**Тәуекелді бағалау әдістері мен бағдарламалық жасақтамасы.**

**CRAMM техникасы**

Бұл ақпараттық қауіпсіздік саласындағы тәуекелдерді талдаудың алғашқы әдістерінің бірі - ол бойынша жұмыс 80-ші жылдардың ортасында басталды. Орталық компьютерлік және телекоммуникация агенттігі (CCTA) Ұлыбритания.

CRAMM әдісі талдаудың сандық және сапалық әдістерін біріктіре отырып, тәуекелдерді бағалаудың кешенді тәсіліне негізделген. Әдіс әмбебап және үлкен және кіші ұйымдарға, үкіметтік және коммерциялық секторларға жарамды.

Әр түрлі ұйымдарға бағытталған CRAMM бағдарламалық жасақтамасының нұсқалары бір-бірінен өздерінің білім қорларымен (профильдерімен) ерекшеленеді. Коммерциялық ұйымдар үшін коммерциялық профиль, мемлекеттік ұйымдар үшін үкіметтік профиль бар. Профильдің үкіметтік нұсқасы американдық ITSEC стандартының талаптарына сәйкестігін тексеруге мүмкіндік береді («Orange Book»).

CRAMM-дегі физикалық ресурстардың мәні оларды жою кезінде қалпына келтіру шығындарымен анықталады.

Деректер мен бағдарламалық жасақтаманың мәні келесі жағдайларда анықталады:

* белгілі бір уақыт кезеңінде ресурстардың қол жетімсіздігі;
* ресурстарды жою - соңғы сақтық көшірмеден кейін алынған ақпараттың жоғалуы немесе оның толық жойылуы;
* персоналдың немесе бөтен адамдардың рұқсат етілмеген қол жеткізуі жағдайында құпиялылықты бұзу;
* модификация - персоналдың кішігірім қателіктері (енгізу қателіктері), бағдарламалау қателіктері, қасақана қателер жағдайлары үшін қарастырылады;
* ақпаратты беруге байланысты қателіктер: жеткізуден бас тарту, ақпаратты жеткізбеу, дұрыс емес мекен-жайға жеткізу.

Ықтимал зиянды бағалау үшін CRAMM келесі параметрлерді қолдануды ұсынады:

* ұйымның беделіне нұқсан келтіру;
* қолданыстағы заңнаманы бұзу;
* персоналдың денсаулығына зиян келтіру;
* жеке тұлғалардың жеке деректерін ашумен байланысты зиян;
* ақпаратты ашудан қаржылық шығындар;
* ресурстарды қалпына келтіруге байланысты қаржылық шығындар;
* міндеттемелерді орындай алмауымен байланысты шығындар;
* қызметті ұйымдастыру.

Мәліметтер мен бағдарламалық жасақтама үшін берілген АЖ-ге қатысты критерийлер таңдалады, ал зақымдану шкаласы бойынша 1-ден 10-ға дейін бағаланады.

CRAMM сипаттамаларында «Ресурстарды қалпына келтіруге байланысты қаржылық шығындар» критерийіне сәйкес осындай рейтингтік шкала мысал келтірілген:

- 2 ұпай - 1000 доллардан аз;

- 6 балл - 1000-нан 10000 долларға дейін;

- 8 ұпай - 10000 доллардан 100000 долларға дейін;

- 10 ұпай - 100 000 доллардан жоғары.

**OCTAVE техникасы**

Бұл техниканың ерекшелігі - бүкіл талдау процесін ұйымның қызметкерлері сыртқы консультанттардың қатысуынсыз жүзеге асырады. Ол үшін техникалық мамандарды да, әртүрлі деңгейдегі менеджерлерді де қамтитын аралас топ құрылады, бұл мүмкін болатын қауіпсіздік оқиғалары және қарсы шараларды әзірлеу бизнесі үшін салдарды жан-жақты бағалауға мүмкіндік береді.

OCTAVE талдаудың үш фазасынан тұрады:

* активке байланысты қауіп профилін әзірлеу;
* инфрақұрылымның осалдығын анықтау;
* қауіпсіздік стратегиялары мен жоспарларын жасау.

Қауіп профилінде активке сілтемелер, активке қол жеткізу түрі, қауіп көзі (әрекет етуші), бұзушылық түрі немесе мотив (түрткі), нәтиже (нәтиже) сілтемелер, жалпы каталогтардағы қауіп сипаттамаларына сілтемелер бар. OCTAVE-дегі қауіп түрлері:

* деректер желісі арқылы әрекет ететін зиянкестен шығатын қатерлер;
* қаскүнемнің физикалық қол жетімділікті қолданатын қауіптері;
* жүйенің істен шығуына байланысты қауіптер;
* басқалар.

**RiskWatch техникасы**

RiskWatch тәуекелдерді талдаудың өзіндік әдістемесін және белгілі бір деңгейде жүзеге асырылатын бағдарламалық жасақтама құралдарын жасады

RiskWatch отбасына қауіпсіздік аудитінің әр түріне арналған бағдарламалық өнімдер кіреді:

• RiskWatch for Physical Security - IP-нің физикалық қорғанысын талдауға арналған;

• Ақпараттық жүйелерге арналған RiskWatch - ақпараттық тәуекелдер үшін;

• Денсаулық сақтау саласына арналған HIPAA-WATCH - негізінен АҚШ-та жұмыс істейтін медициналық мекемелерге қатысты АҚШ медициналық сақтандыру портативтілігі және есеп беру туралы заңының (HIPAA) талаптарына сәйкестігін бағалау;

• ISO 17799 үшін RiskWatch RW17799 - IP-нің ISO 17799 халықаралық стандартының талаптарына сәйкестігін бағалау үшін.

RiskWatch әдісі тәуекелді бағалау мен басқарудың критерийі ретінде жыл сайынғы шығындарды күтуді (ALE) және инвестициялардың кірістілігін (ROI) пайдаланады. RiskWatch қауіпсіздікке қауіп төндіретін шығындар мен қорғаныс шығындары арасындағы байланысты нақты сандық бағалауға бағытталған. RiskWatch өнімі төрт кезеңнен тұратын тәуекелдерді талдау әдістемесіне негізделген.

Бірінші кезең - зерттеу пәнін анықтау. Бұл ұйымның типі, зерттелетін жүйенің құрамы (жалпы түрде), қауіпсіздік саласындағы негізгі талаптар сияқты параметрлерді сипаттайды. Талдаушының жұмысын жеңілдету үшін ұйымның типіне сәйкес шаблондарда («коммерциялық ақпараттық жүйе», «мемлекеттік / әскери ақпараттық жүйе» және т.б.) қорғалатын ресурстар санаттарының тізімдері, шығындар, қауіптер, осалдықтар және қорғау шаралары келтірілген. Олардың ішінен сізге ұйымда барларды таңдау керек

Мысалы, шығындар санаттары:

• кешіктіру және қызмет көрсетуден бас тарту;

• Ақпаратты ашу;

• тікелей шығындар (мысалы, жабдықты өрттің бұзуынан);

• өмірі мен денсаулығы (персонал, тапсырыс берушілер және т.б.);

• деректердің өзгеруі;

• жанама шығындар (мысалы, қалпына келтіру шығындары);

• бедел.