10-mavzu. Kiberxavfsizlik

Reja

Axborot xavfsizligiga tahdidlar. Zararli dasturiy ta'minot. Axborot tizimiga hujum tushunchasi. Axborot xavfsizligini ta'minlash usullari. Axborot tizimlarini himoya qilish vositalari. Axborot xavfsizligini ta'minlash bo'yicha dasturiy-texnik chora-tadbirlar. Axborotlarni kriptohimoyalash usullari. Identifikatsiya va autintifikatsiya masalalari.

Adabiyotlar

1.Aripov M., Begalov B., Begimqulov U., Mamarajabov M. Axborot texnologiяlar. O‘quv qo‘llanma. T.: Noshir, 2009 yil.

2. Misty E. Vermaat, Susan L. Sebok, Steven M. Freund. Jennifer T. Campbel, Mark Frydenberg. Discovering Computers: Tools, Apps, Devices, and the Impact of Technolog (textbook). Cengage Learning. 20 Channel Center Street. Boston, MA 02210. USA, 2016.

3. Романова Ю.Д., Лесничая И.Г., Шестаков В.И., Миссинг И.В., Музычкин П.А. Информатика и информационные технологии: учебное пособие / под ред. Ю.Д.Романовой.-3-е изд., перераб. и доп.-М.: Эксмо, 2008

Киберхавфсизлик нима?

https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security

Киберхавфсизлик (баъзан чақирилади компютер хавфсизлиги) - бу компютерлар, серверлар, mobil қурилмалар, електрон тизимлар, тармоқлар ва маълумотлар учун зарарли ҳужумлардан ҳимоя қилиш усуллари ва амалиётлари тўплами. Киберхавфсизлик бизнес соҳасидан mobil технологияларга қадар турли соҳаларда қўлланилади. Ушбу йўналишда бир нечта асосий тоифалар мавжуд.

* Тармоқ хавфсизлиги-компютер тармоқларини мақсадли ҳужумлар ёки зарарли дастурлар каби турли таҳдидлардан ҳимоя қилиш бўйича ҳаракатлар.

* Дастур хавфсизлиги-қурилмаларни жиноятчилар дастурларда яшириши мумкин бўлган таҳдидлардан ҳимоя қилиш. Инфекцияланган дастур тажовузкорга ҳимоя қилиши керак бўлган маълумотларга кириш ҳуқуқини бериши мумкин. Илованинг хавфсизлиги ривожланиш босқичида, очиқ манбаларда пайдо бўлишидан анча олдин таъминланади.

* Ахборот хавфсизлиги-сақлаш ва узатиш пайтида маълумотларнинг яхлитлиги ва махфийлигини таъминлаш.

* Операцион хавфсизлик-ахборот активларини бошқариш ва ҳимоя қилиш. Ушбу тоифага, масалан, маълумотларни қаерда ва қандай сақлаш ва узатиш мумкинлигини аниқлайдиган тармоққа кириш рухсатномалари ёки қоидаларини бошқариш киради.

* Табиий офатларни тиклаш ва бизнеснинг узлуксизлиги – хавфсизлик ҳодисасига (тажовузкорларнинг ҳаракатларига) ва тизимларнинг ишлашини бузиши ёки маълумотларнинг йўқолишига олиб келиши мумкин бўлган бошқа ҳодисаларга жавоб бериш. Табиий офатларни тиклаш-бу ташкилот ҳужум оқибатларини қандай ҳал қилиши ва иш оқимларини тиклашини тавсифловчи қоидалар тўплами. Бизнеснинг узлуксизлиги-бу ташкилот тажовузкорлар ҳужуми туфайли маълум манбаларга киришни йўқоца, ҳаракатлар режаси.

* Хабардорликни ошириш-фойдаланувчиларни ўқитиш. Ушбу йўналиш киберхавфсизлик соҳасидаги енг олдиндан айтиб бўлмайдиган омил – инсон

таъсирини камайтиришга ёрдам беради. Ҳатто енг хавфсиз тизимга ҳам бировнинг хатоси ёки жоҳиллиги туфайли ҳужум қилиш мумкин. Шунинг учун ҳар бир ташкилот ходимлар учун тренинглар ўтказиши ва уларга асосий қоидалар ҳақида айтиб бериши керак: масалан, електрон почтада шубҳали қўшимчаларни очиш ёки шубҳали УСБ қурилмаларини улаш шарт емас.

Кибер таҳдидларнинг тарқалиш кўлами

Йилдан-йилга дунёда таҳдидлар кўпайиб бормоқда ва маълумотлар тобора кўпайиб бормоқда. Статистика ҳайратда қолдиради: хавфли хавфсизлик ҳисоботига кўра, 7.9 нинг дастлабки тўққиз ойида 2019 миллиард маълумотлар оқими қайд етилган. Ушбу рақамлар 2018 йилда худди шу давр учун рақамларни икки мартадан кўпроқ (112%) оширади.

Кўпинча тиббий ва давлат муассасалари ёки чакана сектор ташкилотлари маълумотларнинг тарқалишига дуч келишади. Аксарият ҳолларда бунинг сабаби жиноятчиларнинг ҳаракатларидир. Баъзи ташкилотлар тажовузкорларни тушунарли сабабга кўра жалб қилишади-молиявий ва тиббий маълумотлар улардан ўғирланиши мумкин. Бироқ, ҳар қандай компания мақсадга айланиши мумкин, чунки жиноятчилар мижозлар маълумотларини ов қилишлари, жосуслик қилишлари ёки мижозлардан бирига ҳужум тайёрлашлари мумкин.

Халқаро маълумотлар корпорацияси, агар кибер таҳдидлар сони ўсишда давом еца, киберхавфсизлик ечимлари учун сарф-харажатлар миқдори 133.7 томонидан 2022 миллиард Ақш долларига етади. Турли мамлакатлар ҳукуматлари жиноятчиларга қарши курашиб, ташкилотларга самарали киберхавфсизлик усулларини амалга оширишда ёрдам бермоқда.

Шундай қилиб, Ақш Миллий стандартлар ва технологиялар институти (НИСТ) хавфсиз ИТ инфратузилмаси тамойилларини ишлаб чиқди. НИСТ зарарли кодни зарар етказмасдан олдин аниқлаш ва унинг тарқалишини олдини олиш учун барча електрон ресурсларни Реал вақтда доимий равишда кузатиб боришни тавсия қилади.

Буюк Британия ҳукуматининг Миллий кибер хавфсизлик маркази кибер хавфсизликка 10 қадам (киберхавфсизликка 10 қадам) қўлланмасини чиқарди. Бу тизимларнинг ишлашини кузатиш қанчалик муҳимлиги ҳақида гапиради. Австралияда сўнгги кибер таҳдидларга қарши курашиш бўйича тавсиялар Австралия кибер хавфсизлик маркази (АССС) томонидан мунтазам равишда еълон қилинади.

Кибер таҳдидларнинг турлари

Киберхавфсизлик уч турдаги таҳдидларга қарши курашмоқда.

1. Кибержиноятчилик-тизимга ҳужум қилиш ёки унинг фаолиятини бузиш ёки молиявий фойда олиш учун бир ёки бир нечта тажовузкорлар томонидан уюштирилган ҳаракатлар.

2. Киберҳужум-асосан сиёсий характердаги маълумотларни тўплашга қаратилган ҳаракатлар.

3. Кибертерроризм-қўрқув ёки ваҳима қўзғаш учун електрон тизимларни беқарорлаштиришга қаратилган ҳаракатлар.

Қандай қилиб тажовузкорлар компютер тизимлари устидан назоратни қўлга киритишади? Улар турли хил воситалар ва техникалардан фойдаланадилар – қуйида биз енг кенг тарқалганларини санаб ўтамиз.

Дастур

Исм ўзи учун гапиради. Зарар келтирадиган дастурий таъминот кибержиноятчиларнинг енг кенг тарқалган воситасидир. Улар уни

Фойдаланувчининг компютерига ва ундаги маълумотларга зарар етказиш ёки ўчириш учун ишлатиш учун ўзлари яратадилар. Зарарли дастур кўпинча зарарсиз файллар ёки електрон почта қўшимчалари ниқоби остида тарқатилади. Кибержиноятчилар ундан пул ишлаш ёки сиёсий сабабларга кўра ҳужум қилиш учун фойдаланадилар.

Зарарли дастур жуда бошқача бўлиши мумкин, бу ерда баъзи кенг тарқалган турлари:

* Вируслар файлларни зарарли код билан зарарлайдиган дастурлардир. Компютер тизимида тарқалиш учун улар ўзларини нусхалашади.

* Троян ҳуқуқий дастурий ниқоби остида яшириш зарарли бор. Кибер жиноятчилар ўз компютерларига троян юклаб олиш учун фойдаланувчиларни алдашади ва кейин маълумот тўплашади ёки зарар етказишади.

* Жосусларга қарши дастур-фойдаланувчи ҳаракатларини яширинча кузатадиган ва маълумот тўплайдиган дастурлар (масалан, кредит карта маълумотлари). Кейин кибержиноятчилар уни ўз мақсадлари учун ишлатишлари мумкин.

* Тўлов дастури файллар ва маълумотларни шифрлайди. Кейин жиноятчилар тикланиш учун тўловни талаб қилишади, акс ҳолда фойдаланувчи маълумотларни йўқотади.

* Реклама дастурлари – зарарли дастурларни тарқатиш учун ишлатилиши мумкин бўлган реклама дастурлари.

* Ботнетлар-бу кибержиноятчилар ўз мақсадлари учун фойдаланадиган зарарли дастур билан касалланган компютерларнинг тармоқлари.

СҚЛ қарши

Ушбу турдаги киберҳужум маълумотлар базаларидан маълумотларни ўғирлаш учун ишлатилади. Кибержиноятчилар маълумотлар базасини бошқариш тилида (СҚЛ) зарарли кодни тарқатиш учун маълумотларга асосланган иловалардаги заифликлардан фойдаланадилар.

Phishing

Fishing ҳужумлари, унинг мақсади Фойдаланувчининг махфий маълумотларини алдашдир (масалан, банк картаси маълумотлари ёки пароллар). Кўпинча бундай ҳужумлар пайтида жиноятчилар жабрланганларга електрон почта хабарларини юборишади ва ўзларини расмий ташкилот сифатида кўрсатишади.

Ўртада одам ҳужумлари ("ўртада одам")

Бу кибержиноятчи маълумотларни узатиш пайтида уни ушлаб турадиган ҳужум-у занжирнинг оралиқ бўғинига айланади ва қурбонлар ҳатто ундан шубҳаланмайди. Агар сиз, масалан, таъминланмаган тармоққа улансангиз, бундай ҳужумга дуч келишингиз мумкин.

Дос ҳужумлари (хизмат ҳужумларини рад етиш)

Кибержиноятчилар ҳужум мақсадининг тармоқлари ва серверларига ортиқча юк яратадилар, шу сабабли тизим normal ишлашни тўхтатади ва ундан фойдаланиш имконсиз бўлиб қолади. Масалан, тажовузкорлар муҳим инфратузилма таркибий қисмларига зарар етказиши ва ташкилот фаолиятини саботаж қилиши мумкин.

Охирги кибер таҳдидлар

Фойдаланувчилар ва ташкилотлар сўнгги кибер таҳдидлардан қайси бирига дуч келишмоқда? Келинг, буюк Британия, Ақш ва Австралия ҳукуматларининг ҳисоботларига киритилганларнинг айримларини кўриб чиқамиз.

Дридех Троян

2019 йил декабр ойида АҚШ Адлия вазирлиги бир гуруҳ кибержиноятчилар раҳбарини Дридех зарарли дастуридан фойдаланган ҳолда ҳужумда иштирок етганликда айблади. Ушбу кампания бутун дунё бўйлаб жамоатчилик, ҳукумат ва бизнес тузилмаларига таъсир кўрсатди.

Дридех пайдо хусусиятлари кенг банк троян ҳисобланади 2014. У fishing електрон почта хабарлари ва зарарли дастурлардан фойдаланган ҳолда қурбонларнинг компютерларига кириб боради. Дридех паролларни, банк картаси маълумотларини ва фойдаланувчиларнинг шахсий маълумотларини ўғирлаши мумкин. Уларга етказилган молиявий зарар миқдори юз миллионлаб баҳоланмоқда.

Ўзингизни ҳимоя қилиш учун буюк Британиянинг Миллий киберхавфсизлик маркази қурилмаларингизга сўнгги версияларнинг сўнгги хавфсизлик янгиланишлари ва antivirus дастурларини ўрнатишни, шунингдек файлларнинг захира нусхаларини мунтазам равишда бажаришни тавсия қилади.

Танишув сайтлари ва иловаларида фирибгарлик

2020 йил феврал ойида ФҚБ Ақш фуқароларини танишиш сайтларида, шунингдек суҳбат хоналарида ва дастурларда фирибгарлик ҳолатлари тўғрисида огоҳлантирди. Шерик топиш истагидан фойдаланган ҳолда, кибержиноятчилар қурбонлардан шахсий маълумотларни тортиб олишади.

ФҚБ ҳисоботидан келиб чиққан ҳолда, 2019 йилда Ню-Мексико штатининг 114 нафар аҳолиси бундай кибер таҳдидларнинг қурбонига айланишди, уларнинг молиявий йўқотишлари тахминан 1,6 million Ақш долларини ташкил етди.

Емотет

2019 йил охирида Австралия киберхавфсизлик маркази ташкилотларни Емотет деб номланган кибер таҳдид тарқалиши тўғрисида огоҳлантирди.

Емотет-бу маълумотларни ўғирлаш, шунингдек зарарли дастурларни қурилмаларга юклаб олишга қодир бўлган мураккаб троян. Унинг қурбонлари кўпинча оддий пароллардан фойдаланганлар-бу фойдаланувчиларга янада мураккаб комбинациялардан фойдаланиш кераклигини яна бир бор еслатди.

Охирги фойдаланувчини ҳимоя қилиш

Келинг, киберхавфсизликнинг яна бир муҳим жиҳати – охирги фойдаланувчилар ва уларнинг қурилмаларини (дастур ёки тизимдан фойдаланадиганлар) ҳимоя қилиш ҳақида гапирайлик. Кўпинча зарарли дастурларни компютерга, ноутбукга ёки смартфонга тасодифан юклаб оладиган охирги фойдаланувчи.

Киберхавфсизлик воситалари (хавфсизлик дастурлари) охирги фойдаланувчилар ва уларнинг қурилмаларини ҳимоя қилишга қандай ёрдам беради? Хавфсизлик воситалари електрон почта, файллар ва бошқа муҳим маълумотларни шифрлашга имкон берадиган криптографик протоколлардан фойдаланади. Ушбу механизм кибержиноятчиларнинг маълумотларни ўғирлаши ва ушлаши ёки унга кириш ҳуқуқини олишига тўсқинлик қилади.

10.1.Axborot xavfsizligi

Axborot xavfsizligi - bu axborotlar, hamda ulardan foydalanish, saqlash va uzatish uchun mo‘ljallangan tizimlar va uskunalarni - saqlash va himoya qilish.

Boshqacha qilib aytganda, bu axborot xavfsizligini himoya qilish uchun zarur bo‘lgan texnologiyalar, standartlar va boshqaruv amaliyotlari to‘plamidir.

Korxonada axborot xavfsizligi tizimlarini muvaffaqiyatli amalga oshirish uchun **uchta asosiy prinsipga rioya qilish kerak**:

1)Konfidensiallik (Maxfiylik). Axborotlarni tuzish, saqlash, qayta ishlash, uzatish va o‘zaro almashish jarayonlarida ularni ruxsatsiz oshkor qilishning oldini olish, yetarli darajadagi xavfsizligini va maxfiyligini ta’minlash.

2)Yaxlitlik (butunlik). U axborot tarkibini buzilishini, o‘zgarishini oldini olish.

3)Доступность - Kirish imkoniyati. U vakolatli shaxslarning ma’lumotlariga ishonchli va samarali kirishni ta’minlaydi. Nosozlik tufayli tizimni tiklash unda bajariladigan operatsiyalarni bajarilishiga salbiy ta’sir ko‘rsatmaydigan tarzda ta’minlanishi kerak.

Mantiqiy (nazoratning texnik vositalari). U- axborot tizimlari, dasturiy ta’minotlar, parollar, brandmauerlar (xavfsizlik devorlari), axborot tizimlariga kirishni nazorat qilish va boshqarish ma’lumotlarga kirishni himoya qilishga asoslanadi.

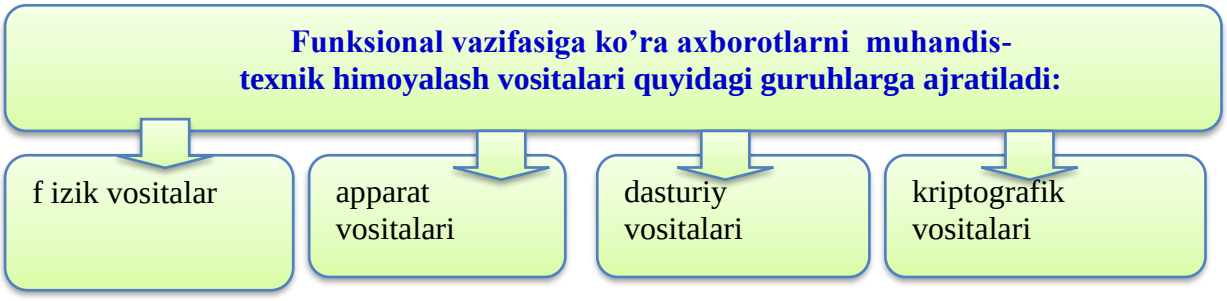
Nazoratning quyidagi turlari ajratiladi:

- **Ma’muriy.** Ma’muriy nazorat turi tasdiqlangan protseduralar, standartlar va prinsiplardan iborat bo‘ladi. Davlat organlari tomonidan yaratilgan qonun va qoidalar ham ma’muriy nazorat turlaridan biridir. Ma’muriy nazoratning boshqa misollariga korporativ xavfsizlik siyosati, parollar va intizomiy choralar kiradi.
- **Mantiqiy (nazoratning texnik vositalari).** Mantiqiy boshqaruv (texnik) boshqaruv vositalari - axborot tizimlari, dasturiy ta’minotlar, parollar, brandmauerlar (xavfsizlik devorlari), axborot tizimlariga kirishni nazorat qilish va boshqarish ma’lumotlarga kirishni himoya qilishga asoslangan.
- **Fizik.** Ish joyi muhiti va hisoblash vositalarini nazorat qilish.

Axborot xavfsizligi himoya qilish vositalari quyidagilarga bo‘linadi:

- **Tashkiliy ta’minot.** Bu tashkiliy-texnik (kompyuter imkoniyatlarini ta’minlash, kabel tizimlarini sozlash va boshqalar.) va tashkiliy-huquqiy (Qonunchilik bazasi, muayyan tashkilotning nizomi) vositalar to‘plami.
- **Dasturiy ta’minot**. Axborotni boshqarish, saqlash va himoya qilishga va unga kirishni himoya qilishga yordam beradigan dasturlar.
- **Texnik (apparatli)ta’minot.** Bu axborotlarga ruxsatsiz kirishdan himoya qiluvchi texnik qurilmalar turi.
- **Aralash apparat va dasturiy ta’minot**. Ular apparat va dasturiy ta’minot funksiyalarini bajaradilar.

10.2.Axborotlarni himoyalashning texnik va dasturiy vositalari



Axborotni himoya qilishning texnik vositalari

Axborotni himoya qilishning texnik vositalari guruhi apparat va dasturiy ta’minotlarni birlashtiradi.

Asosiylari:

• kompyuter tizimidagi eng muhim ma’lumotlar massivlarini zaxira nusxalarini yaratish, masofadan saqlash usullarini muntazam ravishda qo‘llash;

• axborotlarlar xavfsizligi uchun muhim bo‘lgan tarmoqlarning barcha quyi tizimlarini dublirovanie - nusxalash va rezervlash;

• Tarmoqning alohida elementlari ishlamay qolgan hollarda uning resurslarini qayta taqsimlash imkoniyatini yaratish;

• zaxira elektr ta’minoti tizimlaridan foydalanish imkoniyatini ta’minlash;

• uskunalarning yong‘in yoki suvdan shikastlanish xavfsizlikni ta’minlash;

• ma’lumotlar bazalari va boshqa ma’lumotlarga ruxsatsiz kirishdan himoya qiluvchi dasturiy ta’minotlarni o‘rnatish.

Autentifikatsiya va identifikatsiya

Ma’lumotlarga ruxsatsiz kirishni istisno qilish uchun identifikatsiya va autentifikatsiya kabi usullar qo‘llaniladi.

Identifikatsiya - axborot bilan aloqa bo‘ladigan foydalanuvchiga unikal nom yoki rasm berish mexanizmi.

Autentifikatsiya – foydalanuvchini ruxsat berilgan unikal nom yoki rasmga mos kelishini tekshirish usullari tizimi.

Ushbu vositalar axborotlarga kirishga ruxsat berishga yoki aksincha, rad etishga qaratilgan.

Dasturiy vositalar. Axborotlarni dasturiy himoyalash – bu axborotlarni himoya qilish vazifasini amalga oshiruvchi maxsus dasturlar tizimidir.

Konfidensial axborotlarning xavfsizligini ta’minlovchi dasturlari quyidagi yo‘nalishlarga ajratilib ko‘rsatiladi:

Axborotlarni ruxsat berilmagan kirishlardan himoyalash;

Axborotlarni nusxa olishdan himoyalash;

Axborotlarni viruslardan himoyalash;

Aloqa kanallarini dasturiy himoyalash.

Axborotlarni ruxsat berilmagan kirishlardan himoyalashni dasturiy vositalarini bajaradigan funksiyalari quyidagilardan iborat bo‘ladi:

1. Ob’yektlar va sub’yektlarni identifikasiyalash;
2. Hisoblash resurslari va axborot resurslariga kirishga cheklovlar o‘rnatish;
3. Axborot va dasturlar bilan bo‘ladigan harakatlarni nazorat va registrasiya qilish.

Kriptografik vositalar

Kriptografik vositalar-tizim va tarmoq bo’yicha uzatiladigan, EHMlarda saqlanadigan va turli xil usullar bilan shifrlanadigan axborotlarni himoya qilishning maxsus matematik va algoritm vositalaridir

9.3.Axborotlarni himoyalash usullari

https://pirit.biz/reshenija/informacionnaja-bezopasnost

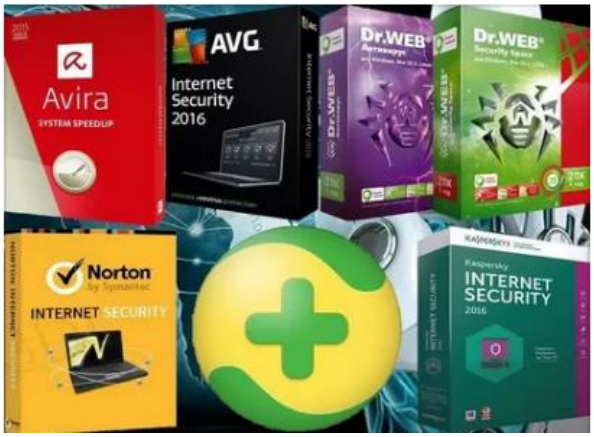
Axborot xavfsizligi vositalarining turlari:

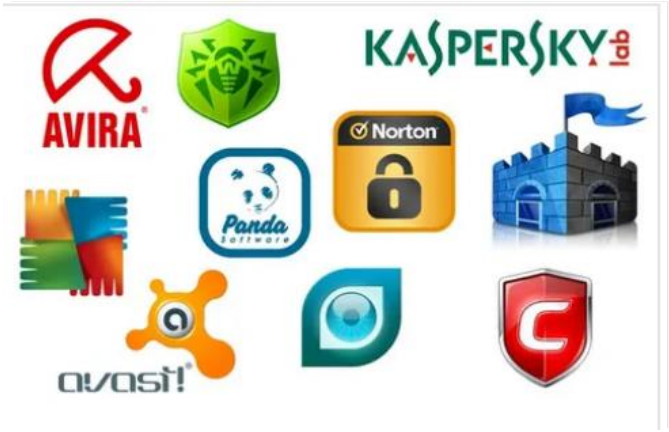
1)Antivirus dasturlari.

Kompyuter virusi - u o‘z nusxalarini yaratuvchi va ularni boshqa dasturlar kodlariga, tizim xotirasi sohalari va yuklash sektorlariga kirituvchi, nusxalarini turli aloqa kanallari orqali tarqatuvchi zararli dasturiy ta’minot turi.

Viruslarning quyidagi turlari mavjud: Черви (chuvalchanlar); **Рекламное ПО** (Reklamali dasturiy ta’minotlar (ДТ); **Шпионское ПО** (Qaроqчи-жосус ДТ); **Программы-вымогатели** (Tovlamachi –dasturlar); **Боты** (Botlar); **Руткиты** (Rutkitlar); **Троянские программы** (Toroyan dasturlari), **Баги** (Baglar)

Antivirus dasturlari-bu kompyuter viruslariga qarshi kurashadigan va zararlangan fayllarni qayta tiklaydigan dasturlar.

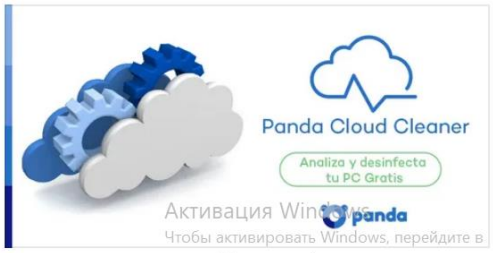




2) Bulutli antivirus - Облачный антивирус (CloudAV)

Bulut texnologiyasiga asoslangan axborot xavfsizligi yechimlaridan biri, ularda himoyalangan kompyuter xavfsizligida yengil agent dasturlari qo‘llaniladi va axborotlarni tahlil qilishni provayder infratuzilmalariga jo‘natadi.

CloudAV skanerlash ishlarini bajaradi. Bulut antiviruslariga: Panda Cloud Antivirus, Crowdstrike, Cb Defense, Immunet, Bitdefender QuickScan, Comodo Cloud Antivirus, ESET Online Scanner, F-Secure Online Scanner, Kaspersky Security Scan, McAfee Security Scan Plus, Norton Security Scan, Panda Cloud Cleaner,Trend Micro HouseCall larni keltirish mumkin.



3)Axborotlarni ruxsatsiz tarqalishidan himoyalash dasturlari DLP (Data Leak Prevention). Dunyo korxonlarida maxfiy axborotlarni yo‘qolishi va tarqalishini oldini olishga qaratilgan texnologiyalari majmui**.**

4)Kriptografik tizimlar - axborotlarni o‘zgartirish tizimi bo‘lib, ularni deshifrlash faqat ma’lum kodlar yoki shifrlar yordamida amalga oshiriladi. Buning uchun **DES – Data Encryption Standard**- Ma’lumotlarni shifrlash standarti, **AES – Advanced Encryption Standard** - Kengaytirilgan shifrlash standarti kabi dasturlar ishlatiladi.

5)Tarmoqlararo ekranlar (**brandmauerlar** yoki **fayrvollar** - xavfsizlik devorlari) - bu tarmoq trafigini blokirovka qilish va filtrlashga mo‘ljallangan tarmoqqa kirishni nazorat qilish moslamalari.

Brandmauerlar (xavfsizlik devorlari) odatda tarmoq yoki xost serverlari sifatida sniflanadi. Tarmoq brandmauerlari tarmoq bazasida **LAN, WAN** va **Intranet** tarmoqlarining shlyuz kompyuterlarida joylashdi.

6) VPN (Virtual Private Network) - Vertual xususiy tarmoq). U axborotlarni uzatish va qabul qilish uchun umumiy tarmoqlar orasidan xususiy tarmoqlarni aniqlash va ulardan foydalanishga imkon beruvchi dasturlar. **VPN** tarmog‘ida ishlaydigan ilovalar ishonchli himoyalangan bo‘ladi. **VPN** yordamida tarmoq ichida masofadan bog‘lanishga imkoniyat yaratadi. **VPN** bilan alohida foydalanuvchilarni tarmoqdagi harakatlari proksi-serverlar yordamida himoya qilinadi (yashiriladi). **VPN** yordamida geografik jihatdan uzoq joylashgan korxonalar uchun umumiy tarmoq yaratish mumkin.

7) Proxy-server (Proksi-server) - u aniq bir kompyuter yoki kompyuter dasturi bo‘lishi mumkin. U ikkita qurilma, masalan, kompyuter va boshqa server o‘rtasidagi bog‘lovchi bo‘ladi. Proksi-serverni **brandmauer** bilan birgalikda bitta kompyuterga yoki boshqa serverga o‘rnatish mumkin. Eng ko‘p so‘rovlar amalga oshiriladigan dasturlarda, masalan Internet-saytlari so‘rovlari proksi-keshda bo‘ladi. Proksi-server bilan o‘zaroharakatlar nosozliklarni aniqlash va ularni bartaraf etish imkoniyatlarini yaratadi.

8)Axborot xavfsizligini monitoring qilish va boshqarish tizimlari, SIEM. Axborot xavfsizligiga tahdidlarni aniqlash va ularga javob berish uchun **SIEM** yechimlaridan foydalaniladi. Tarmoqlararo ekran, antiviruslar, **IPS,** tezkor tizimlar kabi turli manbalardagi hodisalarni to‘playdigan va tahlil qiladigan **SIEM** yechimidan foydalaniladi. **SIEM** tizimi tufayli kompaniyalar hodisalar jurnallarini markazlashgan holda saqlash va ular orqali potensial tahdidlarni, **IT** infratuzilmasidagi nosozliklarni, kiber hujumlarni aniqlanadi.

SIEM Dasturlari: VMware AirWatch, IBM MaaS360, Blackberry Enterprise Mobility Suite, VMware Workspace One

Internet axborot resurslari

VMware AirWatch, IBM MaaS360, Blackberry Enterprise Mobility Suite, VMware Workspace One

https://www.securitylab.ru/news/529985.php Магнитные вихри можно исползоват для генерирования случайных чисел.

https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/

Способы защиты информации | Методы и средства защиты информации – SearchInform

https://studopedia.ru/11_70142_programmnie-sredstva-zashchiti-informatsii.html Программные средства защиты информации — Студопедия

Nazorat savollari

1. Axborot xavfsizligi tushunchasini tasniflang
2. Axborot xavsizlini tamoyllarini tushuntiring
3. Axborot tizimlarini qanday nazorat turlari mavjud?
4. Axborot tizimini himoya qilish vositalarini tushuntiring.
5. Autentifikatsiya va identifikatsiya deganda nimani tushunasiz?
6. Kriptografiya nima?
7. Kompyuter virusi nima?
8. Antiverus deganda nimani tushunasiz?
9. Bulutli texnologiya deganda nimani tushunasiz