULES OF USING MATHEMATICAL MODELING IN THE FIELD OF MEDICINE //ENG YAXSHI XIZMATLARI UCHUN. – 2023. – Т. 1. – №. 6. – С. 582-584.
19. Esirgapovich K. A. MODELING BASED ON DIFFERENTIAL EQUATIONS //TA'LIM VA RIVOJLANISH TAHLILI ONLAYN ILMIY JURNALI. – 2023. – Т. 3. – №. 11. – С. 72-75.