Дәріс 2. Ақпаратты қорғау комплексті тәсілі. Ақпаратты ұйымдық қорғау. Ақпараттық қауіпсіздікті құқықтық қамтамасыз ету. Ақпаратты инженерлі-техникалық, криптографиялық және бағдарламалық–аппараттық қорғау

Ақпараттық қауіпсіздендіру келесі жүйелік қағидалардан құрылуы тиісті:

- жинақтылық;
- қорғаудың үздіксіздігі;
- ақылды жеткіліктілік;
- басқару және қолдану иілгіштігі;
- қорғау алгоритмдерінің және механизмдарының ашықтығы;
- қорғау шараларын және құралдарын қолдану қарапайымдылығы

Жинақтылық қағидасы

Қорғау тұтас жүйелері құру жанында әдістердің және құралдарды комплексті қолдану АЖ қорғауы әр текті құралдардың келісілген қолдануын болжайды, қауіптерді орындау маңызды каналдары барлық қайта жабушының және компоненттердің оның бөлек жапсарларда әлсіз орындарды ұстаушының еместігі болып табылады.

Үздіксіздік қағидасы.

Ақпаратты қорғау - бір жолғы шара емес және өткізілген шаралардың айқын жиынтығы емес және анықталған қорғау құралдары,мақсатқа бағытталған процес, АЖ барлық тіршілік циклы кезеңдеріне лайықты шараларды қабылдау. Қорғау жүйесін өңдеу, қорғайтын жүйені өңдеумен паралель жасалуы тиісті.

Ақылды жеткіліктілік қағидасы.

Абсолютті қорғау жүйесін жасау принципі мүмкін емес. Уақыттың және құралдарды жеткілікті саны жағдайында кез-келген қорғауды жеңуге болады. Сондықтан тек қана қауіпсіздікті қабылдауға болатын деңгейінде әңгіме қозғау мәні бар.

Қорғау иілгіштік қағидасы.

Қорғау жүйесін жасау белгісіздік жағдайында жиі кездеседі. Сондықтан, қабылданған шаралар және анықталған қорғау құралдары, бастапқы дәуірге әсіресе оларды пайдалану, шамадан тыс сияқты, дәл осылай қорғау жеткіліксіз деңгейін қамсыздандыра алады. Қамтамасыз етуге арналған түрлендіру мүмкіншіліктері қорғанушылық деңгейімен, қорғау құралдары айқын иілгіштікке ие болу тиісті.

Алгоритмдердің және қорғау механизмдарының ашықтық қағидасының мәні

Тек қана ұйымдық құрылымның және оның ішкі жүйелерінің жұмыс жасау алгоритмдерінің құпиялығынан қорғауды қамтамасыз етуге тиісті емес. Қорғау жүйесінің жұмыс алгоритмдерін білу оны жеңуге мүмкіндік туғызуға тиісті емес.

Қорғау құралдарын қолдану қарапайым қағидасы.

Қорғау механизмдары интуициялық мәлім болуға тиісті және қолдануда қарапайым. Қорғау құралдарын қолдану арнайы тілдерді білу немесе әрекеттердің орындалуымен байланысты болуы тиісті

емес, көп әрекетті талап ететін маңызды қосымшалар ресми пайдаланушылары әдеттегі жұмысына, сонымен қатар ескішіл түсініксіздеу операциялардың орындалу пайдаланушыларынан талап етуге тиісті емес (бірнеше пароль және аттарды енгізу және т.б.).

Компьютерлік жүйеге ойластырылған қатерлердің типтік тәсілдері және әсер ететін каналдары келесідей болады:

- Қолжетімдік объектілеріне тікелей қатынасы;
- Қорғау құралдарын айналып қол жетімдік объектілеріне қатынас жасайтын бағдарламалық және техникалық құралдарды жасау;
- Қол жетімдік жасауға мүмкіндік беретін қорғау құралдарын өзгерту;
- Компьютерлік жүйенің техникалық құралдарына, функцияларын және құрылымын бұзатын және қол жетімдікті жүзеге асыруға мүмкіндік беретін бағдарламалық және техникалық механизмдерді енгізу.

Ақпаратты алу тәсілі бойынша қол жетімдік каналдарды мыналарға бөлуге болады:

- физикалық;
- электромагниттік (сәулелерді ұстап алу);
- ақпараттық(бағдарламалық– математикалық).

Қол жеткізу әдістері:

- ақпаратты жазу;
- ақпаратты оқу;
- ақпаратты жоюға немесе оны өңдеу және сақтау ережелерін бұзуға әкеліп соғатын КЖ элементтеріне физикалық әсер ету.

Ең көп таралған белгілі әдістер және әсер ететін каналдар мыналар:

- Өңдеуден кейін қалған ақпаратты жинау;
- АЖ-ге оның интерфейстері арқылы біреудің паролін алу жолымен ену;
- «Люк» деп аталатын компьютер мүмкіндіктерін жасырын, құжатталмаған өңдеушілерді қолдану;
- АЖ-ге ақпаратты тасымалдау құралдары арқылы (дискета, CD-ROM) немесе желі арқылы (ЭП, FTP...) бағдарламаларды енгізу;
- Жүйені зерттеуге арналған дизассемблерлер мен отладчиктерді қолдану;
- Қоректену көзін және АЖ компоненттерінің схемасын желі бойынша жоғары күшті импульстерді беру арқылы істен шығару;
- Қосымша электромагниттік сәулелер мен нысаналаулардың (ПЭМИН) эфир немесе комуникация сызықтары бойынша үстап алу;
- Intranet және Internet желілері арқылы желілік шабуылдарды жүргізу.

Әкімшілік аутентификациясының мәліметтерін табуға арналған каналдар маниторингі және ақпараттық ағындардың келесі мүмкіндіктері бар желі протоколдардың анализаторлары:

- Желі ресурстарын қашықтықтан басқару, торабтарға қол жетімдік;
- Желілік трафик жайлы статистикалық мәліметтерді жинау;
- Желі бойынша жіберілетін пакеттерді декодтау.
- Ақпаратты талдау үшін ұстап қалу кезінде мәліметтерді іріктеу.
- Жасырын тыңдау - желілік ағынды ұстау және оны талдау ("sniffing")
- TCP sequence number (IP-spoofing) болжау;
- "десинхрониздік жағдайда" қосуды енгізу
- Пассивті сканерлеу: демондардың қандай TCP-порттарда жұмыс істейтінін анықтау;
- ICMP-пакеттермен ("ping flood") басылу;
- SYN-пакеттермен ("SYN flooding") басылу.

- **Жіберушінің жалған адрестері:**
- Интернеттің электрондық поштасында жіберушілердің адрестеріне сенуге болмайды. Хатты ұстап алу. Пошталық бомба – электрондық пошта арқылы шабуыл жасау:
- Пошталық ақпараттамалар диск толғанша қабылдана береді .
- Кіріс кезегін тағы өңдеу және беру керек хаттамалармен толады.
- Қолданушыға диск квотасы шектен шыққан болуы мүмкін.