5-ші дәріс. Ақпараттық қауіп-қатерлер. Ақпараттық қауіп-қатерлерге қарсы тұру. Ақпаратты қорғау жүйелерінің сипаттамалық ерекшеліктері.

Қауіпсіздіктің негізгі объектісі – құпия ақпаратқа қол жеткізу режимі. Мұндай жүйелердің ақпараттық қауіпсіздігі осы ақпаратты рұқсатсыз кіруден, жоюдан, өзгертуден және басқа әрекеттерден қорғаудан тұрады.
Ақпарат қауіпсіздігін қамтамасыз ету жүйесі мынадай кіші жүйелерді қамтиды:
- компьютерлік қауіпсіздік;
- деректер қауіпсіздігі;
- қауіпсіз программалық қамтамасыз ету;
- коммуникация қауіпсіздігі.
Компьютерлік қауіпсіздік және сонымен байланысты ресурстардың қолжетімділігін, тұтастығын және құпиялығын қамтамасыз ету мақсатында компьютердің аппараттық құралдарына қатысты қолданылатын технологиялық және әкімшілік шаралар кешенімен қамтамасыз етіледі.
Деректердің қауіпсіздігіне қол жеткізу дегеніміз – деректерді авторланбаған, кездейсоқ, қасақана немесе салғырттықтан туындаған модификациялаудан, бұзылулардан немесе жария болудан қорғау. Ал, қауіпсіз программалық қамтамасыз ету деректерді қауіпсіз өңдейтін және жүйенің ресурстарын қауіпсіз пайдаланатын жалпы жүйелік және қолданбалы программалар мен құралдардан тұрады.
Коммуникация қауіпсіздігі авторланбаған адамдарға жүйенің телекоммуникациялық сұранысқа жауап ретінде беруі мүмкін ақпараттың ұсынылуын болдырмайтын шараларды қабылдау арқылы қамтамасыз етіледі.
Қауіпсіздік саясаты ықтимал қауіп-қатерлерді талдауды және белгілі бір ұйым ақпаратты өңдеу және оны қорғау кезінде қолданатын іс-қимыл нормалары мен ережелерінің жиынтығы болып табылатын тиісті қарсы шараларды таңдауды қамтиды.
Ақпараттық қауіпсіздікке қатер – бұрмалауға, рұқсатсыз пайдалануға немесе жүйені басқарудың ақпараттық ресурстарын, сондай-ақ программалық және аппараттық құралдарды жоюға әкелуі мүмкін оқиғалар немесе әрекеттер.
Ақпаратты қорғау жүйесі – бұл ақпаратты ішкі және сыртқы қауіптерден қорғауды қамтамасыз ететін арнайы органдардың, құралдардың, әдістердің және шаралардың ұйымдасқан жиынтығы.
Ақпараттық қатерлердің туындауына келесі себептер әсер етуі мүмкін:
• табиғи факторлар (өрт, су тасқыны және т.б.);
• адами факторлар.
Соңғысы, өз кезегінде:
• кездейсоқ, байқаусызда болатын қатерлер. Бұл ақпаратты дайындау, өңдеу және беру процесіндегі қателіктерге байланысты туындайтын қатерлер;
• адамдардың әдейі, қасақана әрекеттерінен туындайтын қатерлер. Бұл ААЖ ресурстарына рұқсатсыз кірумен байланысты қатерлер.

Қасақана жасалатын қатерлер ААЖ пайдаланушыларына зиян келтіру мақсатын көздейді және өз кезегінде белсенді және пассивті болып бөлінеді.
Пассивті қатерлер, әдетте, ақпараттық ресурстардың жұмысына әсерін тигізбей, оларды пайдалануға, яғни тыңдауға бағытталған.
Белсенді қатерлер аппараттық, программалық және ақпараттық ресурстарға мақсатты әсер ету арқылы жүйенің қалыпты жұмыс істеу процесін бұзуға бағытталған. Белсенді қатерлерге қастық ойлаушының тікелей әрекеттерін, программалық вирустарды және т.б.жатқызуға болады.
Қасақана қатерлер ішкі, яғни сол ұйымның ішінде туындайтын және сыртқы деп бөлінеді.
Ішкі қатерлер деп ұйымның ресурстарына ішкі субъект (инсайдер) болып табылатын инсайдер (орындаушы) ақпараттың қауіпсіздігіне төнетін қатерлер жатады.
Сыртқы қатерлер деп ақпараттың қауіпсіздігіне қауіп төндіреді, оның бастамашысы (орындаушысы) ұйымның ресурстарынан тыс субъект (қашықтағы хакер, бұзушы) болып табылады.
Сыртқы қатерлер деп ұйымның ресурстарына жат субъект (қашықтағы хакер, бұзушы) бастамашының (орындаушының) ақпараттық қауіпсіздікке төндірген қатерлері.

Ішкі қатерлер

• Ақпараттың жария болуы
• Рұқсатсыз кіру (авторланбаған)

Сыртқы қатерлер

• Зиянды программалар (вирустар, трояндар, құрттар және т.б.)
• Хакерлік шабуылдар
• Ddos- шабуылдары
• Мақсатты шабуылдар
• Спам
• Фишинг
• Өндірістік қатерлер (stuxnet, flame, duqu)
•Тыңшылық программалар (spyware, adware)
• botnets (боттар немесе зомби-желілер)

Заманауи жүйелер пайдаланушының немесе қашықтағы хосттың түпнұсқалығын анықтауға мүмкіндік береді. Бұл жүйелер қол жеткізу субъектісін және оның нақты ресурсқа қатысты өкілеттіктерін біржақты анықтауға арналған.
Сәйкестендіру – бұл субъектіні оның идентификаторы арқылы тану процедурасы. Тіркеу процесінде субъект жүйеге өзінің идентификаторын ұсынады және ол оның деректер қорында болуын тексереді. Жүйе үшін идентификаторлары таныс субъектілер заңды (рұқсат етілген) болып саналады, қалған субъектілер заңсыз болып табылады.
Пароль жүйелерінің негізгі "проблемалық" тұстары:
• соңғы пайдаланушының парольді есте сақтай алмуы, яғни «қиындығы» ұйымның қауіпсіздік саясатын бұзуға әкеледі;
• парольдерді «ашық» түрде сақтау; кіру кезінде парольдің «қорғалмауы»

• арнайы ПҚ қолдану нәтижесінде – «клавиатуралық тыңшылар», «кейлогерлер» және т.б.
• аутентификацияның «тұрақсыз» алгоритмдерін және деректерді берудің ашық арналарын қолдану
• арнайы ПҚ көмегімен жеңіл бұзу – «парольді бұзу»
• парольді жіберу каналы – деректерді берудің шифрланбаған ашық каналы.

Операциялық жүйелерде тағайындалған парольдердің күрделілігіне қойылатын талаптардың стандартты саясатын қолдану қашықтан шабуылдаушыға сөздіктерді пайдаланып есептік жазбаларды бұзуды едәуір қиындатады.