

№1 Лекцияның тақырыбы: Ақпараттық қауіпсіздік негіздері
Қауіпсіздікті қамтамасыз ету үрдісінің жалпы сұлбалары, технологиялары

Лекцияның оқыту нәтижелері: Ақпараттық қауіпсіздік негіздері туралы жалпы мәліметтерді, қауіпсіздікті қамтамасыз етудің жалпы сұлбалары мен технологияларын біледі; Ақпаратты түрлендіру (шифрлау) әдістері мен тәсілдерін ажырата біледі.

Лекция мазмұны:

Ақпараттық қауіпсіздік қорғау жолдары

Адамдар өз тарихында ақпаратты абоненттер арасында беру кезінде оны қорғау мәселесімен үнемі айналысып келеді. Адамзат жіберілген хабарлардың мағынасын қарсыластан жасырудың көптеген жолдарын ойлап тапты. Іс жүзінде құпия хабарламаларды қорғау әдістерінің бірнеше топтары әзірленді. Олардың кейбіреулерін атап өтейік.

Бірінші жол – ақпараттың материалдық тасымалдаушысын қарсыластан ***физикалық қорғау***. Қағаз, компьютерлік тасымалдағыштар (DVD, флэш-карта, магниттік диск, компьютердің қатты дискісі және т.б.) мәліметтерді тасымалдаушы қызметін атқара алады. Бұл әдісті жүзеге асыру үшін сізге ұстап алуға қол жетімсіз сенімді байланыс арнасы қажет. Бұл үшін әр кезде тасымалдаушы көгершіндер, арнайы курьерлер, жасырын жиіліктегі радиохабарлар пайдаланылды. Ақпаратты физикалық қорғау әдістері мәліметтерді өңдеудің қазіргі автоматтандырылған жүйелерінде де қолданылады. Мәселен, күрделі ақпараттық қауіпсіздік жүйелері қоршауларсыз және физикалық оқшаулау жүйелерінсіз, сондай-ақ қауіпсіздік жүйелерінсіз мүмкін емес.

Ақпаратты қорғаудың екінші жолы – ежелгі заманнан белгілі ақпаратты ***стеганографиялық қорғау***. Бұл қорғаныс әдісі қарсыластан оны қызықтыратын ақпараттың болуы фактісін жасыру әрекетіне негізделген. Ақпаратты қорғаудың стеганографиялық әдісі кезінде қарсыластан физикалық деректер тасымалдаушысы жасырылады. Мұндай әдістерге, мысалы, құпия ақпараты бар микрофотографияны құпия емес жерде

«жасыру» жатады: пошта конвертіндегі марканың астына, кітаптың мұқабасының астына және т.б. Стеганографияға сондай-ақ киім түймелерінде, аяқ киім өкшелерінде, тіс пломбаларында және т.б. құпия хабарды «жасыру» сияқты танымал әдістер кіреді. Кейбір әдістер көне заманда-ақ жасалған. Мәселен, мысалы, гректер әдеттен тыс шешім тапты: олар құлдың басын қырып, оған хабарламаларын тырнап сызып жазды.

Құлдың басындағы шашы өскен кезде оны хабар жеткізуге жібереді. Хабар қабылдаушы құлдың шашын қырып, мәтінді оқитын. Өкінішке орай, осылайша хабарлама жіберу және жауап алу үшін бірнеше апта қажет болды.

Кейінгі уақытта химиялық сия осы бағытта кеңінен қолданылды. Құпия емес хабарлама жолдарының арасында осы сиямен жазылған мәтін

көрінбейді. Ол тек белгілі бір көрініс технологиясын қолдану нәтижесінде пайда болды.

Ақпаратты қорғаудың үшінші жолы – бүгінгі күні ең сенімді және кең таралған – **криптографиялық қорғау**. Ақпаратты қорғаудың бұл әдісі оның мағынасын қарсыластан жасыру үшін ақпаратты түрлендіруді көздейді.

Ақпарат – бұл адамдар, заттар, оқиғалар, құбылыстар және процесстер туралы мағлұматтар.



1 - Сурет. Ақпараттың классификациясы

Қорғалатын ақпарат деп, құқықтық құжаттар немесе ақпарат иесінің қойған талаптарына сәйкес қорғалатын ақпаратты айтамыз. Бірақ, барлық ақпараттар қорғала бермейді, тек құнды (бағалы) ақпараттарғана қорғалуы мүмкін. Құнды ақпарат деп, ақпаратты алған адамға қандай да бір ұтыс әкелетін ақпаратты айтамыз: моральдық, материалдық, саяси және т.б.

Ақпарат құндылығы екі үлкен топ бойынша бағалануы тиіс:

- ақпараттың тағайындалуы бойынша;
- оны өңдеу шарттары бойынша.

Бірінші топта екі критерийді көрсетуге болады:

- қауіпсіздікті қамтамасыз ету шараларының маңыздылығы;
- сәйкес шараларды орындау үшін ақпараттың маңыздылық деңгейі.

Екінші топта екі критерийді көрсетуге болады:

- ақпаратты өңдеу кезінде болатын жоғалтулар деңгейі;
- ақпаратты қайта қалпына келтіруге кететін шығындар.

Ақпарат құндылығы оны қорғау бойынша шешім қабылдауда критерий болып табылады. Ақшалық түрде ақпаратты қорғауға кететін шығындар,

мүмкін болған жоғалтулардан аспауы керек.

Маңыздылығы бойынша ақпараттар мына түрлерге бөлінеді:

1) тіршілік үшін маңызды, ауыстыруға болмайтын ақпарат – ол ұйымның жұмыс істеуіне қажетті;

2) маңызды ақпарат – ауыстырылуы немесе қайта қалпына келтірілуі мүмкін болған ақпарат, бірақ қайта қалпына келтіру процесі өте қиын және үлкен шығындармен байланысты;

3) пайдалы ақпарат – қайта қалпына келтіру қиын, бірақ ұйым ол ақпаратсызда жақсы жұмыс істей алады

4) маңызсыз ақпарат – ұйымға енді керек болмаған ақпарат

Маңыздылық категориясы, ақпарат құндылықтары уақыт бойынша өзгереді. Ақпаратты қорғау жолдары ақпарат түріне, оны сақтау формаларына, өңдеу, жіберу және оған мүмкін болған шабуылдарға байланысты.

Ақпарат иесі ақпаратқа қашан, кім, қандай жолмен шабуыл жасайтынын білмейді. Сондықтан ақпарат иесі мына сұрақтарға жауап іздеуі тиіс:

- 1) Қандай ақпарат қорғауды талап етеді?
- 2) Ол ақпарат кімді қызықтырады?
- 3) Ақпараттық қандай элементтері құнды?
- 4) Ақпарат қанша уақыт қорғалуы керек?
- 5) Қорғауға қанша ақша кетеді?

Ақпараттық қауіпсіздік

Ақпараттық қауіпсіздік дегенде ақпараттық жүйенің кездейсоқ немесе қасақана қол сұғу арқылы оның иелеріне немесе ақпарат қолданушыларына зиян алып келуден қорғау.

Практикада ақпараттық қауіпсіздіктің үш аспектісі маңызды болып келеді:

Ақпараттың қол жетерлігі – ақпарат, техникалық жүйелер және өңдеу технологияларының қасиеті болып, ақпаратпен жұмыс істей алатындарға ақпаратқа бөгетсіз рұқсатты қамтамасыз ету.

Ақпарат бүтіндігі – ақпарат техникалық жүйелер және оны өңдеу технологияларының қасиеті болып, ақпаратты рұқсат етілмеген немесе қасақана құртуға және бұрмалауға қарсы тұруды білдіреді.

Ақпарат жасырыны – ақпарат, техникалық жүйелер және оны өңдеу техникаларының қасиеті болып, онымен танысуға құқықтары жоқтардан құпияда сақтауда білдіреді.

Оқытудың техникалық құралдары: Интерактивті тақта, компьютер.

Лекция оқудың тәртібі, оқыту әдістері мен түрлері: баяндау, сұрақ-жауап, түсіндіру, кіріспе лекция.

Өртүрлі күрделілік деңгейдегі тапсырмалар (сұрақтар) және оларды бағалаудағы ұпайлардың үлестірілуі:

• Күрделі деңгей:

1. Хабарларды шифрлау әдістеріне жіктеу схемасын түсіндіріңіз. (50 балл)
2. Криптографиялық жүйенің жалпылама сұлбасын суреттеп беріңіз. (50 балл)

• Орта деңгей:

1. Ақпаратты түрлендіру (шифрлау) әдістері мен тәсілдеріне талдау

жасаңыз.(30 балл)

2. Хабарды шифрлау және ары қарай керішифрлаудың мағынасы неде? (30 балл)

- **Жеңіл деңгей:**

1. Криптология ұғымына анықтама беріңіз және оны ашу әдістерін сипаттаңыз. (20 балл)
2. Криптографиялық әдістер шифрлау алгоритмі типі бойынша екі топқа бөлінуі туралы айтып беріңіз. (20 балл)

БӨЖ және ОБӨЖ тапсырмалары:

1. Әлеуметтік желілердегі ақпараттық қауіпсіздіктің өзекті мәселелері.
2. Ақпараттық қауіпсіздік саласындағы отандық және шетелдік стандарттар.
3. Дербес деректерді қорғаудың құқықтық негіздері.

Әдебиеттер:

Негізгі:

1. Г. Камалова, А. Х. Касимова, Л. Б. Диярова. «Ақпараттық қауіпсіздікті басқару». Оқу құралы. /- Алматы: Альманахъ, 2020. - 128 с.
2. Дүйсебекова, К.С. Ақпараттық қауіпсіздік және ақпараттарды қорғау: Оқу құралы. . - Стер. бас - Алматы: Қазақ университеті, 2020. - 156 б.
<http://rmebrk.kz>
3. Дүйсебекова К.С. Ақпараттық қауіпсіздік және ақпараттарды қорғау. - Алматы : Қазақ университеті, 2013. - 156 б.

Қосымша:

1. Ахметова, С. Бағдарламалау технологиясы : Лекция жинағы. / ЮКГУ им. М.О. Ауезова. - Шымкент: ОҚМУ, 2007. - 51 б. <https://rmebrk.kz/book/50006>
2. Ж.З. Сатмағанбетова. Бағдарламалау тілдері және технологиясы: Оқу-әдістемелік куралы. / Қостанай: А. Байтұрсынов атындағы ҚМУ, 2014. - 64 б.
<http://rmebrk.kz>

WEB сайт:

1. www.rmebrk.kz
2. www.elib.kz

Мына тақырыптар бойынша баяндама презентация дайындау:

1

4. Криптология және оның қалыптасуы мен дамуының