

## 10(8)-mavzu. Xavfsizlik

Axborot xavfsizligiga tahdidlar

Zararli dasturiy ta'minot. Axborot tizimiga hujum tushunchasi.

Axborot xavfsizligini ta'minlash usullari

**Safety** va **Security** tushunchalari

Ijtimoiy tarmoqlardan xavfsiz foydalanish

Ma'lumotlarga tahdidlarning xususiyatlari va oqibatlari

**Axborot xavfsizligi** – bu axborotning maxfiyligi, yaxlitligi va foydaliligini ta'minlashga qaratilgan chora-tadbirlar majmuidir.

U axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, o'qish, nusxalash, o'zgartirish, yo'q qilish yoki buzilishdan himoya qilishni o'z ichiga oladi. Axborot xavfsizligi texnik, tashkiliy va huquqiy jihatlarni qamrab oladi va axborot tizimlarining barqaror ishlashini, shaxsiy ma'lumotlarning himoyasini va biznes jarayonlarining uzluksizligini ta'minlashga qaratilgan.

**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.

**Axborot maxfiyligi deganda**, axborotga faqat vakolatli shaxslar yoki tizimlar kirish huquqiga ega bo'lishi tushuniladi.

Bu axborotning ruxsatsiz oshkor etilishidan, o'qilishidan yoki foydalanilishidan himoyalanişini anglatadi. Maxfiylikni ta'minlash uchun shifrlash, kirishni boshqarish, autentifikatsiya va boshqa xavfsizlik choralari qo'llaniladi, bu esa axborotning faqat kerakli shaxslar uchun mavjud bo'lishini kafolatlaydi.

**Axborot yaxlitligi deganda**, axborotning to'liqligi, aniqligi va ishonchliligi tushuniladi.

Bu axborotning ruxsatsiz o'zgartirilishidan, yo'q qilinishidan yoki buzilishidan himoyalanişini anglatadi. Yaxlitlikni ta'minlash uchun ma'lumotlarni tekshirish, versiyalarni boshqarish, zaxira nusxalarini yaratish va boshqa xavfsizlik choralari qo'llaniladi, bu esa axborotning asl holatida saqlanishini kafolatlaydi.

**Zararli dasturiy ta'minot deganda**, kompyuter tizimlariga zarar yetkazish, ma'lumotlarni o'g'irlash, buzish yoki ruxsatsiz kirishni ta'minlash uchun mo'ljallangan har qanday dasturiy ta'minot tushuniladi. Bularga viruslar, qurtlar, troyanlar, josuslik dasturlari, to'lov talab qiluvchi dasturlar va boshqa xavfli kodlar kiradi.

Zararli dasturlar tizimning ishlashini buzishi, shaxsiy ma'lumotlarni o'g'irlashi, moliyaviy firibgarliklarga olib kelishi va boshqa ko'plab salbiy oqibatlarga sabab bo'lishi mumkin.

**Zararli dasturiy ta'minotga misollar:**

1) Viruslar: Bular boshqa fayllarga yopishib, ularni zararlaydi va tarqalish uchun foydalanuvchi aralashuvini talab qiladi.

2) Qurtlar (Worms): Tarqalish uchun tarmoqlardan foydalanadi va o'z-o'zidan ko'payadi, foydalanuvchi aralashuvimiz tarqalishi mumkin.

3) Trojanlar (Trojans): O'zini foydali dastur sifatida ko'rsatadi, lekin aslida tizimga zarar yetkazadi yoki ma'lumotlarni o'g'irlaydi.

4) Josuslik dasturlari (Spyware): Foydalanuvchi faoliyatini kuzatib boradi va shaxsiy ma'lumotlarni o'g'irlaydi.

5) To'lov talab qiluvchi dasturlar (Ransomware): Foydalanuvchi ma'lumotlarini shifrlaydi va ularni ochish uchun to'lov talab qiladi.

6) Reklama dasturlari (Adware): Foydalanuvchiga doimiy ravishda reklama ko'rsatadi va tizimni sekinlashtirishi mumkin.

7) Rootkitlar: Zararli dasturni yashirish va tizimga chuqur kirib borish uchun ishlatiladi.

8) Klaviatura josuslari (Keyloggers): Foydalanuvchi kiritgan barcha ma'lumotlarni yozib oladi, shu jumladan loginlar va parollar.

Ushbu dasturlar kompyuter xavfsizligiga jiddiy tahdid soladi va ulardan himoyalangan uchun antivirus dasturlari va xavfsizlik choralari zarur.

**Axborot tizimiga hujum deganda**, axborot tizimining maxfiyligini, yaxlitligini yoki foydalanish imkoniyatini buzishga qaratilgan har qanday harakat tushuniladi.

Bu hujumlar turli shakllarda bo'lishi mumkin, masalan, zararli dasturlarni yuborish, ma'lumotlarni o'g'irlash, tizimni ishdan chiqarish yoki ruxsatsiz kirishga urinish. Hujumlar natijasida axborot tizimi ishdan chiqishi, ma'lumotlar yo'qolishi yoki buzilishi, shuningdek, moliyaviy va reputatsion zarar yetishi mumkin.

**Axborot xavfsizligini ta'minlash** usullari quyidagilarni o'z ichiga oladi:

#### **1) Texnik usullar:**

Antivirus dasturlari: Zararli dasturlarni aniqlash va yo'q qilish uchun.

Devorlar (Firewalls): Tizimga ruxsatsiz kirishni bloklash uchun.

Intruzivlikni aniqlash tizimlari (IDS) va intruzivlikni oldini olish tizimlari (IPS): Xavfli faoliyatni aniqlash va bloklash uchun.

VPN (Virtual Private Network): Internet orqali xavfsiz ulanishni ta'minlash uchun.

Shifrlash: Ma'lumotlarni himoya qilish uchun.

Multi-faktorli autentifikatsiya (MFA): Hisoblarga kirishni himoya qilish uchun.

#### **2) Tashkiliy usullar:**

Xavfsizlik siyosati va standartlari: Xavfsizlik talablarini belgilash va ularga rioya qilish.

Xodimlarni o'qitish: Xavfsizlik xatarlaridan xabardorlikni oshirish va xavfsiz xatti-harakatlarni o'rgatish.

Kirishni boshqarish: Ma'lumotlarga kirish huquqlarini cheklash.

Hodisalarni boshqarish: Xavfsizlik hodisalariga tezkor javob berish va ularni bartaraf etish.

Doimiy monitoring: Tizim xavfsizligini doimiy nazorat qilish.

### **3) Fizik usullar:**

Server xonalarini himoya qilish: Ruqsatsiz kirishni oldini olish.

Ma'lumotlarni saqlash joylarini himoya qilish: Ma'lumotlarni o'g'irlash yoki yo'q qilishdan saqlash.

Xodimlarning fizik xavfsizligini ta'minlash: Xodimlarni tahdidlardan himoya qilish.

### **4) Huquqiy usullar:**

Qonunlar va me'yoriy hujjatlar: Axborot xavfsizligini ta'minlash bo'yicha qonuniy talablarni belgilash.

Shartnomalar: Ma'lumot almashish shartlarini belgilash va xavfsizlik talablarini kiritish.

Ushbu usullarni kompleks ravishda qo'llash axborot xavfsizligini yuqori darajada ta'minlashga yordam beradi.

"Safety" va "Security" tushunchalari ko'pincha bir-biriga o'xshash bo'lib tuyulsa-da, ular turli xil xavflarni bartaraf etishga qaratilgan.

**"Safety" deganda**, odamlarning, mulklarning va atrof-muhitning tasodifiy xavflardan himoyalanganligi holati tushuniladi.

Bu xavflar baxtsiz hodisalar, texnik nosozliklar, tabiiy ofatlar yoki inson xatolari natijasida yuzaga kelishi mumkin. "Safety"ni ta'minlash, xavflarni aniqlash, ularni baholash va oldini olish yoki kamaytirish uchun choralar ko'rishni o'z ichiga oladi. Masalan, yo'l harakati xavfsizligi, mehnat xavfsizligi, yong'in xavfsizligi va boshqa sohalarda "safety"ni ta'minlashga qaratilgan qoidalar va standartlar mavjud.

"Safety" odatda tasodifiy xavflardan, masalan, baxtsiz hodisalar, tabiiy ofatlar yoki texnik nosozliklardan himoya qilishni anglatadi.

**"Security" deganda**, odamlarning, mulklarning, ma'lumotlarning va tizimlarning qasddan qilingan xavflardan himoyalanganligi tushuniladi.

Bu xavflar jinoyatchilik, terrorizm, sabotaj, josuslik, kiberhujumlar va boshqa zarar yetkazishga qaratilgan harakatlar natijasida yuzaga kelishi mumkin. "Security"ni ta'minlash, xavflarni aniqlash, ularni baholash va oldini olish, kamaytirish yoki ularga javob berish uchun choralar ko'rishni o'z ichiga oladi. Bu texnik vositalar (masalan,

kuzatuv kameralari, signalizatsiya tizimlari, firewalllar), tashkiliy choralar (masalan, xavfsizlik siyosati, kirishni boshqarish, xodimlarni o'qitish) va fizik himoya (masalan, qo'riqlash, to'siqlar)ni o'z ichiga olishi mumkin. "Security"ning maqsadi - xavfsizlikni buzishga urinishlarni oldini olish yoki ularga qarshi turish, shuningdek, sodir bo'lgan hodisalarning oqibatlarini kamaytirishdir.

"Security" esa qasddan qilingan xavflardan, masalan, jinoyatchilik, terrorizm yoki kiberhujumlardan himoya qilishni nazarda tutadi.

Demak, "safety" tasodifiy xavflarni kamaytirishga qaratilgan bo'lsa, "security" qasddan qilingan xavflarni oldini olish va ularga qarshi kurashishga yo'naltirilgan.

**Ijtimoiy tarmoqlardan xavfsiz foydalanish** uchun shaxsiy ma'lumotlaringizni himoya qilish, akkauntlaringiz xavfsizligini ta'minlash va onlayn xatti-harakatlaringizga e'tiborli bo'lish muhim.

Profil sozlamalarida shaxsiy ma'lumotlaringizni faqat do'stlaringiz ko'ra oladigan qilib cheklang, murakkab va noyob parollardan foydalaning, ikki faktorli autentifikatsiyani yoqing va shubhali havolalarga bosmang. Shuningdek, onlayn do'stlaringiz bilan shaxsiy ma'lumotlaringizni baham ko'rishda ehtiyot bo'ling, kiberbulling va ta'qib qilish holatlariga duch kelsangiz, darhol xabar bering va ijtimoiy tarmoqlarda o'tkazgan vaqtingizni cheklash orqali ruhiy salomatligingizni saqlang.

**Ma'lumotlarga tahdidlar xususiyatiga** ko'ra turli shakllarda namoyon bo'lishi mumkin, jumladan: viruslar, zararli dasturlar, fishing, kiberhujumlar, ma'lumotlarning o'g'irlanishi yoki yo'q qilinishi, shuningdek, ichki xodimlar tomonidan suiiste'mol qilish.

Bu tahdidlarning oqibatlari juda og'ir bo'lishi mumkin: moliyaviy yo'qotishlar, biznesning to'xtab qolishi, mijozlar ishonchining yo'qolishi, shaxsiy ma'lumotlarning oshkor bo'lishi, reputatsiyaga zarar yetishi va hatto qonuniy javobgarlikka tortilish. Shuning uchun ma'lumotlarni himoya qilish, xavfsizlik choralarini ko'rish va xodimlarni xavfsizlik qoidalariga o'rgatish muhim ahamiyatga ega.

### **1-qadam: Ma'lumotlarga tahdidlarning xususiyatlarini aniqlash**

Zararli dasturlar (Malware): Bularga viruslar, troyanlar, qurtlar, ransomware va spyware kiradi. Ular kompyuter tizimlariga zarar yetkazish, ma'lumotlarni o'g'irlash yoki shifrlash uchun yaratilgan.

Fishing: Bu shaxsiy ma'lumotlarni (parollar, bank hisobi raqamlari va boshqalar) o'g'irlash uchun soxta elektron pochta xabarlar, veb-saytlar yoki xabarlar orqali odamlarni aldash usuli.

Kiberhujumlar: Bularga DDoS hujumlari (xizmatdan voz kechish), SQL inyeksiyalari, cross-site scripting (XSS) va boshqa usullar kiradi, ular veb-saytlar, serverlar va tarmoqlarni ishdan chiqarish yoki ma'lumotlarni o'g'irlash uchun ishlatiladi.

Ichki tahdidlar: Bularga xodimlar tomonidan ma'lumotlarga ruxsatsiz kirish, ma'lumotlarni o'g'irlash yoki yo'q qilish kiradi. Bu qasddan yoki tasodifan sodir bo'lishi mumkin.

Ijtimoiy injeneriya: Bu odamlarni aldash va ulardan ma'lumot olish yoki zararli harakatlarni bajarishga undash usuli.

## **2-qadam: Tahdidlarning oqibatlarini tahlil qilish**

Moliyaviy yo'qotishlar: Ma'lumotlarning o'g'irlanishi, ransomware hujumlari yoki kiberhujumlar natijasida yuzaga kelishi mumkin. Bunga to'lovlar, jarimalar, tizimni tiklash xarajatlari va biznesning to'xtab qolishi kiradi.

Biznesning to'xtab qolishi: Kiberhujumlar yoki tizim nosozliklari natijasida yuzaga kelishi mumkin. Bu mijozlarga xizmat ko'rsatishni to'xtatib qo'yishi, ishlab chiqarishni to'xtatishi va daromadni kamaytirishi mumkin.

Mijozlar ishonchining yo'qolishi: Ma'lumotlarning oshkor bo'lishi yoki kiberhujumlar natijasida yuzaga kelishi mumkin. Bu mijozlarning kompaniyaga bo'lgan ishonchini yo'qotishi va ularning boshqa kompaniyalarga o'tishiga olib kelishi mumkin.

Shaxsiy ma'lumotlarning oshkor bo'lishi: Mijozlar, xodimlar yoki biznes hamkorlarining shaxsiy ma'lumotlari o'g'irlanishi yoki oshkor bo'lishi mumkin. Bu shaxsiy ma'lumotlarning suiiste'mol qilinishiga, shaxsiy hayotning buzilishiga va qonuniy javobgarlikka olib kelishi mumkin.

Reputatsiyaga zarar yetishi: Kiberhujumlar, ma'lumotlarning oshkor bo'lishi yoki boshqa xavfsizlik hodisalari natijasida yuzaga kelishi mumkin. Bu kompaniyaning obro'siga putur yetkazishi va uning biznesiga salbiy ta'sir ko'rsatishi mumkin.

Qonuniy javobgarlik: Ma'lumotlarni himoya qilish qonunlarini buzganlik uchun yuzaga kelishi mumkin. Bunga jarimalar, sud xarajatlari va boshqa qonuniy sanksiyalar kiradi.

## **3-qadam: Tahdidlardan himoyalanish choralarini ko'rish**

Xavfsizlik siyosatini ishlab chiqish va amalga oshirish: Bu siyosat kompaniyaning ma'lumotlarni himoya qilish bo'yicha majburiyatlarini belgilaydi va xavfsizlik qoidalarini, protseduralarini va standartlarini o'z ichiga oladi.

Xavfsizlik texnologiyalarini qo'llash: Bularga firewalllar, antivirus dasturlari, intrusion detection systems (IDS), intrusion prevention systems (IPS) va ma'lumotlarni shifrlash kiradi.

Xodimlarni xavfsizlik qoidalariga o'rgatish: Xodimlar fishing, ijtimoiy injeneriya va boshqa xavfsizlik tahdidlaridan xabardor bo'lishlari kerak. Ular xavfsiz parollarni yaratish, shubhali elektron pochta xabarlariga e'tiborli bo'lish va ma'lumotlarni himoya qilish qoidalariga rioya qilishni o'rganishlari kerak.

Xavfsizlikni muntazam ravishda tekshirish va baholash: Xavfsizlik zaifliklarini aniqlash va ularni bartaraf etish uchun muntazam ravishda xavfsizlik tekshiruvlarini o'tkazish kerak.

Hodisalarga javob berish rejasini ishlab chiqish: Agar xavfsizlik hodisasi sodir bo'lsa, unga tez va samarali javob berish uchun reja bo'lishi kerak. Bu reja hodisani aniqlash, uni bartaraf etish, tizimlarni tiklash va kelajakda bunday hodisalarning oldini olish uchun choralarni ko'rishni o'z ichiga olishi kerak.

### **Nazorat savollarini:**

Axborot xavfsizligiga tahdidlar

- 1) Axborot xavfsizligiga tahdid nima?
- 2) Tahdidlarning qanday turlari mavjud?
- 3) Axborot xavfsizligini buzishning oqibatlari qanday bo'lishi mumkin?

Zararli dasturiy ta'minot

- 4) Zararli dasturiy ta'minot (virus) nima?
- 5) Viruslar kompyuterga qanday yuqadi?
- 6) Viruslardan himoyalaniş uchun nima qilish kerak?

Axborot tizimiga hujum tushunchasi

- 7) Axborot tizimiga hujum nima?
- 8) Hujumlar qanday maqsadda amalga oshiriladi?
- 9) Hujumlardan qanday himoyalaniş mumkin?

Axborot xavfsizligini ta'minlash usullari

- 10) Axborot xavfsizligini ta'minlashning asosiy usullari qanday?
- 11) Parolni qanday qilib xavfsiz saqlash mumkin?
- 12) Firewall nima uchun kerak?

Safety va Security tushunchalari

- 13) Safety va Security o'rtasida qanday farq bor?
- 14) Qaysi biri ko'proq texnik xavfsizlikka tegishli?
- 15) Qaysi biri inson xavfsizligiga tegishli?

Ijtimoiy tarmoqlardan xavfsiz foydalanish

- 16) Ijtimoiy tarmoqlarda qanday xavfsizlik qoidalariga rioya qilish kerak?
- 17) Shaxsiy ma'lumotlarni kimlar bilan baham ko'rish mumkin?
- 18) Kiberbulling nima?

Ma'lumotlarga tahdidlarning xususiyatlari va oqibatlari

- 19) Ma'lumotlarga qanday tahdidlar mavjud?
- 20) Tahdidlarning oqibatlari qanday bo'lishi mumkin?

### **Adabiyotlar**

1. Aminov S.M., Muxamadiyev S.I., Rasulov S.Sh. Axborot kommunikatsion texnologiyalar fanidan amaliy va laboratoriya mashg'ulotlarini bajarish bo'yicha o'quv qo'llanma. –T.:ToshDAU, 2020 yil. – 248 bet.

2. Urdushev X., Mavlyanov M., Eshanqulov S. Sohada axborot-kommunikatsiya texnologiyalari. I-qism. O'quv qo'llanma. – Samarqand: Samarqand davlat veterinariya meditsinasi, chorvachilik va biotexnologiyalar universiteti Nashr matbaa markazi, 2024. 188 b.

3. Urdushev X., Mavlyanov M., Eshanqulov S. Sohada axborot-kommunikatsiya texnologiyalari. II-qism. O'quv qo'llanma. – Samarqand: Samarqand davlat veterinariya meditsinasi, chorvachilik va biotexnologiyalar universiteti Nashr matbaa markazi, 2025. 200 b.

4. D. Watson and H. Williams Computer Science. Hodder Education, 2nd edition, 2023 year. – 404 pages.

5. G. Brown and D. Watson. Cambridge IGCSE ICT. Hodder Education, 3rd edition, 2023 year. – 571 pages.

### **Internet axborot resurslari**

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

<https://www.securitylab.ru/news/529985.php> Магнитные вихри можно использовать 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](https://studopedia.ru/11_70142_programmnie-sredstva-zashchiti-informatsii.html) Программные средства защиты информации — Студопедия

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

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

### **Qo'shimcha materiallar**

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.

**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 rasimga 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:

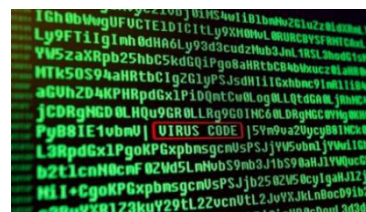
- 1) Ob'yektlar va sub'yektlarni identifikatsiyalash;
- 2) Hisoblash resurslari va axborot resurslariga kirishga cheklovlar o'rnatish;
- 3) Axborot va dasturlar bilan bo'ladigan harakatlarni nazorat va registrasiya qilish.

<https://pirit.biz/resheniya/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 (Qarochi-josus 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, Immundet, 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.

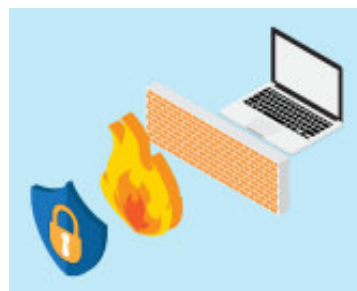


## 4)Kriptografik tizimlar - axborotlarni

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 trafiginı 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](#)