4-ші дәріс. Ақпараттық қауіпсіздіктің техникалық аспектілері.

Ақпаратты қорғаудың бағдарламалық-техникалық құралдары

Программалық-техникалық құралдар, бұл компьютерлік нысандарды – жабдықтарды, программалар және/немесе деректерді басқаруға бағытталған құралдар – ақпараттық қауіпсіздіктің соңғы және маңызды шекарасын құрайды.
Программалық-техникалық деңгейдің негізі қауіпсіздік қызметі болып табылады, оған келесі негізгі және көмекші қызметтер кіреді: сәйкестендіру және аутентификация, хаттамалау және аудит, шифрлау, тұтастықты бақылау, экрандау, ақаулыққа төзімділік, туннельдеу және басқару, RFID технологиялары, штрих – технологиялар.
Жоғарыда аталған қауіпсіздік қызметтерінің жиынтығы толық жиынтық деп аталады. Бұл, негізінен, программалық-техникалық деңгейде сенімді қорғауды құру үшін жеткілікті деп саналады, алайда бірқатар қосымша шарттар сақталған болуы керек (осал жерлердің болмауы, қауіпсіз басқару және т.б.).

Сәйкестендіру мен аутентификацияны программалық және техникалық қауіпсіздік құралдарының негізі деп санауға болады, өйткені қалған сервистер аталған субъектілерге қызмет көрсетуге арналған. Сәйкестендіру және аутентификация – бұл бірінші қорғаныс желісі, ұйымның ақпараттық кеңістігінің «шлюзі».

Сәйкестендіру – пайдаланушының атын орнатуға мүмкіндік беретін процесс. Сәйкестендіруге мысал ретінде визиттік карточканы алуға болады, онда адамның аты-жөні, лауазымы секілді нақты ақпараттар көрсетілген.

Аутентификация – жүйеге енгізілген пайдаланушының аты-жөнінің түпнұсқалығын (шынайылығын) тексеру процесі. Мысалы, пайдаланушының аты-жөнін оның сыртқы түріне сәйкес келетінін фотосуретпен салыстыру арқылы тексеру.

Kerberos аутентификация сервері. Kerberos – бұл 1980 жылдардың ортасында Массачусетс технологиялық институтында жасалған программалық өнім, ол содан бері бірқатар түбегейлі өзгерістерге ұшырады. Kerberos клиенттік компоненттері көптеген заманауи операциялық жүйелерде кездеседі.
Kerberos – бұл қызмет көрсетілетін объектілердің жеке кілттерін иеленетін және оларға жұптық аутентификациялауға көмектесетін сенімді үшінші тұлға (яғни, барлығы сенетін тарап). Ақпараттық технологияларда сәйкестендіру және аутентификация әдістері ұйымның ақпараттық кеңістігіне немесе осы кеңістіктің жеке бөлімдеріне қол жетімділікті қамтамасыз ететін құрал болып табылады.

Сәйкестендіру және аутентификацияның келесі әдістері бар:

- пароль әдістері;
- мамандандырылған аппараттық құралдарды қолдану әдістері;
- пайдаланушының биометриялық сипаттамаларын талдауға негізделген әдістер.

Қазіргі уақытта биометриялық сипаттамаларға негізделген қолданушыны сәйкестендіру құралдарын қолдану ең перспективалы болып табылады, атап айтқанда саусақ ізі, көздің шатырша қабығының суреті, алақан ізі. Бұл әдістердің сенімділігі

айтарлықтай жоғары және пайдаланушыдан күрделі парольдерді есте сақтауды немесе аппараттық сәйкестендірудің қауіпсіздігіне алаңдауды талап етпейді.
Ақпараттық қауіпсіздікті қамтамасыз ету процесінде ақпаратты хаттамалау (тіркеу) мен аудитке ерекше назар аударылады.

Хаттамалау – бұл ақпараттық-есептеу жүйесінде болып жатқан оқиғалар туралы ақпаратты жинау және оларды жинақтап отыру.
Әр программаның жіктеуге болатын әртүрлі оқиғалар жиынтығы бар, оларды сыртқы (басқа программалардың немесе жабдықтардың әрекеттерінен туындаған), ішкі (программаның әрекеттерінен туындаған) және клиенттік (пайдаланушылар мен әкімшілердің әрекеттерінен туындаған) деп жіктеуге болады.
Аудит дегеніміз – жинақталған ақпаратты жедел, нақты бір уақытта немесе мерзімді түрде талдау.

Қауіпсіздік саясаты мен модельдерін, сондай-ақ қауіпсіз ақпараттық жүйелерді құру мен пайдаланудың аксиомалық принциптерін іс жүзінде орындау үшін бірқатар программалық және технологиялық мәселелерді шешу қажет. Бұл мәселелерді келесі бағыттар бойынша топтастыруға болады:
* сәйкестендіру және аутентификация технологиялары;
* деректер базасының қауіпсіздігі;
* объектілерді қайта пайдалану қауіпсіздігін қамтамасыз ету технологиялары;
* сенімді жобалау және әкімшілендіру технологиялары.

Сәйкестендіру және аутентификация

Сәйкестендіру және аутентификация технологиялары қауіпсіз жүйелердің таптырмас элементі болып табылады, өйткені олар субъектілерді дербестендірудің аксиоматикалық принципін қамтамасыз етеді және сол арқылы компьютерлік жүйелерде ақпаратты қорғаудың бірінші (бастапқы) программалық-аппараттық желісін енгізеді.

Сәйкестендіру дегеніміз – субъектілерді, объектілерді, процестерді олардың кескінімен, аттарымен көрсету арқылы ажырату.
Аутентификация дегеніміз – анықталған субъектінің, объектінің, процестің кескінінің түпнұсқалығын тексеру және растау.

Парольдік жүйелер пайдаланушының аутентификация кезінде арнайы құпия сөзді (тек шынайы пайдаланушыға белгілі) немесе таңбалар жиынтығы--парольді ұсынуға негізделген. Пайдаланушы парольді пернетақтадан енгізеді, крипто-трансформациядан өтеді және жүйеде оның сәйкесінше шифрланған есептік көшірмесімен салыстырылады. Сыртқы және ішкі пароль аутентификаторы сәйкес келген кезде тиісті субъектінің түпнұсқалығын тану және растау жүзеге асырылады.
Парольдік жүйелер қарапайым, бірақ парольдерді таңдау мен пайдалану дұрыс ұйымдастырылған жағдайда, атап айтқанда, пайдаланушылар өздерінің парольдерін құпия түрде, аутентификацияның сенімді құралы ретінде сақтаған жағдайда және осы жағдайға байланысты олар кеңінен қолданылады.

Спам – бұл электрондық пошта арқылы келген анонимді хабарламалар, яғни әдеттегі пошта жәшіктерін толтырып тастайтын қағаз жарнамалық хат-хабардың электрондық баламасы. Спам көбінесе тауарлар мен қызметтерді жарнамалау үшін қолданылады. Спамерлер көптеген жарнамалық хабарламалар жібереді және соған жауап беретіндерді пайдаланады. Сонымен қатар, зиянкестер спамды фишингтік шабуылдар жүргізу және зиянды программаларды тарату үшін пайдаланады.