№6 дәріс. АҚПАРАТТЫҚ ҚАУІПСІЗДІК ИНФРАҚҰРЫЛЫМЫ

Жоспары:

1. Ақпараттық қауіпсіздік инфрақұрылымына кіріспе
2. Ақпараттық қауіпсіздік инфрақұрылымының жіктелуі
3. Ақпараттық қауіпсіздік инфрақұрылымының міндеттері мен функциялары
4. Ақпараттық қауіпсіздікке арналған заманауи технологиялар мен құралдар
5. Ақпараттық қауіпсіздік инфрақұрылымының мәселелері мен сын-қатерлері
6. Қорытынды

Ақпараттық қауіпсіздік инфрақұрылымына кіріспе

Ақпараттық қауіпсіздік инфрақұрылымы (АҚ) - бұл ақпарат пен ақпараттық жүйелерді көптеген қауіптер мен осалдықтардан қорғау үшін бірлесіп жұмыс істейтін әдістер, технологиялар, процестер мен адамдар кешені. Деректер ең құнды активтердің бірі болып табылатын қазіргі әлемде ақпаратты қорғау кез-келген ұйым үшін, оның көлеміне немесе қызмет саласына қарамастан маңызды міндетке айналады. Кибершабуылдардың, деректердің бұзылуының және құпиялылық қаупінің үнемі артуы сенімді және тиімді АҚ инфрақұрылымын құру қажеттілігін көрсетеді.

АҚ инфрақұрылымының негізгі компоненттерін үш негізгі элементке бөлуге болады: адамдар, технологиялар және процестер. Қауіпсіздік саясатын жүзеге асыруда адамдар, атап айтқанда Ақпарат қауіпсіздігі мамандары мен пайдаланушылар шешуші рөл атқарады. Олардың ықтимал қауіптер туралы хабардар болуы және қорғаныс әдістерін үйрену тәуекелдерді айтарлықтай төмендетуі мүмкін. Процестер стратегияларды әзірлеуден бастап оқиғаларға жауап беруге дейінгі қауіпсіздікті басқарудың барлық аспектілерін қамтиды. Бұл қызметкерлердің іс-әрекеттерінің біркелкілігін қамтамасыз ету үшін нақты және түсінікті саясаттарды құруды талап етеді.

Бағдарламалық жасақтама мен аппараттық құрал сияқты технологиялар да қауіпсіздікті қамтамасыз етуде маңызды рөл атқарады. Мысалы, брандмауэрлер, антивирустық бағдарламалар, кіруді болдырмау және шифрлау жүйелері деректерді рұқсатсыз кіруден және жоғалтудан қорғауға көмектеседі. Бұл технологиялар үнемі жаңартылып, жаңа қауіптерге бейімделуі керек, өйткені киберқылмыскерлер шабуыл әдістерін үнемі жетілдіріп отырады.

Сонымен қатар, АҚ-ның тиімді инфрақұрылымы деректердің бұзылуын болдырмайды, сонымен қатар егер олар орын алса, оқиғалардың салдарын азайтады. Бұл ұйымдарға клиенттер мен серіктестердің сенімін сақтауға мүмкіндік береді, бұл бизнесті сәтті жүргізудің маңызды аспектісі. Үнемі өзгеріп отыратын қауіп-қатер ландшафтында ұйымдар зиянкестерден бір қадам алда

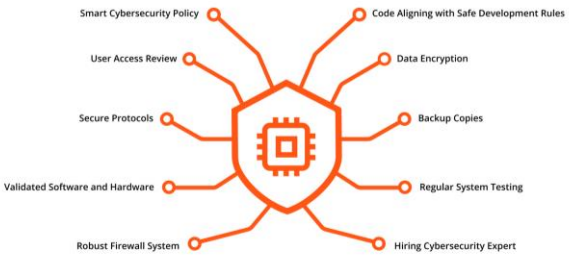
болу үшін қауіпсіздік стратегияларын бейімдеуге және жаңартуға дайын болуы керек. ISO/IEC 27001 сияқты ең жақсы тәжірибелер мен стандарттарды қолдану ақпараттың қауіпсіздігін басқарудың сенімді жүйесін құруға көмектеседі.

Ақпараттық қауіпсіздік инфрақұрылымының жіктелуі

Ақпараттық қауіпсіздік инфрақұрылымын (АҚ) жіктеу оның құрылымы мен ұйымдастырылуын түсіну үшін маңызды. Бұл жіктеу ұйымдық құрылымды, техникалық құралдарды және процестерді қоса алғанда, әртүрлі критерийлер бойынша жүруі мүмкін. Бұл бөлу жалпы қауіпсіздік стратегиясының бөлігі ретінде негізгі элементтер мен олардың функцияларын анықтауға көмектеседі.

Ұйымдық құрылым АҚ инфрақұрылымының маңызды аспектісі болып табылады, өйткені ол қызметкерлер арасында рөлдер мен міндеттердің бөлінуін анықтайды. Мысалы, Ақпарат қауіпсіздігі жөніндегі директор (CISO) қауіпсіздік стратегияларын әзірлеуге және енгізуге жауапты. Ұйымдағы әрбір рөл қауіпсіздікті қамтамасыз ету контекстінде өз міндеттерін нақты түсінуі маңызды. Оқиғаларға жауап беру топтары (CSIRT) оқиғалардың салдарын басқаруда және олардың себептерін талдауда шешуші рөл атқарады, бұл бар процестерді жақсартуға ықпал етеді.

АҚ инфрақұрылымының техникалық құралдары Ақпаратты қорғау үшін қолданылатын жабдықтар мен бағдарламалық жасақтаманы қамтиды. Бұған брандмауэрлер, кірудің алдын алу жүйелері (IDS/IPS), антивирустық бағдарламалар және қауіпсіздікті басқару жүйелері (SIEM) кіреді. Бұл технологиялар ұйымдарға ақпаратқа рұқсатсыз қол жеткізуді болдырмауға және деректердің тұтастығын қамтамасыз етуге көмектесетін көп деңгейлі қорғауды құру арқылы бірге жұмыс істейді.



Сурет 1. АТ инфрақұрылымын Қорғауға арналған киберқауіпсіздік практикасы

Процестер мен процедуралар АҚ инфрақұрылымының тиімді жұмысының негізін құрайды (Сурет 1). Олар қауіпсіздік саясатын құруды және енгізуді, сондай-ақ тұрақты аудиттер мен тәуекелдерді бағалауды қамтиды. Қауіпсіздік саясаты түсіністік пен сәйкестікті қамтамасыз ету үшін барлық қызметкерлер үшін нақты құжатталған және қолжетімді болуы керек. Тәуекелдерді үнемі бағалау осалдықтар мен ықтимал қауіптерді анықтауға мүмкіндік береді, бұл тиімді қорғаныс шараларын әзірлеудің кілті болып табылады.

Сонымен қатар, қызметкерлерді заманауи қауіптер туралы хабардар ету және олардың ақпарат қауіпсіздігін сақтаудағы рөлін түсіну үшін оқыту

маңызды. Ұйымда қауіпсіздік мәдениетін құру хабардарлық деңгейін арттыруға және адам факторына байланысты оқиғалардың ықтималдығын азайтуға ықпал етеді. Осылайша, АҚ инфрақұрылымын дұрыс жіктеу және құрылымдау ақпаратты қорғауға біртұтас және ұйымдасқан тәсілді қамтамасыз етеді.

Ақпараттық қауіпсіздік инфрақұрылымының міндеттері мен функциялары

Ақпараттық қауіпсіздік инфрақұрылымы (ақ) ақпарат пен жүйелерді қорғауға бағытталған көптеген міндеттер мен функцияларды орындайды. Негізгі міндеттер үш негізгі аспектіні қамтамасыз етуге бағытталған: құпиялылық, тұтастық және деректердің қолжетімділігі. CIA моделі деп аталатын бұл модель қауіпсіздік шараларын әзірлеуге және енгізуге негіз болады.

Деректердің құпиялылығын қамтамасыз ету ақпаратты рұқсатсыз кіруден қорғауды білдіреді. Бұған қол жеткізуді басқару, шифрлау және көп факторлы аутентификация технологияларын пайдалану сияқты әртүрлі әдістер арқылы қол жеткізіледі. Қол жеткізуді басқару тек уәкілетті пайдаланушылар үшін деректерге қол жеткізуді шектеуге көмектеседі, бұл жеке және құпия ақпаратты қорғау үшін өте маңызды. Деректерді шифрлау рұқсат етілмеген адамдар оларға қандай да бір жолмен қол жеткізе алса да, оларды қол жетімсіз етуге мүмкіндік береді. Көп факторлы аутентификация, өз кезегінде, пайдаланушылардан бірнеше сәйкестендіру формаларын ұсынуды талап ете отырып, шабуылдаушыларға қиындық туғызады.

Деректердің тұтастығын қамтамасыз ету ақпараттың өмір бойы өзгеріссіз және дәл болуын қамтамасыз етеді. Осы мақсатқа жету үшін бақылау сомалары, хэштеу және интрузияны анықтау жүйелері (IDS) қолданылады. Бұл технологиялар деректердің рұқсатсыз өзгеруін анықтауға және алдын алуға көмектеседі, бұл ұйымдарға ақпаратқа деген сенімділіктің жоғары деңгейін сақтауға мүмкіндік береді. Мысалы, цифрлық қолтаңбаларды қолдану деректердің тұтастығын тексеруге және олардың көзін анықтауға мүмкіндік береді.

Деректердің қолжетімділігін қамтамасыз ету ақпарат кез келген уақытта Уәкілетті пайдаланушылар үшін қолжетімді болуы керек дегенді білдіреді. Бұған деректердің сақтық көшірмесін жасау, апаттан кейін қалпына келтіру жоспарларын құру және сервер жүктемесін басқару арқылы қол жеткізіледі. Сенімді сақтық көшірме жүйелері деректерді жоғалтқан немесе бүлінген жағдайда қалпына келтіруге көмектеседі, ал оқиға болған жағдайда нақты іс-қимыл жоспарының болуы Бос уақыт пен бизнестің салдарын азайтуға мүмкіндік береді.

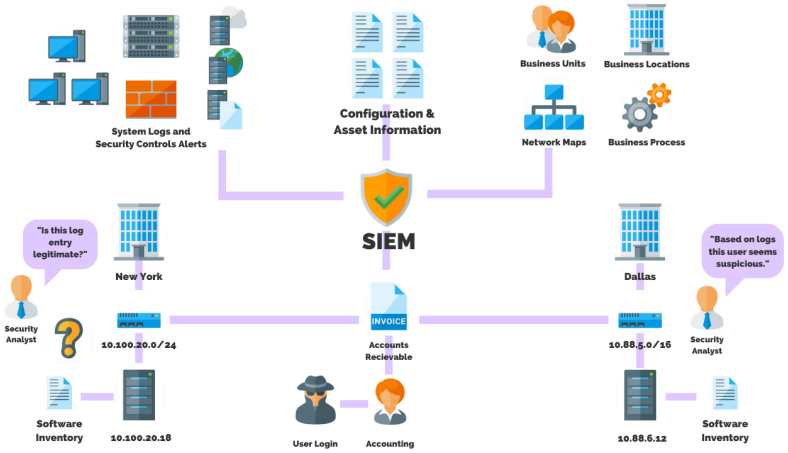
Сонымен қатар, барлық үш аспект бір-бірімен байланысты: егер олардың біреуі бұзылса, бұл бизнес үшін ауыр зардаптарға әкелуі мүмкін. Мысалы, құпиялылықты жоғалту қаржылық шығындар мен беделге нұқсан келтіруі мүмкін, ал деректердің қол жетімсіздігі бизнес-процестерді бұзып,

тұтынушылардың жоғалуына әкелуі мүмкін. Сондықтан осы аспектілердің әрқайсысын тиімді басқарудың маңыздылығын асыра бағалау қиын.

Ақпараттық қауіпсіздікке арналған заманауи технологиялар мен құралдар

Заманауи технологиялар ақпараттық қауіпсіздіктің (ақ) тиімді инфрақұрылымын құруда және қолдауда шешуші рөл атқарады. Олар ұйымдарға көптеген құралдар мен шешімдерді қолдана отырып, өз деректері мен жүйелерін көптеген қауіптерден қорғауға мүмкіндік береді. Енгізілетін негізгі технологияларға қауіпсіздікті басқару жүйелері (SIEM), брандмауэрлер, антивирустық бағдарламалар, кіруді анықтау және алдын алу жүйелері (IDS/IPS) және шифрлау әдістері кіреді.

Қауіпсіздікті басқару жүйелері (SIEM, Сурет 2) - Бұл Нақты уақыттағы әртүрлі көздерден қауіпсіздік оқиғалары туралы деректерді жинайтын және талдайтын кешенді шешімдер. Бұл жүйелер қауіпсіздікті орталықтандырылған бақылауды қамтамасыз ету арқылы оқиғаларды анықтауға және оларға жауап беруге көмектеседі. Олар сондай-ақ есептер мен хабарламалар жасай алады, бұл ұйымдарға ықтимал қауіптерге тез жауап беруге мүмкіндік береді. SIEM жүйелері әсіресе киберқауіптердің күрделілігі мен әртүрлілігі жағдайында өзекті бола бастайды, бұл ұйымдарға деректердің үлкен көлемін талдауға және шабуыл әрекеттерін көрсете алатын ауытқуларды табуға мүмкіндік береді.



Сурет 2. SIEM диаграммасы

Брандмауэрлер мен антивирустық бағдарламалар желі мен құрылғыларды қорғаудың бірінші деңгейін құрайды. Брандмауэрлер кіріс және шығыс трафикті басқарады, қалаусыз кіруді блоктайды және жүйелерге шабуылдардың алдын алады. Антивирустық бағдарламалар, өз кезегінде, соңғы құрылғыларды зиянды бағдарламалардан қорғайды, бұл үлкен зиян келтіруі мүмкін. Бұл технологиялар жаңа осалдықтар мен қауіптерден қорғауды қамтамасыз ету үшін үнемі жаңартылып отыруы керек.

Шифрлау және аутентификация деректердің қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады. Шифрлау деректерді беру және сақтау кезінде қорғауға мүмкіндік береді, бұл ақпаратты рұқсат етілмеген пайдаланушылар үшін қол жетімді етпейді. Деректерді барынша қорғау үшін ұйымдар AES (Advanced

Encryption Standard) сияқты заманауи шифрлау стандарттарын қолдануы маңызды. Пайдаланушының аутентификациясы парольдер, биометрика және бір реттік таңбалауыштар сияқты әртүрлі әдістерді қолдана отырып, олардың жеке басын растайды. Тиімді аутентификация жүйелері ұйымның жалпы қауіпсіздігін нығайта отырып, жүйелер мен деректерге рұқсатсыз қол жеткізуді болдырмауға көмектеседі.

Қызметкерлерді оқыту да маңызды аспект болып табылады, өйткені бұл көбінесе қауіпсіздік жүйесіндегі әлсіз буынға айналатын адам факторы. Тұрақты тренингтер мен киберқауіптер туралы хабардарлықты арттыру ұйым ішінде қауіпсіздік мәдениетін қалыптастыруға көмектеседі, осылайша қорғаныс технологиялары мен құралдарын тиімді пайдалануға ықпал етеді. Осылайша, АҚ инфрақұрылымына заманауи технологияларды енгізу ұйымның қауіпсіздік деңгейін және киберқауіптерге төзімділігін айтарлықтай арттырады.

Firewall (брандмауэр)

Firewall немесе брандмауэр-ақпараттық қауіпсіздік инфрақұрылымының негізгі компоненттерінің бірі. Оның негізгі функциясы берілген қауіпсіздік ережелеріне байланысты кіріс және шығыс желілік трафикті бақылау және бақылау болып табылады. Брандмауэрлер бағдарламалық жасақтама немесе аппараттық құрал болуы мүмкін және желіні рұқсатсыз кіруден, шабуылдардан және зиянды бағдарламалардан қорғау үшін қолданылады.

1. Жұмыс принциптері: брандмауэрлер IP мекенжайлары, порттар және протоколдар сияқты әртүрлі параметрлерге негізделген ережелерді орнату арқылы пакеттерді сүзу принципі бойынша жұмыс істейді. Мысалы, әкімшілер белгілі бір веб-сайттарға немесе қолданбаларға кіруге тыйым сала алады, сонымен қатар трафикке тек белгілі бір көздерден рұқсат бере алады. Заманауи брандмауэрлер сонымен қатар қауіптерді анықтау үшін деректер пакетінің мазмұнын талдайтын терең пакетті тексеру (DPI) сияқты күрделі әдістерді қолдана алады.

2. Брандмауэр түрлері:

Пакеттік сүзгілер: деректер пакеттерін белгіленген ережелерге сәйкестігін тексеретін қарапайым құрылғылар.

Желілік брандмауэрлер: желілік Протокол деңгейінде жұмыс істейді және трафиктің үлкен көлемін өңдей алады.

Прокси-серверлер: деректерді сүзуге және кэштеуге мүмкіндік беретін клиент пен сервер арасындағы аралық түйін ретінде әрекет етеді.

Интрузияның алдын алу жүйелері (IPS): олар желілік шабуылдарды анықтау және алдын алу үшін брандмауэр мүмкіндіктерін бақылау мүмкіндіктерімен біріктіреді.

3. Қауіпсіздіктегі рөлі: брандмауэр шабуылдаушылардың ішкі ресурстарға қол жеткізуіне жол бермей, ұйымды сыртқы қауіптерден қорғауға көмектеседі. Олар сондай-ақ қызметкерлердің белгілі бір ресурстарға қол жеткізуін шектеу үшін пайдаланылуы мүмкін, бұл жалпы қауіпсіздік деңгейін арттырады.

VPN (виртуалды жеке желі)

VPN (Virtual Private Network) — пайдаланушы мен интернет арасында немесе екі желі арасында қауіпсіз және шифрланған байланысты қамтамасыз ететін технология. VPN клиент пен сервер арасында берілетін деректерді шифрлайды, бұл оны бөгде адамдар үшін қол жетімді етпейді.

1. Жұмыс принциптері: VPN ақпаратты ұстап қалудан және бұзудан қорғайтын шифрланған "туннель" жасайды. Пайдаланушы vpn серверіне қосылады, содан кейін ол интернет-трафикті шифрлайды және қайта бағыттайды. Бұл пайдаланушының нақты IP мекенжайын жасыруға және географиялық шектеулерді айналып өтуге мүмкіндік береді.

2. VPN пайдаланудың артықшылықтары:

Деректерді қорғау: шифрлау деректерді ұстап қалудан қорғайды, әсіресе қоғамдық Wi-Fi желілерін пайдалану кезінде.

Құпиялылық: пайдаланушының IP-мекен-жайын жасыру интернеттегі әрекеттерді қадағаламауға көмектеседі.

Қашықтан қол жеткізу: VPN қызметкерлерге корпоративтік желіге қосылу және ресурстарға кеңседе болғандай қол жеткізу арқылы әлемнің кез келген жерінен жұмыс істеуге мүмкіндік береді.

3. Ұйымдарда қолдану: VPN корпоративтік ресурстарға қауіпсіз қол жетімділікті қамтамасыз ету үшін ұйымдарда кеңінен қолданылады. Бұл, әсіресе, жұмысшылар кеңседен тыс жерде қауіпсіз деректерге қол жеткізуді қажет ететін қашықтағы немесе шашыраңқы кеңселері бар компанияларға қатысты. VPN сонымен қатар құпия ақпаратты беру кезінде қауіпсіздікті қамтамасыз етуге көмектеседі, бұл оны ақпараттық қауіпсіздік инфрақұрылымының маңызды құралы етеді.

Ақпараттық қауіпсіздік инфрақұрылымының мәселелері мен сын-қатерлері

Ақпараттық қауіпсіздік инфрақұрылымы (ақ) ақпараттың қорғалуын қамтамасыз ету үшін назар аударуды және шешуді қажет ететін көптеген мәселелер мен қиындықтарға тап болады. Негізгі қиындықтардың бірі-кибершабуылдардың саны мен күрделілігінің артуы. Қазіргі зиянкестер жүйелерді бұзу үшін барған сайын жетілдірілген әдістерді қолданады, бұл қорғаныс технологиялары мен әдістерін үнемі жаңартып отыру қажеттілігін тудырады. Мысалы, әзірлеушілер әлі білмейтін осалдықтарды пайдаланатын нөлдік күндік шабуылдар үлкен қауіп төндіруі мүмкін, өйткені оларға дайындалу және жауап беру қиын.

Тағы бір маңызды мәселе - адам факторы. Фишингтік хаттарды ашу немесе әлсіз құпия сөздерді пайдалану сияқты қызметкерлердің қателіктері көбінесе сәтті шабуылдарға әкеледі. Сондықтан қызметкерлерді оқыту және хабардар ету адам факторына байланысты тәуекелдерді азайту үшін маңызды болады. Қауіпсіздік бойынша тұрақты тренингтер, киберқауіптер туралы хабардар

болуды тестілеу және технологияны пайдалану бойынша нақты саясаттарды құру пайдаланушылардың қателіктеріне байланысты оқиғалардың ықтималдығын азайтуға көмектеседі.

Заңнамалық және этикалық аспектілер де ұйымдар үшін маңызды міндеттерді білдіреді. Деректерді қорғаудың жалпы ережесі (GDPR) және жеке ақпаратты қорғау туралы Заң (HIPAA) сияқты нормалар мен стандарттарды сақтау компаниялардан айтарлықтай күш пен ресурстарды талап етеді. Заң талаптарын орындай алмау айыппұлдар мен беделді шығындарға әкелуі мүмкін. Сондықтан талаптарды сақтау ғана емес, сонымен қатар клиенттер мен серіктестердің сенімін арттыруға ықпал ететін этикалық стандарттарға сәйкес келетін ішкі саясатты әзірлеу маңызды.

Сонымен қатар, көптеген ұйымдар ресурстардың жетіспеушілігі мен ақпараттық қауіпсіздік саласындағы білікті мамандарға тап болады. Еңбек нарығы өсіп келе жатқан қажеттіліктерге ілесе алмайды және көптеген компаниялар қауіпсіздік мамандарын жалдау және сақтау қиынға соғады. Бұл қолданыстағы командаларға қосымша стресс туғызады, бұл шаршауға және жұмыс тиімділігінің төмендеуіне әкелуі мүмкін.

Сайып келгенде, ақ инфрақұрылымын тиімді басқару үшін ұйымдар осы аспектілердің барлығын ескеретін стратегияларды әзірлеуі керек. Бұл технологиялар мен құралдарды енгізуді ғана емес, сонымен қатар қауіпсіздік мәдениетін, тиісті заңнамалық нормаларды құруды және қызметкерлерді қауіп-қатерлерге тиімді жауап беруге дайындауды қамтиды. Үнемі жетілдіру және жаңа сын-қатерлерге бейімделу ақпараттық қауіпсіздік саласындағы табысты жұмыстың негізгі факторлары болып табылады.

Қорытынды

Қорытындылай келе, ақпараттық қауіпсіздік инфрақұрылымы (ақ) ақпарат пен жүйелерді әртүрлі қауіптерден қорғаудың маңызды аспектісі болып табылады. Тиімді АҚ заманауи технологияларды қолдануды, қызметкерлерді оқытуды, саясат пен процестерді әзірлеуді және қауіпсіздік стратегияларын үнемі жаңартуды қамтитын кешенді тәсілді қажет етеді. Кибершабуылдар мен қауіптердің көбеюі жағдайында ақпаратты қорғау барлық көлемдегі және саладағы ұйымдар үшін маңызды міндетке айналады.

АҚ инфрақұрылымына салынған инвестициялар деректерді қорғап қана қоймай, клиенттер мен серіктестердің сенімін нығайтады. Сенімді қауіпсіздік жүйесін құру деректердің бұзылуымен және кибершабуылдармен байланысты тәуекелдерді азайтуға мүмкіндік береді, бұл өз кезегінде бизнестің тұрақты дамуына ықпал етеді. Сонымен қатар, заңнамалық нормалар мен стандарттарды сақтау қазіргі заманғы бизнес жағдайында ұйымдардың табысты жұмыс істеуі үшін міндетті шарт болып табылады.

Ұйымдар қауіпсіздік мәдениетін қалыптастырудың маңыздылығын да есте ұстауы керек, мұнда әр қызметкер ақпаратты қорғаудағы өз рөлін түсінеді. Тұрақты тренингтер мен киберқауіптер туралы хабардарлықты арттыру

тәуекелдерді білетін және оқиғаларға тиімді жауап бере алатын ұжым құруға көмектеседі. Бұл мәдениет жалпы қауіпсіздік стратегиясының маңызды бөлігіне айналады және ұйымға ықтимал зиянкестерден бір қадам алда болуға көмектеседі.

Ақырында, технологияның қарқынды дамуы және қауіп ландшафтының өзгеруі жағдайында ұйымдар қауіпсіздік стратегияларын үнемі бейімдеп, жаңартып отыруы керек. Бұған жаңа қауіптерді бақылау, осалдықтарды талдау және заманауи қорғаныс технологияларын енгізу кіреді. Ақпарат қауіпсіздігіне кешенді және белсенді көзқарас қана сенімді қорғауды қамтамасыз ете алады және ықтимал оқиғалардың салдарын азайтады.

Бақылау сұрақтары:

1. Ақпараттық қауіпсіздік инфрақұрылымы дегеніміз не, және оның негізгі компоненты қандай?
2. Ақпараттық қауіпсіздік инфрақұрылымындағы құпиялылық, тұтастық және қолжетімділік принциптерін (триадасы ЦРУ) түсіндіріңіз.
3. Киберқатерлердің негізгі түрлерін атаңыз және олардың әрқайсысының мысалдарын келтіріңіз.
4. Ақпараттық қауіпсіздік инфрақұрылымында брандмауэрлер (брандмауэры) қандай рөл атқарады?
5. Антивирустық бағдарламалық қамтамасыз этудің рөлі қандай және оның негізгі қызметтері қандай?
6. Криптография және шифрлау әдістері ақпараттық қауіпсиздікті қалай қамтамасыз етеді?
7. Аутентификация мен авторизация арасындағы айырмашылықты түсіндіріңіз.
8. Қауіпсіздік оқиғалары мужчины в случае инцидента в любой момент және оларға жауап беру жүйелери (IDS/IPS) дегенимиз не және олар қалай жұмыс істейді?
9. Ақпараттық қауіпсіздік инфрақұрылымында қауіп-қатерлерді басқару және бағалау тәсілдерін сипаттаңыз.
10. Ақпараттық қауіпсиздікте әлеуметтик инженерия әдістері қалай қолданылады және олардан қалай қорғануға болады?

Ұсынылған әдебиеттер:

Негізгі әдебиеттер:

1. Основы информационной безопасности. М.: Издательство "БИНОМ", 2020.
2. Stamp, M. Information Security: Principles and Practice. 3rd ed. New York: Wiley, 2018.
3. The Cybersecurity Landscape: Trends and Implications. Journal of Cyber security Research, 2022.
3. Human Factor in Cybersecurity: Threats and Solutions. International Journal of Information Security, 2021.

4. GDPR (General Data Protection Regulation). Brussels: European Union, 2016.
5. Национальный институт стандартов и технологий (NIST)

Қосымша әдебиеттер:

6. Krebs, B. Krebs on Security. Available online: https://krebsonsecurity.com.
7. CISA (Cybersecurity & Infrastructure Security Agency). Available online: https://www.cisa.gov.
8. Coursera. Courses on Cybersecurity. Available online: https://www.coursera.org.
9. NIST Cybersecurity Framework. National Institute of Standards and Technology, 2023. Available online: https://www.nist.gov/cyberframework.
10. ISACA. Information Security Resources. Available online: https://www.isaca.org.