ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ІШКІ ІСТЕР МИНИСТРЛІГІ

Бәрімбек Бейсенов атындағы Қарағанды академиясы

Е.П. ШУЛЬГИН, Ж.Н. САПАРҒАЛИЕВ,
Е.О. ДОСЫМБЕТОВ, П.А. ТАФИНЦЕВ

АҚПАРАТТЫҚ ҚАУІПСІЗДІККЕ ӘРЕКЕТ ЕТУДІ ҰЙЫМДАСТЫРУ

ОҚУ ҚҰРАЛЫ

ҚАРАҒАНДЫ-2023

Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясының оқу-әдістемелік кеңесінің 2023 жылғы 20 шілдедегі № 11 хаттамасымен бекітілген шешімі бойынша жарияланады.

Рецензенттер: Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасының бастығы полиция полковнигі ***Б.Т. Байсеитов*;** Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясының қылмыстық процесс кафедрасының бастығы, заң ғылымдарының кандидаты, полиция полковнигі ***Т.Н. Сулейменов.***

Құрастырушылар: киберқауіпсіздік және ақпараттық технологиялар кафедрасының бастығы з.ғ.к., полиция майоры *Е.П. Шульгин*; киберқауіпсіздік және ақпараттық технологиялар кафедрасының аға оқытушысы з.ғ.м., полиция подполковнигі *Ж.Н. Сапарғалиев*; киберқауіпсіздік және ақпараттық технологиялар кафедрасының оқытушысы полиция майоры *Е.О. Досымбетов*; киберқауіпсіздік және ақпараттық технологиялар кафедрасының аға оқытушысы з.ғ.м., полиция майоры *П.А. Тафинцев.*

Шульгин Е.П., Сапарғалиев Ж.Н., Досымбетов Е.О., Тафинцев П.А. Ақпараттық қауіпсіздікке әрекет етуді ұйымдастыру: оқу құралы. – Қарағанды: Қазақстан Республикасы ІІМ Бәрімбек Бейсенов атындағы Қарағанды академиясы, 2023. – 63 б.

Бұл оқу құралы курсанттарға, ақпараттық қауіпсіздік және құқық қорғау саласындағы мамандарға, сондай-ақ компьютерлік ақпарат саласындағы алаяқтық мәселелеріне қызығушылық танытқандарға арналған. Онда мұндай қылмыстарды тергеудің ерекшеліктері, сондай-ақ тергеу кезінде қолданылатын әдістер мен құралдар қарастырылған.

Оқу құралы құқық қолдану қызметін жүзеге асыратын органдардың қызметкерлері, сондай-ақ Қазақстан Республикасы ІІМ жоғары оқу орындарының оқытушылары, докторанттары, магистранттары мен курсанттары үшін қызығушылық тудырады.

МАЗМҰНЫ

КІРІСПЕ

Қазіргі уақытта ақпараттық технологиялар мен деректерді бұзудың дамуымен ақпараттың қауіпсіздігін қамтамасыз ету әртүрлі көлемдегі ұйымдар үшін маңызды міндетке айналуда. Бұл нұсқаулықта біз ақпараттық қауіпсіздік инциденттеріне жауап беруді ұйымдастырудың негізгі аспектілерін қарастырамыз, мысалы, инциденттерді анықтау, жауап беру тобын құру, стратегияны әзірлеу және т.б.

Барған сайын дамып келе жатқан киберқауіптер мен шабуылдарды ескере отырып, компаниялар өздерінің ақпараттары мен деректерін қорғау үшін барлық қажетті шараларды қабылдауы керек.

Ақпараттық қауіпсіздік оқиғаларына жауап беру-бұл туындаған мәселелерге тиімді және жедел жауап беруге және ықтимал зиянды азайтуға мүмкіндік беретін процесс. Оқиға болған жағдайда қандай қадамдар жасау керектігін анықтайтын толық іс-қимыл жоспарының болуы маңызды.

Ақпараттық қауіпсіздік инциденттеріне жауап беруді ұйымдастырудың алғашқы қадамы инциденттерге жауап беруге жауапты арнайы команда құру болып табылады. Бұл команда туындаған мәселелерді бірлесіп шешу үшін IT, заң бөлімі және PR сияқты әртүрлі бөлімдердің өкілдерін қамтуы керек.

Келесі қадам оқиға болған жағдайда егжей тегжейлі іс қимыл жоспарын жасау. Бұл жоспарда жауап беру тобының әрбір мүшесінің рөлдері мен міндеттері, сондай-ақ зиянды азайту үшін жасалуы керек қадамдар көрсетілуі керек. Жоспар қауіптің жаңа түрлері мен технологияларын ескеру үшін икемді және жаңартылатын болуы керек.

Топ мүшелерін үнемі оқыту және практикалық жаттығулар өткізу ақпараттық қауіпсіздік оқиғаларына жауап беруді ұйымдастырудың маңызды аспектісі болып табылады. Тек сауатты дайындалған мамандар туындаған проблемаларға тиімді жауап бере алады және оларды шешудің жолдарын тез таба алады.

Сонымен қатар, компанияларда ақпараттық қауіпсіздік оқиғаларын анықтау тетіктері болуы керек. Мұны бақылау жүйелері, белсенділік журналын талдау, интрузияны анықтау жүйелері және басқа құралдар арқылы жүзеге асыруға болады. Оқиғалар неғұрлым тез анықталса, соғұрлым олар тезірек назар аударып, әрекет ете алады.

Клиенттер, серіктестер және реттеушілер сияқты мүдделі тараптармен байланыс жоспарын дайындау да маңызды. Дұрыс қарым-қатынас дүрбелеңді болдырмауға және мүдделі тараптардың сенімін сақтауға көмектеседі.

Тұтастай алғанда, ақпараттық қауіпсіздік инциденттеріне ден қоюды ұйымдастыру кешенді және көп сатылы процесс болып табылады. Бұған топ құру, іс-қимыл жоспарын құру, қызметкерлерді оқыту және бақылау және анықтау жүйелерін қамтамасыз ету кіреді. Тек ұқыпты жоспарлау және сауатты ұйымдастыру компанияға туындаған проблемалар мен минимизацияларға тиімді жауап беруге мүмкіндік береді.

§1. Компьютерлік қылмыс және ақпараттық қауіпсіздік инциденті ұғымдары

Қазіргі қылмыс барған сайын кәсіби болып келеді. Қылмыстық әлемнің кәсібилігінің көрсеткіші ретінде компьютерлік қылмыс сияқты қылмыстың пайда болуын атауға болады. Оның заманауи ауқымы ақпаратты қорғау бойынша ең белсенді жұмысты талап етеді.

Жағдай күрделене түседі, өйткені құқық қорғау органдарының өздері де заманауи есептеу техникасымен қаруланған қылмыскерлердің назарына айналады. Сондықтан бүгінгі таңда ішкі істер органдары үшін өзекті мәселе өз ақпаратын қорғау болды.

Ақпараттық қауіпсіздік-бұл ақпарат иелеріне немесе пайдаланушыларға және қолдау инфрақұрылымына зиян келтіруі мүмкін табиғи немесе жасанды сипаттағы кездейсоқ немесе қасақана әсерлерден ақпарат пен қолдау инфрақұрылымының қорғалуы.

Ақпараттық қауіпсіздік мәселесі, әсіресе ішкі істер органдары үшін бүгінгі таңда үлкен қызығушылық тудырады. Компьютерлік қылмысқа қарсы күрес-ақпараттық жүйелердің, жергілікті және жаһандық желілердің орасан зор дамуы аясында құқық қорғау органдарының маңызды міндеттерінің бірі.

Компьютерлік қылмыс пен ақпараттық қауіпсіздік оқиғасы қазіргі әлемде өзекті және маңызды мәселелер болып табылады, мұнда ақпараттық технологиялар біздің өмірімізде маңызды рөл атқарады.

Компьютерлік қылмыс ұғымы ақпараттық технологиялар мен компьютерлік желілерді қолдану арқылы жасалған кез-келген заңсыз әрекеттерді білдіреді. Компьютерлік қылмыстарға хакерлік, хакерлік, жеке басын ұрлау, зиянды бағдарламалық жасақтаманы тарату және ақпараттық қауіпсіздік заңдары мен ережелерін бұзатын басқа да әрекеттер жатады.

Ақпараттық қауіпсіздік оқиғасы өз кезегінде ақпараттың қауіпсіздігін қамтамасыз етуге байланысты нормалар мен ережелерді бұзуды білдіреді. Бұл компьютерлік қылмыстың нәтижесі немесе жүйенің жұмысындағы кездейсоқтық немесе қателік болуы мүмкін. Мұндай оқиғалар маңызды ақпаратқа рұқсатсыз қол жеткізуге, оның жоғалуына немесе ағып кетуіне, құпиялылықтың бұзылуына немесе деректердің тұтастығына әкелуі мүмкін.

Компьютерлік қылмыстар мен ақпараттық қауіпсіздік инциденттерінің өсуінің негізгі себептерінің бірі - ақпараттық технологияларды біздің өміріміздің әртүрлі салаларына-банк жүйесі мен коммерциялық компаниялардан бастап мемлекеттік мекемелер мен білім беру мекемелеріне дейін жан-жақты енгізу болып табылады. Сандық ақпарат пен технологияға тәуелділіктің артуы бізді компьютерлік қылмыскерлерге және ақпаратқа рұқсатсыз қол жеткізуге осал етеді.

Компьютерлік қылмыстармен күресу және ақпараттық қауіпсіздік оқиғаларының алдын алу үшін әртүрлі шаралар мен құралдар бар. Бұған антивирустық бағдарламалық жасақтаманы орнату, күшті парольдерді пайдалану, деректерді шифрлау, бағдарламалық жасақтаманы үнемі жаңартып отыру және қызметкерлерді ақпараттық қауіпсіздік ережелеріне үйрету кіреді.

Компьютерлік қылмыстар мен ақпараттық қауіпсіздік инциденттерін барынша байыпты қарастыру және компаниялар мен мемлекеттердің қауіпсіздік жоспарлары мен даму стратегияларына енгізу қажет. Жаңа технологияларды дамыту ақпаратты қорғау жүйесін үнемі жетілдіруді және қылмыскерлерге қарсы тұруды талап етеді. Тек осылай ғана Ақпараттық технологиялар саласындағы қауіпсіздік пен тұрақтылықты қамтамасыз етуге және өзіңізді және деректеріңізді ықтимал қауіптерден қорғауға болады.

Компьютерлік құқық бұзушылық (қылмыс) және АҚ инциденті ұғымдары әр түрлі, алайда оларды тергеу тәсілдері, қолданылатын әдістер және компьютерлік жүйелерді криминалистикалық зерттеудің ілеспе процедуралары мен әдістері көп жағынан ұқсас. Тұрмыстық деңгейде бұл ұғымдар әдетте «компьютерлік қылмыс» (компьютерлік қылмыс) немесе «киберқылмыс» (кибер қылмыс) терминімен біріктіріледі. Бұл термин кеңірек немесе тар мағынада түсіндірілуі мүмкін. Мысалы, бір қабылданған анықтама киберқылмысты компьютерлік жүйелер қылмыстық әрекеттің құралы, мақсаты немесе орны болып табылатын кез келген әрекет ретінде сипаттайды.

Компьютерлік қылмыс термині алғаш рет 60-жылдардың басында американдық, содан кейін басқа шетелдік басылымдарда пайда болды. 1983 жылы Парижде ЭЫДҰ сарапшылар тобы компьютерлік қылмыстың криминологиялық анықтамасын берді, ол деректерді автоматтандырылған өңдеуге және (немесе) деректерді беруге әсер ететін кез келген заңсыз, этикалық емес немесе шешілмеген мінез-құлықты түсінді.

Компьютерлік қылмыс қылмыстық-құқықтық ұғым ретінде-бұл жеке және заңды тұлғалардың, қоғам мен мемлекеттің құқықтық қорғалуға жататын құқықтары мен мүдделеріне зиян келтіру үшін жасалған, деректерді өңдеудің автоматтандырылған жүйелеріне қатысты басқалардың құқықтары мен мүдделерін қылмыстық заңда көзделген кінәлі бұзу.

Ақпарат рұқсатсыз танысудан (мемлекеттік құпияны құрайтын мәліметтер немесе өзге де құпия ақпарат) ғана емес, оның мазмұнын немесе деректемелерін бұрмалаудан немесе өзгертуден де қорғалуы мүмкін. Сонымен қатар, ақпарат айналымы зиянды деп шектелуі мүмкін (мысалы, зорлық-зомбылыққа шақырады, әлеуметтік, нәсілдік немесе діни алауыздықты қоздырады, порнографиялық материалдарды қамтиды және т.б.).

Компьютерлік бағдарламалардың зияндылығы немесе пайдалылығы олардың ақпаратты жою, блоктау, өзгерту немесе көшіру қабілетімен емес (бұл компьютерлік бағдарламалардың типтік функциялары), бірақ келесі белгілердің болуымен анықталады:

– бағдарламаның рұқсат етілмеген жұмысы, бұл келесі екі шарттың кем дегенде біреуін орындауды білдіреді: компьютерлік ақпараттың меншік иесіне (адал иесіне, пайдаланушыға) бағдарлама әрекеттерінің сипаты туралы алдын-ала ескертудің болмауы;

– мұндай әрекеттерді орындауға компьютерлік ақпарат иесінің (адал иесінің, пайдаланушының) келісімін (санкциясын) алмау;

– компьютерлік бағдарламаның нәтижесі ақпаратты жою, бұғаттау, өзгерту немесе көшіру немесе компьютерлік ақпаратты қорғау құралдарын бейтараптандыру болып табылады. Егер бағдарлама жоғарыда аталған әрекеттердің ешқайсысын жасамаса, онда оны зиянды деп санауға болмайды.

Есептеу машинасы (компьютер) – адамның қатысуынсыз кейбір функцияларды орындайтын және берілген бағдарлама бойынша жұмыс істейтін СВТ.

Электрондық есептеу машинасы-негізгі функционалдық құрылғылары электрондық компоненттерде орындалған есептеу машинасы.

Компьютерлік ақпарат-оны сақтау, өңдеу және беру құралдарына қарамастан есептеу машинасында өңдеуге жарамды нысанда ұсынылған ақпарат.

Мұнда негізгі жіктеу белгісі-бұл ақпарат компьютерлік жүйелермен өңдеуге арналған ба, жоқ па.

Қазіргі уақытта компьютерлік ақпарат тек компьютерлерде ғана емес, сонымен қатар ұялы телефондарда, банкоматтарда, төлем терминалдарында және т.б. болуы мүмкін, сондықтан көбінесе компьютерлік және телекоммуникациялық технологияларды қолдана отырып жасалған қылмыстардың кең тобы қарастырылады, олар көбінесе жоғары технологиялық қылмыстар деп аталады (компьютерлік қылмыстар, киберқылмыстар).

Өзін-өзі бақылау мәселелері:

1. Компьютерлік қылмыс дегеніміз не?
2. Компьютерлік қылмыстың қандай түрлері бар?
3. Компьютерлік қылмыстың ұйымға немесе адамға қандай салдары болуы мүмкін?
4. Ақпараттық қауіпсіз оқиғалардың қандай түрлері бар?
5. Компьютерлік қылмыстар мен ақпараттық қауіпсіздік оқиғаларының алдын алу үшін қандай қауіпсіздік шараларын қолдануға болады?
6. Компьютерлік қылмыстармен күресу үшін қандай заңнамалық шаралар қолданылды?
7. Компьютерлік қылмыстың мақсаты қандай маңызды деректер болуы мүмкін?
8. Компьютерлік қылмыстарды тергеу қалай жүзеге асырылады?
9. Зиянды бағдарламалық жасақтама дегеніміз не және оны компьютерлік қылмыстарды жүзеге асыру үшін қалай пайдалануға болады?
10. Қазіргі әлемдегі ақпараттық қауіпсіздіктің маңызы қандай және оған қандай қауіп төнуі мүмкін?

Өзін-өзі бақылауға арналған тест тапсырмалары:

1. Компьютерлік қылмыс дегеніміз не?

a) компьютерлердің өнімділігінің айтарлықтай өсуі;

b) компьютерлік ақпаратты заңсыз пайдалану;

c) операциялық жүйені жаңарту;

d) желілік жабдықтың сапасын жақсарту;

e) жаңа бағдарламалық жасақтаманы әзірлеу.

2. Компьютерлік қылмыстың қандай түрлері бар?

a) физикалық қылмыстар;

b) экономикалық қылмыстар;

c) діни қылмыстар;

d) жыныстық қылмыстар;

e) киберқылмыстар.

3. Ақпараттық оқиға дегеніміз не?

a) АТ саласындағы заңнаманы бұзу;

b) пайдаланушылар туралы ақпаратты заңсыз пайдалану;

c) зиянды бағдарламалық жасақтаманы жүктеу;

d) компьютерлердің өнімділігін төмендету;

e) көпіршікті Ромашка сорты.

4. Компьютерлік қылмыстарды жүргізу кезінде қандай негізгі мақсаттар көзделеді?

a) ақпараттық қауіпсіздік жағдайын жақсарту;

b) ақпаратқа рұқсатсыз қол жеткізу;

c) компьютерлік жүйелердің өнімділігін арттыру;

d) пайдалы бағдарламаларды тарату;

e) жаңа технологияларды әзірлеу.

5. Компьютерлік қылмыстардан қорғау үшін қандай қауіпсіздік шараларын қолдануға болады?

a) антивирустық бағдарламалық жасақтаманы орнату;

b) пайдаланушылардың барлық әрекеттерін Логиялау;

c) барлық деректерді ашық қол жетімділікке жариялау;

d) әлсіз парольдерді қолдану;

e) барлық брандмауэрлерді өшіру.

6. Компьютерлік қылмыстың салдары қандай болуы мүмкін?

a) Ақпараттық жүйелердің сапасын жақсарту;

b) құпия деректердің жоғалуы;

c) киберқауіпсіздік деңгейін арттыру;

d) компьютерлердің өнімділігін арттыру;

e) желілік жабдықтың сапасын жақсарту.

7. Ақпараттық оқиғалардан қорғау үшін қандай қауіпсіздік шараларын қолдану керек?

a) екі факторлы аутентификацияны қосу;

b) барлық есептік жазбалар үшін бір әмбебап құпия сөзді пайдалану;

c) барлық құрылғыларға желіге кіруді ашу;

d) бағдарламалық жасақтаманы тұрақты емес жаңарту;

e) әдепкі Бағдарламалық құралды өшіру.

8. Ақпараттық оқиғаларды анықтау үшін қандай әдістерді қолдануға болады?

a) желілік белсенділікті бақылау;

b) күдікті оқиғаларды елемеу;

c) есептік жазбаларды әкімшілік және пайдаланушы болып бөлу;

d) барлық деректерді жария ресурстарда жариялау;

e) барлық жүйелік журналдарды өшіру.

9. Компьютерлік қылмыс қандай әрекеттер болуы мүмкін?

a) бұзу, деректерді ұрлау, зиянды бағдарламаларды тарату;

b) иесінің рұқсатынсыз компьютерді кез келген пайдалану;

c) интернеттегі файлдарды заңсыз көшіру;

d) вирустарды электрондық пошта арқылы беру;

e) әлеуметтік желілерде жалған аккаунттар құру.

10. Ақпараттық қауіпсіздік оқиғасы дегеніміз не?

a) ақпараттың құпиялылығын, тұтастығын немесе қолжетімділігін бұзу;

b) ақпарат өзекті болмайтын жағдай;

c) бағдарламалық жасақтамада осалдықтардың болуы;

d) компьютерлік жүйелердің жұмысындағы техникалық ақау;

e) бағдарламалық қамтамасыз ету үшін төлем жасамау.

§2. Компьютерлік саладағы құқық бұзушылықтардың жіктелуі

Қазіргі ақпараттық қоғамда компьютерлер мен интернет біздің күнделікті өмірімізде маңызды рөл атқарады. Алайда, компьютерлер мен интернетті пайдалану кезінде компьютерлік саладағы қылмыстар немесе киберқылмыстар деп аталатын қылмыстардың жаңа түрлері де пайда болады. Бұл мәтінде біз компьютерлік саладағы құқық бұзушылықтардың жіктелуін қарастырамыз.

Бірінші санат-ақпаратты ұрлауға байланысты киберқылмыстар. Бұл санатқа хакерлік шабуылдар, фишинг, жеке басын ұрлау, шоттарды бұзу және басқа да осындай қылмыстар кіреді. Қаскүнемдердің мақсаты жеке басының пайдасы немесе басқа адамдарға зиян келтіру үшін басқа біреудің ақпаратын алу.

Екінші санат-зиянды бағдарламалық жасақтаманы таратумен байланысты киберқылмыстар. Бұл құқық бұзушылықтарға вирустардың, құрттардың, трояндардың және басқа да зиянды бағдарламалардың жасалуы мен таралуы жатады. Зиянкестер мұндай бағдарламалық жасақтаманы басқа адамдардың компьютерлері мен желілеріне кіру, ақпаратты ұрлау немесе жүйелерге зиян келтіру үшін қолдана алады.

Үшінші санат – авторлық құқықты бұзу және қарақшылықпен байланысты киберқылмыстар. Бұл санатқа авторлық туындыларды заңсыз жүктеу және тарату, бағдарламалық жасақтаманы, фильмдер мен музыканы қарақшылық сияқты құқық бұзушылықтар жатады. Зиянкестер қорғалған ақпаратқа қол жеткізуге және басқа адамдардың белгілерін заңсыз пайдалануға тырысады, бұл заңды иелеріне қауіп төндіреді.

Төртінші санат – желілік қауіпсіздікті бұзумен байланысты киберқылмыстар. Бұған DDoS шабуылдары, веб-сайттардың осалдығы, желілік инфрақұрылымды манипуляциялау және басқа да осындай қылмыстар сияқты құқық бұзушылықтар кіреді. Зиянкестердің мақсаты-желінің жұмысын бұзу, ақпаратты ұрлау немесе желіні жеке мүддесі үшін пайдалану.

Сонымен, бесінші санат – бұл интернеттегі алаяқтықпен байланысты киберқылмыстар. Бұған жалған интернет-дүкендер, онлайн төлемдер бойынша алаяқтық, қаржы пирамидалары, жалған инвестициялық схемалар және басқа да осындай қылмыстар сияқты құқық бұзушылықтар кіреді. Зиянкестер адамдарды қаржылық ресурстарына немесе жеке деректеріне қол жеткізу үшін алдауға тырысады.

Компьютерлік саладағы құқық бұзушылықтардың жіктелуі қазіргі ақпараттық қоғамда кездесетін қылмыстардың әртүрлі түрлерін түсінуге мүмкіндік береді.

Компьютерлік құқық бұзушылықтарды жіктеу негізіне құқық бұзушылық жасау тетігіндегі компьютерлік ақпарат пен ақпараттық технологиялардың (ат) орнына сәйкес бөлу негізделуі мүмкін:

– компьютерлік ақпарат және АЖ қылмыстық қол сұғудың объектісі (нысанасы) болып табылады, мысалы, ақпаратты ұрлау немесе АЖ зиян келтіру;

– ат құқық бұзушылықтар мен электрондық шабуылдар жасау құралы (құралы) ретінде пайдаланылады;

– It, IP және its-бұл қылмыстық зорлық-зомбылық объектілерін қамтитын орта (мысалы, рұқсатсыз қол жеткізілетін сақтау құрылғылары).

Компьютерлік саладағы құқық бұзушылықтарды тергеудің тиімді әдістерін әзірлеу қажеттілігі сот-медициналық негіздерді және, ең алдымен, құқық бұзушылық жасау тәсілін ескеруді талап етеді. Криминалистикалық классификация тек криминалистикалық сипаттаманың негізі ғана емес, сонымен қатар құқық бұзушылықтарды тергеудің жеке криминалистикалық әдістерінің жүйесін құруға қызмет ете алады. Осы тұрғыдан алғанда, құқық бұзушылық әдісі бойынша жіктеу ең үлкен практикалық қызығушылық тудырады, дегенмен көптеген авторлардың пікірінше, бұл жағдайда қылмыстық-құқықтық ұғымдар мен компьютерлік жүйелерді іске асырудың техникалық ерекшеліктері сөзсіз араласады.

1. Компьютерлік деректер мен жүйелердің құпиялылығына, тұтастығына және қол жетімділігіне қарсы қылмыстар.

– компьютерлік жүйелерге рұқсатсыз қол жеткізу (бұзу, алдау және басқа құралдар арқылы);

– деректерді заңсыз алу (ақпараттық тыңшылық);

– аңсыз ұстау;

– ақпаратты бұрмалау.

– жүйенің бұрмалануы.

Бұл топқа вирустық инфекциялар ,қызмет көрсетуден бас тарту шабуылдары (DoS, DDoS).

2. Мазмұнға байланысты қылмыстар.

Бұл санатқа заңнамаға қайшы келетін мазмұнды (ақпараттық материалдарды) тарату жатады. Интернет арқылы материалдарды тарату құқық бұзушыларға бірқатар артықшылықтар береді, соның ішінде таратудың төмен құны, арнайы жабдықтың болмауы және жаһандық аудитория. Мазмұнды құқықтық бағалау және заңнама негізгі мәдени және құқықтық принциптерді ескеретін және айтарлықтай өзгеруі мүмкін ұлттық ерекшеліктерге қатты тәуелді.

Заңсыз деп саналатын мазмұнды таратуды шектеуді қамтамасыз етудің бір әдісі-сүзгілеу жүйелерін құру және сайттарды бұғаттау. Ресейде домендік атауларды, «Интернет» желісіндегі сайттардың бет көрсеткіштерін және желілік мекен-жайларды бұғаттауды байланыс операторлары мен хостинг провайдерлері тізілім негізінде жүзеге асырады.

Электрондық пошта провайдерлері спамның өсіп келе жатқан деңгейіне кілт сөздерді сүзуді қолдану және спамерлердің IP және пошта мекенжайларының «қара тізімдерін» жүргізу арқылы жауап береді. Спамды анықтау құқық бұзушылардың желілік роботтар мен зомби желілерін пайдалануын қиындатады.

Бопсалау әдеттегі құқық бұзушылық болып саналады, дегенмен жақында компьютерлік жүйеге кіруді бұғаттайтын және төлем төленгеннен кейін оның құлпын ашуды ұсынатын зиянды бағдарлама кеңінен таралды. Бұл ретте құқық бұзушылар анонимді байланыс технологияларын, сондай-ақ

виртуалды әмияндарды немесе криптовалюталарды пайдалана отырып төлеуді пайдалана алады, бұл оларды анықтауды қиындатады.

Интернетті құқық бұзушылар тек тікелей шабуылдар үшін ғана емес, сонымен қатар қылмыстарды қозғау, ұсыну және ынталандыру, тауарларды заңсыз сату және заңсыз әрекеттерді (мысалы, жарылғыш құрылғылар мен басқа да қарулар жасау) орындау туралы ақпарат пен нұсқаулар тарату алаңы ретінде кеңінен қолданады).

3. Меншік құқығымен және сауда белгілерімен байланысты қылмыстар.

Интернет арқылы өнімді тарататын компаниялар авторлық құқықты бұзумен байланысты құқықтық мәселелерге тап болуы мүмкін. Сонымен қатар, қарақшылық мәселелері цифрлық түрде ұсынылуы мүмкін өнімдерге (мысалы, аудиовизуалды өнімдер, кітаптар) және жалған өнімдерді таратуға қатысты, мұнда контрафактілік өндірушілер логотиптерді де, табысты брендтердің өнімдерін де көшіріп, белгілі бір компаниямен байланысты доменді тіркеуге тырысады.

Авторлық және сабақтас құқықтарды бұзумен байланысты қылмыстар.

Қолданыстағы авторлық және сабақтас құқықтарды бұзудың негізі цифрлық туындыны (компьютерлік бағдарламалар, аудио/видео және цифрлық өнімнің басқа да түрлері, сондай-ақ деректер базасы мен кітаптар) жылдам және дәл жаңғырту мүмкіндігі болып табылады. Цифрландыруға дейін аудио және бейне таспаларды көшіру сапаның төмендеуіне әкелді. Қазіргі уақытта сандық өнімдерді сапаны жоғалтпай көшіруге болады, сонымен қатар кез-келген көшірмеден көшірмелер жасауға болады. Файл алмасу желілерінде цифрлық туындылардың заңсыз көшірмелерін орналастырудан, сондай-ақ DRM (digital restrictions management)цифрлық құқықтарды басқару жүйелерін айналып өтуден тұратын құқық бұзушылықтар жиі кездеседі.

Сауда белгілерімен байланысты қылмыстар.

Бұл қылмыс тобы авторлық және сабақтас құқықтарды бұзуға ұқсас, сонымен қатар сауда белгілері пайдаланушыларды адастыру үшін пайдаланылуы мүмкін (мысалы, фишингтік схемаларда). Қылмыстың бұл түріне белгілі өнімнің немесе компанияның сауда белгілеріне ұқсас немесе ұқсас домендік атауларды заңсыз тіркеу жатады (киберквотинг). Тағы бір мысал-доменді «ұрлау» немесе кездейсоқ жоғалған домендік атауларды тіркеу. Мұндай әрекеттердің мақсаты сауда белгісінің иесіне доменді кейіннен жоғары бағамен қайта сату немесе оны тауарлар мен қызметтерді сату үшін пайдалану, пайдаланушыларды осы тауар белгісіне болжамды қатынасы арқылы адастыру болуы мүмкін.

4. Компьютерлік техниканы қолдануға байланысты қылмыстар.

Бұл санатқа компьютерлік жүйе жасалатын қылмыстар кіреді: компьютерлік жүйелерді қолданумен байланысты алаяқтық немесе жалғандық, фишинг және жеке басын ұрлау, сондай-ақ компьютерлік құрылғыларды теріс пайдалану.

Компьютерлік алаяқтық.

Қылмыстық құқық жүйелерінің көпшілігі мұндай құқық бұзушылықтарды компьютерлерді қолданумен байланысты қылмыстар

ретінде емес, қарапайым алаяқтық ретінде қарастырады. Ең көп таралған алаяқтық әрекеттерге мыналар жатады:

– онлайн-аукциондармен алаяқтық: жоқ тауарларды сатуға ұсыну, сондай-ақ оларды төлеу ниетінсіз, оның ішінде үшінші тұлғалардың шоттарын (шоттарды «айдап әкету», шоттарды "тартып алу") пайдалана отырып, тауарларды сатып алу;

– алдын ала төленген алаяқтық: қомақты бонустардың уәдесі (ұтыс, әлеуметтік көмек және т.б.) және ресімдеу үшін немесе басқа сылтаумен шағын ақша сомасын алдын ала аудару туралы өтініш; банктік шоттың деректемелерін жариялау кезінде оларды алаяқтар басқа құқық бұзушылықтар үшін пайдалана алады.

Интернет желісіндегі алаяқтық комбинацияны жүзеге асыру кезектілігін, әдетте, екі кезеңге бөлуге болады:

1. Жәбірленушілерге оларды адастыру мақсатында жалған ақпарат беру немесе таңу;

2. Қол сұғушылық нысанасын тікелей иемдену.

Жалған ақпаратты берудің ең көп тараған тәсілдері-алаяқтық сайттар мен электрондық пошта. Алайда, алаяқтар мессенджерлерді, форумдарды немесе чаттарды қолдана алады. Веб-сайт, әдетте, жасырын болу үшін тегін хостингке тіркеледі. Алайда, алаяқтар сайтты ақылы қызметтерді ұсынатын хостинг компанияларының серверлеріне орналастыра алады.

Қол сұғушылық нысанасын тікелей иемдену несие карталарының тіркеу деректерін енгізу, қаражатты «электрондық әмияндарға», ұялы телефон нөмірлеріне және т.б. аудару арқылы жүзеге асырылуы мүмкін. Электрондық ақша аударымы (WebMoney, Yandex Money) алдын-ала төленген схемаларға (ұялы алаяқтық, жоқ тауарларды ұсыну) тән. Дәстүрлі алаяқтықтан айырмашылығы, интернеттегі алаяқтықтың ерекшелігі-бұл дәстүрлі іздер аз және жәбірленушілер қылмыскерлерді бетпе-бет білмейді.

Компьютерлерді қолдану арқылы жасалған жалғандық.

Электрондық хаттарды немесе цифрлық құжаттарды бұрмалау (ұйымның электрондық бланкісін имитациялай отырып құжат жасау, түпнұсқа құжаттың мәтінін өзгерту, цифрлық қолтаңбаны қолдан жасау немесе «бөтен» заңды цифрлық қолтаңбаны пайдалану, цифрлық кескіндер мен бейнелерді қолдан жасау).

Жеке басын ұрлау.

Жеке басын ұрлау ұғымының нақты анықтамасы мен нақты қолданылуы жоқ, ол «бөтен» тұлғаны (дербес деректерді) алаяқтықпен алу және пайдалану жөніндегі қылмыстық әрекетті білдіреді. Жалпы бұл түрдегі қылмыстар үш түрлі кезеңнен өтеді.

1. Қылмыскер жеке басын куәландыратын ақпаратты зиянды бағдарламалар, фишингтік шабуылдар, компьютерлік ақпарат құралдарын ұрлау немесе басқа тәсілдермен (мысалы, әлеуметтік медиа деректерін іздеу және талдау арқылы) алады. Сонымен қатар, жәбірленушіні жеке ақпаратты ашуға сендіру үшін әлеуметтік инженерия әдістері кеңінен қолданылады.

2. Екінші кезең жеке деректермен тікелей пайдаланылғанға дейін өзара әрекеттесуімен сипатталады, мысалы, сәйкестік туралы ақпаратты Сату.

Бірегейлікке қатысты ақпараттың «қара» нарығының көлемінің өсуін айтуға болады. Ірі ағып кету салдарынан бұзылған дербес деректердің едәуір бөлігі кейіннен сатылымда болады.

3. Жеке басын куәландыратын құжаттарды қолдан жасау немесе несие карталарын алдау сияқты қылмыс жасау кезінде жеке басын куәландыратын ақпаратты пайдалану.

Құрылғыларды теріс пайдалану.

Құқық бұзушылықтардың бұл тобына құқық бұзушылықтарды жүзеге асыру мақсатында құрылғыларды, компьютерлік бағдарламаларды, компьютерлік парольдерді немесе кіру кодтарын жасау, сату, пайдалану, тарату үшін сатып алу немесе басқаша пайдалану үшін беру жатады. Интернет желісінің қылмыстық бөлігінде спам-хабарламаларды, dos шабуылдарын жүргізуге, компьютерлік вирустарды құруға, шифрланған хабарламаларды дешифрлеуге немесе компьютерлік жүйелерге рұқсатсыз қол жеткізуге арналған автоматтандырылған құралдар кеңінен ұсынылған. Сонымен қатар, көптеген осындай бағдарламалардың интерфейстері кеңсе қосымшаларынан әрең ерекшеленеді және игеруге интуитивті, ал зиянды бағдарламаны енгізу қылмыскерге бағдарламаны іске қосу және нәтижелерді күту жеткілікті болған кезде автоматты режимде жүзеге асырылады.

Қазіргі уақытта зиянды бағдарламаны жалға беру нарығы дамып келеді. Тапсырыс беруші белгілеген арнайы тапсырмалар үшін осындай бағдарламаларды құру немесе өзгерту «қызмет ретінде қылмыс» сияқты кең таралған құбылыстың бір түрі болып табылады. Ақылы түрде көрсетілген серверлерге DDoS шабуылына тапсырыс беруге немесе сол мақсаттарды жүзеге асыру үшін ботнет алуға болады. Сондықтан әр түрлі ұлттық заңдарда қудалау сондай ақ осындай құралдарға ие болу қарастырылған.

5. Аралас қылмыстар.

Бұл топқа бірқатар түрлі құқық бұзушылықтарды біріктіретін күрделі қылмыстық әрекеттер жатады. Мысалы, Интернет желісін террористік мақсатта пайдалану (кибертерроризм), компьютерлік технологияларды қолдана отырып ақшаны жылыстату және фишинг.

Интернет желісі және басқа да желілік ат негізінде құрылған тауарларды жеткізудің, қызметтер көрсетудің, жеке және заңды тұлғалар арасында қаражат аударудың, ақпаратты сақтаудың және оған әрбір компьютерді қосудың трансшекаралық инфрақұрылымы компьютерлік қылмыстарды жетілдіру үшін де, алынған ақшаны компьютерлік технологиялардың көмегімен жылыстату үшін де кең мүмкіндіктер береді. Бұл ретте құқық бұзушылардың мүмкіндіктері Интернет желісінің қылмыстық әрекеттер жасау ортасы ретіндегі мынадай қасиеттерімен сипатталады:

– қылмыстың жылдамдығы және төмен құны;
– жоғары технологиялық;
– күрделі сипат;
– анонимділік;
– трансұлттық сипат;
– адамдардың кең ауқымына қол жетімділік (танымалдылық);
– қатысушылардың ұйымдастырылған сипаты мен аралас құрамы.

Ең күрделі қылмыстық істер, әдетте, мақсатты шабуылдармен (APT), интернет-банк немесе қаржы ұйымдарының мобильді қосымшалары арқылы ақша ұрлаумен айналысатын ірі қылмыстық топтармен байланысты. Бұл жағдайларда шабуылдаушылар өздерінің жеке басының құпиялылығына көп көңіл бөледі-ресурстарға қол жеткізу үшін бірнеше сервер тізбегін пайдаланады, шифрлауды қолданады, шабуылдар үшін қолданылатын бағдарламалық жасақтаманы үнемі өзгертеді. Өкінішке орай, көбінесе бір оқиғаға байланысты зиянкестерді анықтау мүмкін емес. Тек бірнеше эпизодта жұмыс істеуге болатын материал теріледі, бірақ сол кезде де іздеу процесі ұзаққа созылуы мүмкін.

Тағы бір қиындық - мұндай қылмыстық топтарда, әдетте, рөлдер нақты бөлінеді және бөлшектеледі, сондықтан құқық бұзушылықты басынан аяғына дейін әртүрлі адамдар жасайды. Топ жетекшісі белгілі бір тапсырмаларды орындау үшін орындаушыларды жалдайды, олардың кейбіреулері қылмыстық әрекетке қатысып жатқанын білмеуі де мүмкін.

Интернет желісін террористік мақсатта пайдалану.

Террористік топтар компьютерлік технологияны, атап айтқанда Интернет желісін қолдана алады:

– насихаттау;

– ақпарат жинау;

– нақты әлемдегі шабуылдарды дайындау;

– оқу материалдарын жариялау;

– үйлестіру және байланыс;

– террористік операциялар мен топтарды қаржыландыру;

– КИИ нысандарына шабуылдар.

Кибер соғыс.

«Кибер соғыс» термині көбінесе елдің компьютерлік жүйелеріне жаппай шабуыл жасау үшін қолданылады. Алайда, қазіргі уақытта бірыңғай терминология жоқ, сонымен қатар бұл ұғымның жалпы қабылданған анықтамасы да жоқ. Тар мағынада кибер соғыс дегеніміз-бұл барлық түрдегі және барлық деңгейдегі ақпаратты басқару және пайдалану, әсіресе біріккен және бірлескен әскери іс-қимылдар кезінде айқын әскери артықшылыққа қол жеткізу. Бұл тұрғыда кибер соғыс бейбіт уақытта жүргізілмейді, сондықтан тек кибер операциялар туралы айтуға болады. Терминнің кеңірек түсіндірмелері ақпарат басып алынатын немесе жойылатын стратегиялық құрал ретінде әрекет ететін кез келген электрондық қақтығысты білдіреді.

Сонымен бірге, киберқылмыс пен кибер соғыс ұғымдарын нақты төгу керек, өйткені егер компьютерлік қылмыстар ұлттық заңнамамен реттелсе, онда соғыс қимылдарына қатысты ережелер мен ережелер негізінен халықаралық құқық нормаларымен, атап айтқанда Біріккен Ұлттар Ұйымының Жарғысымен реттеледі.

Компьютерлік технологияларды қолдана отырып ақшаны жылыстату.

Тарату онлайн қаржылық қызметтер және электрондық ақша (виртуалды валюталар, криптовалюталар) бүкіл әлем бойынша көптеген қаржылық операцияларды жылдам орындауға мүмкіндік береді және банктік қолма-қол ақшасыз есеп айырысуларға тән қатаң шектеулер мен тексерулерді айналып

өтуге мүмкіндік береді. Бұл ретте ақшаны жылыстатуға қарсы күрес саласындағы күдікті мәмілелерді анықтау мәмілеге қатысатын қаржы мекемелерінің міндеттемелеріне негізделген.

Ақшаны жылыстату жалпы үш кезеңге бөлінеді:

1. Қолма-қол ақшаны орналастыру,

2. Стратификация (үлкен ақшаны кішірек ақшаға бөлу);

3. Қорытындылау.

Интернет қызметтерін әсіресе қылмыскерлер стратификация немесе маскировка сатысында іздейді. Онлайн-казинолар мен виртуалды валюталар ақша сомасын стратификациялау үшін пайдаланылған кезде қылмыстарды тергеу ерекше қиындық тудырады.

Фишинг.

Фишингтің мақсаттары тек онлайн-банктік операцияларды жүргізу үшін парольдерді алумен ғана шектелмейді, шабуылдаушылар компьютерлерге, аукцион алаңдарына және жеке деректерге қол жеткізу кодтарына қызығушылық танытуы мүмкін, бұл «жеке басын ұрлау» сияқты қылмыстарға әкелуі мүмкін. Дәстүрлі фишингтік шабуыл схемасы келесі кезеңдерді қамтиды.

1. Бірінші кезеңде онлайн қызметтерді ұсынатын және клиенттермен электронды түрде өзара әрекеттесетін компаниялар анықталады, мысалы, қаржы институттары.

2. Әрі қарай, құқық бұзушылар жәбірленушіден әдеттегі кіру процедураларын орындау талап етілетін заңды сайттарға ұқсайтын жалған веб-сайттар (фишингтік сайттар) жасайды, бұл құқық бұзушыларға шот нөмірлері мен онлайн банктік парольдер сияқты жеке ақпаратты алуға мүмкіндік береді.

3. Пайдаланушыларды жалған сайттарға бағыттау үшін, әдетте, электрондық пошта хабарламалары қолданылады, ал хатта жәбірленуші алданған сайтқа өтуі керек дайын сілтеме бар. Бұл пайдаланушылардың дұрыс мекенжайды қолмен енгізуіне жол бермейді. Фишингтік шабуылдардың басқа схемалары бар.

Жеке ақпарат ашылғаннан кейін, құқық бұзушылар жәбірленушілердің шоттарына кіріп, ақша аудару, төлқұжатқа өтініштер немесе жаңа шоттар және т.б. сияқты қылмыстар жасайды.

Қазіргі ақпараттық қоғамда компьютерлік жүйелерге рұқсатсыз қол жеткізу, жеке басын ұрлау, вирустық шабуылдар және компьютерлік қылмыстың басқа аспектілері жеке адамдарға, компаниялар мен мемлекеттерге үлкен қауіп төндіреді. Компьютерлік саладағы құқық бұзушылықтардың жіктелуі мұндай қылмыстарды түсіну мен онымен күресудің маңызды құралы болып табылады.

Мұндай құқық бұзушылықтарды талдау барысында кибербандализм, кибер алаяқтық, кибер тыңшылық, кибертерроризм және басқаларын қоса алғанда, әртүрлі санаттар анықталды. Алайда, технологияның дамуы мен компьютерлік қылмыстың жаңа түрлерінің пайда болуын ескере отырып, осы классификацияны үнемі жаңартып отыру қажет.

Компьютерлік құқық бұзушылықтарды жіктеу туралы хабардар болу ақпараттық қауіпсіздікті қорғаудың белсенді шараларын дамытудың маңызды сәті болып табылады. Қылмыс түрлерінің арасындағы айырмашылықты түсіну тиісті стратегияларды әзірлеуге, жаңа қауіптердің алдын алуға және қорғаныс шараларын күшейтуге мүмкіндік береді.

Қорытындылай келе, компьютерлік қылмыстармен тиімді күрес актілерді түсінуді және жіктеуді ғана емес, сонымен қатар халықаралық ынтымақтастықты дамытуды, тиісті заңнаманы қабылдауды және халықты киберқауіпсіздік негіздеріне оқытуды қамтамасыз етуді талап ететінін атап өткен жөн. Тек осылайша, бірлескен күш-жігермен виртуалды кеңістікте қауіпсіздікті қамтамасыз етуге болады.

Бірінші кезекте ақпараттық қауіпсіздікті бұзумен байланысты құқық бұзушылықтар санаттары зерделенді. Бұған компьютерлік жүйелерге рұқсатсыз қол жеткізу, бұзу, желідегі алаяқтық, зиянды бағдарламаларды тарату және киберқылмыстың басқа түрлері кіреді.

Авторлық құқық пен зияткерлік меншікті бұзуға байланысты құқық бұзушылықтар да қарастырылды. Бұған бағдарламалық жасақтаманы қарақшылық, мазмұнды заңсыз тарату, патенттік құқықты бұзу және басқа да осындай әрекеттер кіреді.

Компьютерлік саладағы құқық бұзушылықтарды жіктеудің маңызды аспектісі оларды белсенді және пассивті деп бөлу болып табылады. Белсенді құқық бұзушылықтарға хакерлік шабуылдар немесе зиянды бағдарламаларды тарату сияқты заңнаманы бұзуға бағытталған тікелей әрекеттер жатады. Пассивті құқық бұзушылықтар жүйеге тікелей енбестен ақпаратты немесе бағдарламалық жасақтаманы заңсыз пайдаланумен байланысты.

Қорытындылай келе, компьютерлік саладағы құқық бұзушылықтардың жіктелуі киберқылмысты түсіну мен онымен күресудің маңызды құралы болып табылады. Құқық бұзушылықтардың әртүрлі түрлерін ажырату оларға тиімді жауап беруге және құқық бұзушылардың алдын алу және жазалау бойынша тиісті шараларды қабылдауға мүмкіндік береді. Технологияның қарқынды дамуына және компьютерлік саланың кеңеюіне байланысты ақпараттық қауіпсіздік саласындағы өзгеріп отыратын шындықтар мен сын-қатерлерге сәйкес келетін классификацияны үнемі жаңартып, толықтырып отыру қажет.

Өзін-өзі бақылауға арналған сұрақтар:

1. Компьютерлік саладағы құқық бұзушылықтардың қандай түрлерін ажыратуға болады?
2. Ақпараттық қауіпсіздікті бұзуға байланысты құқық бұзушылықтар санаты нені қамтиды?
3. Компьютерлік жүйелерге рұқсатсыз кіруге қандай киберқылмыс түрлері жатады?
4. Желідегі алаяқтық ретінде қандай әрекеттерді жіктеуге болады?
5. Зиянды бағдарламалардың қандай түрлері бар және олар қандай қылмыстар жасай алады?
6. Қандай құқық бұзушылықтар авторлық құқық пен зияткерлік меншікті бұзумен байланысты?
7. Бағдарламалық жасақтама қарақшылығына киберқылмыстың қандай түрлері жатады?
8. Мазмұнды заңсыз таратумен қандай құқық бұзушылықтар байланысты?
9. Компьютерлік салада патенттік құқықты бұзу нені қамтиды?
10. Компьютерлік саладағы құқық бұзушылықтарды белсенді және пассивті деп қалай бөлуге болады?

Өзін-өзі бақылауға арналған тест тапсырмалары:

1. Аталған құқық бұзушылықтардың қайсысы "хакерлік" шабуылдарға жатады?

a) вирустар;
b) фишинг;
c) кибер тыңшылық;
d) жоғарыда айтылғандардың барлығы;
e) тек a) және b).

2. Төмендегілердің қайсысы кибербуллингтің түрлері?

a) хакерлік шабуылдар;
b) онлайн қорлау;
c) интернетте адам туралы жалған ақпаратты тарату;
d) тек b) және c);
e) жоғарыда айтылғандардың барлығы.

3. Компьютерлік қауіпсіздік саласындағы қандай әрекет құпия ақпаратты жария етуге жатады?

a) кибер тыңшылық;
b) DDoS-шабуыл;
c) кибервандализм;
d) фишинг;
e) кейлоггинг.

4. Киберқылмыстың аталған түрлерінің қайсысы қаржылық алаяқтықпен байланысты?

a) вирустар;
b) кардинг;
c) фарминг;
d) жоғарыда айтылғандардың барлығы;
e) тек б) және в).

5. Ақпарат алу немесе зиян келтіру үшін қорғалған компьютерлік жүйелерге ену қалай аталады?

a) вирус;
b) бұзу;
c) қорқыту;
d) DDoS-шабуыл;
e) фишинг.

6. Жоғарыда айтылғандардың қайсысы интернетте балалар порнографиясын таратуға байланысты қылмыстарға жатады?

a) sell spam;
b) киберпорнография;
c) кибертерроризм;
d) кибервандализм;
e) кибер тыңшылық.

7. Төмендегілердің қайсысы кибертерроризмнің бір түрі?

a) интернетте жалған ақпарат тарату;
b) маңызды инфрақұрылымға кибершабуылдар;

c) киберпорнография;
d) тек a);
e) тек b).

8. Киберқылмыстың қандай түрі бопсалау мақсатында пайдаланушылардың жеке деректерін бақылаумен байланысты?

a) тыңшылық;
b) фишинг;
c) DDoS-шабуыл;
d) кейлоггинг;
e) кардинг.

9. Төмендегілердің қайсысы кибервандализмге қатысты?

a) мемлекеттік сайттарға кибершабуылдар;
b) компьютерлік вирустардың таралуы;
c) компьютерлік деректерді өзгерту немесе жою;
d) тек a) және c);
e) тек b) және c).

10. Компьютерлік қауіпсіздік саласында қылмыс жасағаны үшін жаза қандай атаумен белгіленеді?

a) кибершраф;
b) сандық жауапкершілік;
c) кибер кек алу;
d) кибернаказания;
e) кибершабуылдар.

3. Компьютерлік саладағы құқық бұзушылықтардың криминалистикалық сипаттамасы

Сот-медициналық сипаттама-бұл белгілі бір түрдегі қылмыстың типтік белгілерінің жүйесі. Криминалистикалық сипаттама тәжірибені ресімдейді және типтік құқық бұзушылық туралы білім жүйесін қалыптастырады, сондықтан бір құрамдағы ұқсас қылмыстық әрекеттерді немесе тіпті бір құрамдағы құқық бұзушылықтардың әрқайсысын қарастырған кезде пайдалы.

Ең маңызды сот-медициналық ақпарат:

– қылмыстық қол сұғушылықтың мәні;

– құқық бұзушының жеке басы;

– қылмыстық мінез-құлықтың себептері мен мақсаттары;

– қылмысты дайындаудың, жасаудың және жасырудың типтік тәсілдері;

– қылмыстық қол сұғушылықтардың уақыты, орны және жағдайы;

– із түзу механизмі.

Компьютерлік саладағы құқық бұзушылықтардың криминалистикалық сипаттамасы белгілі бір ерекшелікке ие, атап айтқанда: құқық бұзушылықтың осы түрінің техникалық компоненті-ең маңыздыларының бірі. Компьютерлік қылмыстар жоғары кідіріспен сипатталады, демек, мұндай қылмыстардың аз ғана бөлігі ресми түрде тіркеледі және ашылады, яғни сотқа жеткізіледі – одан да аз. Мамандардың пікірінше, компьютерлік қылмыстардың 70-90 пайызы қылмыстық есептен тыс қалады. Сонымен қатар, сот-медициналық сипаттамаларға арналған статистикалық үлестірулер (мысалы, қылмыскердің жеке басының сипаттамалары) тек ашылған қылмыстардың мәліметтері бойынша есептеледі. Сондықтан әдебиетте келтірілген криминалистикалық статистика өте шартты. Статистика жоғары технологиялар саласында тіркелген қылмыстар санының тұрақты өскенін көрсетеді.

Қылмыстық қол сұғушылықтың мәні. Ақпараттық ресурстар (компьютерлік ақпараттың өзі және АЖ), сондай-ақ ақша немесе өзге де материалдық құндылықтар және олармен байланысты құқықтар компьютерлік құқық бұзушылықтардың нысанасы болуы мүмкін. Ақпараттық ресурстардың түрі қылмыскердің себептері мен мақсатына байланысты. Бұл заңмен қорғалатын ақпарат (құпиялардың әртүрлі түрлері, Дербес деректер), материалдық құндылығы жоғары мәліметтер (өндіріс құпиялары, «ноу-хау», инсайдерлік ақпарат, кредиттік және төлем карталарының деректемелері, авторлық құқық объектілері), мемлекеттік билік органдарының, саяси және қоғамдық ұйымдардың, жекелеген компаниялардың сайттары, КИИ объектілері болуы мүмкін. Қылмыстық зорлық-зомбылық тақырыбы көбінесе қылмыскерлердің белгілі бір санатын көрсетеді. Мысалы, өндірістік құпиялар бәсекелестер үшін қызықты, ал саяси қайраткер туралы жала жабу туралы ақпарат оның қарсыластарының мүддесі үшін таратылады және т.б.

Құқық бұзушының жеке басының сипаттамасы. Компьютерлік саладағы қылмыскерлердің басым көпшілігі (80% – дан астамы) ер адамдар. Алайда,

ат-мен байланысты «әйелдер» кәсіптерінің таралуымен (бухгалтерлер, кассирлер, операторлар) әйелдердің үлесі артады.

Компьютерлік құқық бұзушылықтардың едәуір бөлігін қызметі компьютерлік немесе телекоммуникациялық технологиялармен байланысты адамдар жасайды. Бұл ретте қылмыскерлердің 50%-дан астамы ақпаратты автоматтандырылған өңдеу саласында арнайы даярлықтан өтті, ал 30%-ы компьютерлерді пайдалануға және оған бағдарламалық қамтамасыз етуді әзірлеуге тікелей байланысты болды. Алайда, бұқаралық ақпарат құралдары салған "хакердің" бейнесіне қарамастан, құқық бұзушылар әрқашан АТ саласындағы жоғары білікті мамандар бола бермейді. Шынында да, киберқылмыс жасау (мысалы, фишингтік поштаны ұйымдастыру) әрқашан маңызды арнайы білімді қажет етпейді. Сонымен қатар, зиянды бағдарламалардың "қара нарығын" дамыту, шабуыл құралдары мен әдістерінің жалпыға қол жетімділігі шабуылдаушылардың арнайы білім деңгейіне деген сұраныстың төмендеуіне әкеледі. Екінші жағынан, күрделі шабуылдарды жалғыз жасау мүмкін емес. Зерттеушілер компьютерлік қылмысты ұйымдастырудың жоғары дәрежесін атап өтті - кейбір мәліметтер бойынша, компьютерлік құқық бұзушылықтардың 60% - ы ұйымдасқан топтар мен қауымдастықтардың құрамында жасалады. Әдетте, олардың қылмыстық мамандану негізінде оқшауланған жеке құрылымдық бөлімшелері бар: зиянды бағдарламаларды жасаушылар; желілік инфрақұрылымға шабуыл жасау үшін пайдаланылатын әкімшілер; жұқтырған компьютерлердің ботсет операторлары; ұрланған ақшаны алу мен қолма-қол ақшаны қамтамасыз ететін топтар.

Осылайша, қаржылық мәселелерден басқа, компьютерлік салада әрекет ететін құқық бұзушылар келесі себептерді басшылыққа ала алады:

– саяси мақсаттар: терроризм, тыңшылық, мемлекеттің қаржылық-экономикалық және саяси тұрақтылығына нұқсан келтіру, нәсілдік, ұлтаралық және діни алауыздықты қоздыру және т.б.);

– зерттеу қызығушылығы мен қызығушылығы;

– бұзақылық шақырулар;

– кек алу (белгілі бір адамдарға немесе ұйымдарға);

– өзін-өзі растауға және өз ортасында тануға ұмтылу, атақ алуға, интеллектуалды артықшылықты көрсетуге деген ұмтылыс;

– басқа қылмысты жасыруға немесе оны жасауды жеңілдетуге ұмтылу.

Құқық бұзушылықты жасау тәсілі мен құралдары. Криминалистикалық мағынада қылмыс жасау тәсілі ең маңызды болып табылады, өйткені ол біріншіден, криминалистикалық маңызды ақпараттың ең үлкен көлемімен сипатталады, екіншіден, криминалистикалық сипаттаманың барлық басқа элементтері онымен байланысты. Криминалистикалық мағынада қылмыс жасау тәсілі құқық бұзушылықты дайындау, жасау және жасыру бойынша іс-қимыл жүйесі ретінде сипатталады, сонымен қатар іздер мен әртүрлі материалдық объектілер түрінде сыртқы көрініске ие.

Компьютерлік ақпарат саласындағы құқық бұзушылықтарды жасау тәсілдері әр түрлі, белгілі бір дәрежеде олар бұрын келтірілген классификациямен көрсетіледі.

Шабуылдарды дамытудың келесі кезеңдерін ажыратуға болады:

1. Ішкі корпоративтік желіге ену. Ол әдетте фишингтік хаттарды мақсатты немесе жаппай спам-жіберу арқылы жүзеге асырылады, онда қосымша ретінде арнайы жасалған құжат немесе үшінші тарап ресурсына зиянды сілтеме бар. Бұл құжаттың ашылуы немесе сілтеме бойынша өту зиянды бағдарламамен жүйенің инфекциясына әкеледі.

2. Барлау және сату. Бұзылған компьютерлерге қашықтан басқару және басқару бағдарламалары орнатылады, олардың көмегімен қылмыскерлер жүйе әкімшілерінің тіркелгі деректерін иемденуге тырысады. Заңды қашықтан басқару және басқару бағдарламалары, сондай-ақ көптеген пайдаланушыларға белгілі функционалдығы бар операциялық жүйелердің штаттық құралдары (мысалы, Power Shell және WMI) кеңінен қолданылады.

3. Соңғы кезеңде желілік компьютерлер мен қызметтерге рұқсатсыз қол жеткізу мүмкіндіктері жүзеге асырылады, оның мақсаты болуы мүмкін:

– заңсыз қаржылық операцияларды орындау және ақша ұрлау;

– пайдаланушылардың жеке деректерін иемдену;

– ботнетті қалыптастыру;

– ТП АБЖ-ны бақылауды тоқтату;

– компанияның клиенттеріне немесе серіктестеріне мақсатты шабуылдар жасау үшін ішкі корпоративтік ресурстардан көшірілген ақпаратты пайдалану және т.б.

Құқық бұзушылықты жасау уақыты, орны және жағдайы. Компьютерлік құқық бұзушылықты жасау уақыты әрдайым күнге дейін, тіпті одан да көп сағат пен минутқа дейін белгіленбеуі мүмкін. Қосылу/ажырату сәті жүйелік журналдарда, байланыс журналдарында, тарифтеу серверіндегі журналдарда және т.б. тіркелген кезде нақты уақытты белгілеуге болады. Бұл ретте іс-әрекеттің өзі, туындаған салдарлар және олардың анықталуы уақыт бойынша бөлінуі мүмкін.

Желілік технологиялар мен қашықтан қол жеткізу мүмкіндіктерін пайдалану әлеуметтік қауіпті әрекеттерді (мысалы, зиянды бағдарламаны құру) бір жерде жасауға және оның салдарын (мысалы, зиянды бағдарламаны жұқтырудың салдары) басқа жерде, көбінесе айтарлықтай қашықтықта жасауға әкеледі. Бұл ретте құқық бұзушы жәбірленуші тараппен тікелей байланысқа түспейді және жәбірленуші тараптың ЖТҚ-на физикалық қол жеткізе алмауы мүмкін. Осыған байланысты, компьютерлік құқық бұзушылық орын деп әлеуметтік қауіпті іс-әрекет жасалған жер, яғни бұзушы пайдаланған компьютерді басқару құрылғылары (пернетақта, тінтуір және т.б.) орналасқан жер түсініледі.

Қылмыс жасалған жерден айырмашылығы, оқиға орны құқық бұзушылықты жүзеге асыру нәтижесінде қалған іздің болуымен сипатталады. Сондықтан компьютерлік құқық бұзушылық болған жағдайда оқиға орны болуы мүмкін:

– қылмыстық әрекеттер жасалды (компьютерлік желіге кіру, командалар мен ақпарат енгізілді, зиянды бағдарламалар жасалды және т. б.);

– заңсыз әсер ету нәтижесінде зиян келтірілген ақпараттық ресурстар орналасқан;

– зиянды салдарлар болған жерде немесе басқа жерлерде, мысалы, транзиттік ақпарат тасығыштардың орналасқан жері және т. б.

Компьютерлік құқық бұзушылықтар үшін бірнеше орын болуы мүмкін, соның ішінде әр түрлі юрисдикцияларда (мысалы, шетелде)бір-бірінен едәуір алыс.

Компьютерлік құқық бұзушылықты жасау жағдайына қылмыстық әрекет орын алатын ортаның материалдық және әлеуметтік-психологиялық факторлары (мысалы, ақпаратты қорғаудың белгіленген құралдары, шабуылға ұшыраған ұйымның қызметкерлеріне әлеуметтік инженерия әдістерін қолдану мүмкіндігі және т.б.) жатады. Жағдайдың маңызды ерекшелігі оның динамикалық екендігінде көрінеді.

Жағдайдың жай-күйі компьютерлік саладағы құқық бұзушылықтарға қатысушылардың мінез-құлқына айтарлықтай әсер етеді. Әдетте, құқық бұзушылықтың алдында мұқият дайындық бар, ол зерттеуге және анықталған жағдайға бейімделуге байланысты. Осы мақсатта жағдайға өзгерістер енгізілуі мүмкін, мысалы, шабуылдаушы компьютерлік жүйеге зиянды бағдарламаны енгізу арқылы. Мұндай әрекеттердің мақсаты қорғаныс жүйесінің функцияларын бейтараптандыру немесе өзгерту және заңсыз қол жеткізу мүмкіндігін алу болып табылады.

Қылмыс жасауға ықпал ететін факторларға компьютерлік жүйелер мен желілердің қауіпсіздігінің төмен деңгейі, қорғалмаған дерекқорлардағы әртүрлі мақсаттағы компьютерлік ақпараттың шоғырлануы, компьютерлік ақпаратқа қол жеткізуді басқарудағы қателіктер, пайдаланушылардың кең ауқымы, бөгде адамдардың SVT-ге физикалық қол жеткізу мүмкіндігі жатады.

Қылмыс жасалғаннан кейін қалыптасқан жағдайға кейіннен орын алатын жағдайлар мен жағдайлар із қалдырады. Сонымен, қылмыс жасау нәтижесінде пайда болған жүйеде болу іздерін құқық бұзушылар мақсатты түрде жоя алады (мысалы, операциялық жүйенің журналдарын, қолданбалы жүйелер журналдарын тазарту және жүйелік файлдарды жою немесе ақпарат тасығышты шифрлау арқылы). Жүйенің жұмыс істеу процесінде кейбір цифрлық іздер табиғи түрде жаңаларымен сүртілуі мүмкін, оларды қалпына келтіру мүмкін болмайтындай дәрежеде. Сонымен, Group-IB мамандарының айтуынша, үш айдан кейін толыққанды тергеу жүргізу және болған оқиғаның суретін қалпына келтіру проблемалы болып көрінеді.

Із түзу механизмі. Оқиға орнында жәбірленушілердің де, құқық бұзушылардың да электронды құрылғыларының жадында қалған "дәстүрлі" іздерді де, виртуалды іздерді де табуға болады.

Компьютерлік құралдарды қолдануға байланысты қылмыс іздерінің келесі топтарын ажыратуға болады:

– құқық бұзушылық жасалған компьютерлік техника құралдарындағы іздер: Бағдарламалық жасақтамаға заңсыз қол жеткізу үшін пайдаланылған, its-ке қосылу журналдары, сақталған кіру кодтары, бағдарламалардың мәтіндері, жәбірленуші тараптан көшірілген Ақпарат және т. б. мұндай іздер операциялық жүйенің жазбаларында, компьютерлік құралдардың

аппараттық-бағдарламалық конфигурациясында, электрондық тасымалдағыштарда және т. б. қалуы мүмкін;

– «транзиттік» (телекоммуникациялық) ақпарат тасығыштардағы іздер, ол арқылы адам қашықтағы АЖ-мен немесе ресурстармен байланысты жүзеге асырды: телематикалық қызметтер операторы арқылы трафик туралы құжатталған ақпарат, желіде орналастырылған ақпарат, электрондық хат алмасу және т. б.;

– әсер еткен компьютерлік жүйедегі, оның ішінде электрондық тасымалдағыштардағы іздер: компьютерлік ақпаратты заңсыз жою, бұғаттау, модификациялау, ақпаратты қорғау құралдарына әсер ету және компьютерлік жүйеге рұқсатсыз қол жеткізу нәтижелері. Бұл іздердің орналасуы бұзушының компьютерлік жүйесіндегі іздерге ұқсас;

– қылмыс жасауға тікелей қатыспаған, бірақ қылмыстық іс үшін маңызы бар мәліметтерді қамтитын өзге де компьютерлік құралдардағы (компьютерлерде, ұйымдастырушыларда, ұялы телефондарда, цифрлық камераларда, бейнекамераларда, диктофондарда, басқа да ақпарат тасығыштарда) іздер;

– компьютерлік техника құралдарын пайдалана отырып жасалған құжаттар;

– материалдық сияқты дәстүрлі іздер;

– қолдар, аяқ киімдер, құралдар, құралдар және т.б., сондай-ақ мінсіз. Идеал іздер дегеніміз-оқиғаның адамның санасында бейнеленуі, бұл жағдайда сот-медициналық маңызды ақпаратты ауызша немесе басқа түрде (мысалы, айғақтар ретінде)шығаруға болады.

Сандық түрде сақталған ақпараттың, оның ішінде виртуалды іздердің айрықша белгілері:

– оны қабылдауды қамтамасыз ету үшін арнайы құралдарды (бағдарламалық, аппараттық) пайдаланудың жасырын түрі мен қажеттілігі;

– қысқа мерзімде және қашықтан жою немесе өзгерту мүмкіндігі;

– осы ақпаратқа қол жеткізуді шектейтін арнайы құралдардың болуы;

– пайдаланушының жұмысы және әртүрлі операцияларды орындау барысында ақпараттың үнемі өзгеруі;

– байланыс арналары арқылы деректерді беру кезінде бір мезгілде әртүрлі құрылғыларда өзара байланысты ақпаратты қалыптастыру.

Сандық деректердің аталған қасиеттері цифрлық дәлелдемелерді тіркеу және алу кезінде, сондай-ақ оларды сот-сараптамалық зерттеу кезінде белгілі бір ережелерді сақтау қажеттілігін анықтайды.

Компьютерлік саладағы құқық бұзушылықтардың криминалистикалық сипаттамасы Қазіргі әлемдегі қылмысқа қарсы күрестің маңызды құрамдас бөлігі болып табылады. Деректерді талдау және ақпараттық қауіпсіздіктің соңғы тенденцияларымен танысу криминалистерге компьютерлік технологияны қолдану арқылы жасалған қылмыстармен тиімді күресуге мүмкіндік береді.

Компьютерлік саладағы криминалистикалық сараптама жұмысының негізгі бағыттары қылмыс жасау кезінде пайдаланылған техникалық құралдарды зерттеуді, Интернет желісіндегі қылмыстық әрекеттің іздерін

зерттеуді, сондай-ақ электрондық деректер мен құжаттарды талдауды қамтиды.

Компьютерлік саладағы құқық бұзушылықтарды криминалистикалық сипаттау процесінде мамандар қылмыс жасау тәсілдерін анықтайды, қылмыскерлердің себептері мен мақсаттарын талдайды, қылмыстардың салдарын анықтайды және олардың алдын алу әдістерін әзірлейді.

Осылайша, компьютерлік саладағы құқық бұзушылықтардың криминалистикалық сипаттамасы ақпараттың қауіпсіздігін қамтамасыз етуде және желідегі қылмыстық әрекеттерден қорғауда маңызды рөл атқарады. Оны өткізу қылмыскерлерді анықтауға және жазалауға, сондай-ақ жаңа қылмыстардың алдын алу және қоғамның ақпараттық қауіпсіздігін нығайту жөніндегі шараларды әзірлеуге ықпал етеді.

Өзін-өзі бақылауға арналған сұрақтар:

1. Компьютерлік қылмыстың қандай түрлері бар?
2. Компьютерлік қылмыстарды анықтаудың және ашудың негізгі әдістері қандай?
3. Киберқылмыс дегеніміз не және киберқылмыстың қандай мысалдарын келтіруге болады?
4. Қылмыстарды дәлелдеу үшін компьютерлік сараптаманың қандай әдістері қолданылады?
5. Киберқылмыскерлер шабуылдар мен бұзушылықтарды жүзеге асыру үшін қандай технологияларды қолданады?
6. Компьютерлік қылмыстарды қандай заңдар мен ережелер реттейді?
7. Компьютерлік қылмыстардан қорғау үшін қандай қауіпсіздік шараларын қолдануға болады?
8. Компьютерлік қылмыстың салдары қандай болуы мүмкін?
9. Компьютерлік қылмыстарды тергеу кезінде криминалист қандай құзыреттерге ие болуы керек?
10. Компьютерлік криминалистикада қандай мамандандырылған аналитикалық құралдар қолданылады?

Өзін-өзі бақылауға арналған тест тапсырмалары:

1. Компьютерлік қылмыстың қандай түрі ақпараттың құпиялылық құқығын бұзу болып табылады?

a) вирустар;

b) фишинг;

c) спам;

d) DDoS шабуылы;

e) серверлерді бұзу.

2. Компьютерлік қылмыстарды анықтау және дәлелдеу процесі қалай аталады?

a) кибер тыңшылық;

b) компьютерлік бұзу;

c) компьютерлік сараптама;

d) кибершабуыл;

e) вирустық ластану.

3. Компьютерден жойылған деректерді талдау және қалпына келтіру үшін қандай құрал қолданылады?

a) антивирус;

б) брандмауэр;

c) дискіні тазалау;

d) деректерді қалпына келтіру;

д) жанжал.

4. Аталған әрекеттердің қайсысы киберқылмыстың мысалы болып табылады?

a) оның қауіпсіздігін жақсартуға көмектесу үшін компьютерлік желіні бұзу;

b) құпия ақпаратты ұрлау мақсатында зиянды бағдарламаларды тарату;

c) жүйені зиянды бағдарламалық жасақтамадан қорғау;

d) жүйеде осалдықтарды анықтау және бұл туралы әкімшіге хабарлау;

e) ақпараттың жоғалуын болдырмау үшін деректердің сақтық көшірмесін жасау.

5. Қазақстан Республикасындағы компьютерлік қылмыстарға қарсы іс-қимылды қандай заңнамалық акт реттейді?

a) Еуропа Кеңесінің киберқылмыс туралы Конвенциясы;

b) Біріккен Ұлттар Ұйымының халықаралық киберқауіпсіздік туралы Конвенциясы;

c) барлық жауаптар дұрыс;

d) дұрыс жауаптар жоқ;

e) Қазақстан Республикасының Қылмыстық кодексі.

6. Қандай қауіпсіздік шаралары компьютерлік қылмыстардың алдын алуға көмектеседі?

a) антивирустық бағдарламаны үнемі жаңартып отыру және деректердің сақтық көшірмесін жасау;

b) ақпаратқа жылдам қол жеткізу үшін жалпыға ортақ құпия сөздерді пайдалану;

c) желіні жылдамдату үшін брандмауэрді өшіру;

d) барлық есептік жазбалар мен жүйелерге кіру үшін бір құпия сөзді пайдалану;

e) құпия ақпаратты жалпыға қол жетімді серверлерде орналастыру.

7. Компьютерлік қылмыстың ұйым үшін салдары қандай?

a) компанияның беделін жақсарту;

b) құпия ақпараттың және қаржылық шығындардың жоғалуы;

c) сату мен пайданың артуы;

d) серіктестікті нығайту;

e) желінің қауіпсіздік деңгейін арттыру.

8. Компьютерлік криминалистика үшін қандай арнайы құралдар қолданылады?

a) Wireshark, қабық, FTK;

б) Microsoft Word, Excel, PowerPoint;

c) Adobe Photoshop, Illustrator, InDesign;

d) Windows Media, iTunes, Spotify ойнатқышы;

e) Google Chrome, Firefox, Safari.

9. Компьютерлік қылмыстарды сәтті тергеу үшін қандай құзыреттер қажет?

a) бағдарламалау негіздері мен алгоритмдерін білу;

b) математикалық есептерді шеше білу;

c) желілік құрылғылармен жұмыс тәжірибесі;

d) халықаралық құқықты білу;

e) экстремалды жүргізу дағдылары.

10. Киберқылмыс дегеніміз не?

a) киберкеңістікте жасалатын құқыққа қайшы әрекеттер;

b) ақпараттық технологияларды заңды пайдалану;

c) қаржымен айла-шарғы жасау;

d) зиянды бағдарламалық қамтамасыз ету;

e) интернеттегі спам және алаяқтық.

§4. Оқиға орнын тексеру, компьютерлік техника құралдары мен ақпарат тасығыштарды алу және тексеру

Компьютерлік саладағы құқық бұзушылық туралы істер бойынша тексерулер жүргізілуі мүмкін:

– оқиға орындары;

– есептеу техникасы құралдарын;

– электрондық ақпарат тасығыштар;

– электрондық құжаттар.

Маманның қатысуымен арнайы іс-шараларды өткізу кезінде негізгі міндет компьютерлік жүйелерде және электрондық ақпарат тасымалдағыштарда бар ақпараттың сақталуын қамтамасыз ету болып табылады. Ол үшін істің мән-жайына байланысты:

– энергияға тәуелді деректердің сақталуын қамтамасыз ету үшін энергиямен жабдықтауды өшіруге жол бермеңіз (тарату тақтасын қорғау қажет болуы мүмкін);

– тергеу тобының мүшелеріне де компьютерлермен және ақпарат құралдарымен кез-келген манипуляция жасауға тыйым салу, барлық әрекеттерді маман орындайды, егер маман өз қолымен әрекет ете алмаса, ол оның бақылауымен жүзеге асырылады;

– жұмыс істеп тұрған компьютерлерді пернетақта пернелерін, жүйелік блок түймелерін және құрылғыларды кездейсоқ немесе әдейі басудан қорғаңыз;

– барлық қызметкерлерді компьютерлік техникамен және ақпарат тасығыштармен өз бетінше манипуляциялауға жол бермеу туралы ескерту;

– компьютерлер мен ақпарат тасымалдағыштар орналасқан үй-жайлардан барлық жарылғыш, каустикалық және тез тұтанатын материалдарды алып тастаңыз;

– сымсыз деректер жүйелерін өшіруді қамтамасыз етіңіз.

Егер соңғы тармақ сақталса, кейбір ақпаратты қашықтағы желілік ресурста өңдеуге болатындығын есте ұстаған жөн, бұл жағдайда белгілі бір уақытта желілік ресурстың деректерін тіркей отырып, осындай ақпаратты сақтау үшін шаралар қабылдау қажет.

SVT және электрондық тасымалдағыштарды тексерудің мақсаты, ең алдымен, оқиға немесе қылмыс жасау нәтижесінде пайда болған іздерді анықтау, сондай-ақ SVT және электрондық тасымалдағыштардың техникалық жағдайын анықтау болып табылады. Компьютерлік ақпаратты іздеу және тіркеу, әдетте, орындарда жүзеге асырылады:

– ақпаратты тікелей өңдеу және тұрақты сақтау;

– компьютерлік жабдықты тікелей пайдалану;

– компьютерлік ақпаратты және АТС сақтау, өңдеу немесе беру құралдарын пайдалану қағидаларын тікелей бұзу;

– зиянды салдардың басталуы.

Көптеген басқа дәлелдерден айырмашылығы, компьютерлік ақпаратты адам тікелей қабылдай алмайды. Оны қабылдау үшін техникалық аппараттық және бағдарламалық жасақтама арқылы қажет, және бұл техникалық

делдалдардың саны мен күрделілігі соншалықты үлкен, сондықтан бастапқы ақпарат пен адам қабылдаған бейненің арасындағы байланыс әрдайым айқын бола бермейді. Сонымен, компьютерлік құқық бұзушылықтар жағдайында тексеру визуалды тексеру емес, қолданылатын техникалық құралдар мен олардың жұмыс істеу принциптері туралы белгілі бір білімді қажет ететін аспаптық тексеру болып табылады. Сондықтан компьютерлік техниканы, электрондық ақпарат тасығыштарды және электрондық құжаттарды қарау маманның қатысуымен жүргізіледі.

Оқиға орнын тексеру кезінде бастапқыда оқиға (оқиға)туралы жалпы ақпарат анықталады:

– оқиғаның анықталған күні мен уақыты (құқық бұзушылық белгілері);

– оқиғаны анықтаған адамның байланыс деректері;

– оқиға түрі;

– тартылған компьютерлік жүйенің бұзылу белгілерін анықтау құралдары;

– жүйені қалпына келтіру бойынша қабылданған іс-шаралар;

– оқиға қазіргі уақытта жалғасуда ма;

– анықтау құрылғысы туралы ақпарат.

Оқиғаға қатысатын құрылғылар орналасқан үй-жайға қатысты мыналар анықталады:

– жұмыс/ жұмыс уақытынан тыс уақытта үй-жайға кім кіре алады;

– қол жеткізуді бақылау және басқару жүйесінің болуы (СКУД);

– бейнебақылаудың болуы;

– күзеттің болуы.

Бұдан басқа, ұйымның Итинфрақұрылымын ұйымдастыру туралы деректер анықталуда:

– құрылғылардың орналасуы, желі топологиясы;

– сымсыз желілердің болуы;

– жүйелік әкімшілендіру туралы деректер (жүйелік әкімшінің байланыс деректері);

– домен, жұмыс станцияларындағы пайдаланушылардың құқықтары, саясаттар;

– Интернетке кіру қалай жүзеге асырылады (технология, қосылу схемасы);

– қызмет провайдері, хостинг провайдері, домендік атауды Тіркеуші;

– брандмауэр/ прокси-сервер деректері;

– ұйымның сыртқы IP мекенжайлары;

– соңғы уақытта жабдықтың штаттық/ штаттан тыс істен шығуы болды ма.

Жүйелік әкімшінің сауалнамасы келесі сұрақтарды анықтауға мүмкіндік береді:

– пайдаланылатын серверлердің саны мен түрлері;

– жұмыс орындарының саны мен түрлері;

– қолданылатын операциялық жүйелердің түрлері;

– қолданылатын қолданбалы бағдарламалық жасақтама (мәліметтер базасы, құжат айналымы жүйелері және т. б.);

– қолданылатын ақпаратты қорғау және шифрлау құралдары;

– ортақ деректер файлдарының, серверлік дискілердің және дерекқорлардың резервтік көшірмелерінің болуы және сақтау орны;

– жүйе әкімшілерінің құпия сөздері;

– пайдаланушы пар мен парольдер.

Қатысатын компьютерлік құрылғылар үшін мыналар анықталады:

– құрылғының (компьютердің) атауы және оның жергілікті желідегі IP мекенжайы;

– пайдаланушының аты-жөні;

– операциялық жүйенің түрі;

– MS Office нұсқасы;

– антивирустық бағдарламаның болуы және антивирустық мәліметтер базасының өзектілігі;

– іске қосылған процестер;

– желілік қосылыстар және қызметтер;

– операциялық жүйенің жаңартулары;

– пайдаланылған шолғыш, нұсқа;

– журналдау, операциялық жүйенің журналдары теңшелген бе;

– құрылғы түнде өшеді ме.

Құқық бұзушылық іздерін және басқа да табылған заттарды тексеру әдетте сол жерде жүргізіледі. Егер тексеру жүргізу үшін ұзақ уақыт талап етілсе немесе орнында тексеру қиын болса, онда заттар алынып, буып-түйіліп, мөрленіп, тексеру орнында тергеушінің қолымен куәландырылуы тиіс. Қылмыстық іске қатысы болуы мүмкін заттар ғана алып қоюға жатады. Бұл ретте тексеру хаттамасында мүмкіндігінше алынатын заттардың жеке белгілері мен ерекшеліктері көрсетіледі. Тексеру кезінде табылған және алынған барлық нәрсе тексеруге қатысушыларға көрсетілуі керек.

Тексеру барысында жүргізілетін барлық іс-әрекеттер хаттамаланады. Тергеу әрекетінің барысы мен нәтижелерін тіркеудің техникалық құралдарын қолданған жағдайда куәгерлердің қатысуынсыз тексеру жүргізуге рұқсат етіледі (әдетте, бейнежазба).

Алу қылмыстық іс үшін маңызы бар белгілі бір заттар мен құжаттарды алып қою қажет болған кезде және егер олардың қайда және кімде екендігі нақты белгілі болса жүргізіледі. Мемлекеттік немесе федералдық заңмен қорғалатын өзге де құпияны қамтитын заттар мен құжаттарды, азаматтардың банктердегі және өзге де кредиттік ұйымдардағы салымдары мен шоттары туралы ақпаратты қамтитын заттар мен құжаттарды алу сот шешімі негізінде жүргізіледі.

Қаржылық қылмыстар бойынша (алаяқтық, иемдену немесе жымқыру, алдау немесе сенімді теріс пайдалану арқылы мүліктік зиян келтіру – кәсіпкерлік қызмет саласында, сондай-ақ коммерциялық, банктік және салықтық құпияларды жария ету, бағалы қағаздарды шығару кезінде теріс пайдалану және т. б. қылмыстар.

Электрондық ақпарат тасығыштар маманның қатысуымен тергеу іс-қимылдарын жүргізу барысында алынады. Алынатын электрондық ақпарат тасығыштардың заңды иесінің немесе оларда қамтылған ақпарат иесінің

өтініші бойынша тергеу әрекетіне қатысатын маман алынатын электрондық ақпарат тасығыштардан куәгерлердің қатысуымен ақпаратты көшіруді жүзеге асырады.

Ақпаратты көшіру алынатын электрондық ақпарат тасығыштардың заңды иесі немесе оларда қамтылған ақпараттың иесі ұсынған басқа электрондық ақпарат тасығыштарға жүзеге асырылады. Егер көшіру оның жоғалуына немесе өзгеруіне әкеп соғуы мүмкін болса, ақпаратты көшіру жүзеге асырылмайды. Көшірілген ақпаратты қамтитын электрондық ақпарат тасығыштар алынатын электрондық ақпарат тасығыштардың заңды иесіне немесе олардағы ақпараттың иесіне беріледі.

Көшірілген ақпаратты қамтитын ақпаратты көшіруді жүзеге асыру және электрондық ақпарат тасығыштарды беру туралы алынатын электрондық ақпарат тасығыштардың заңды иесіне немесе олардағы ақпараттың иесіне тергеу әрекетінің хаттамасына жазба жасалады.

Алынған электрондық ақпарат тасығыштар қылмыстық істе бөгде адамдардың оларда қамтылған ақпаратпен танысу мүмкіндігін болдырмайтын және олардың аталған ақпараттың сақталуы мен сақталуын қамтамасыз ететін жағдайларда мөрленген түрде сақталады.

Тергеуші тергеу әрекетін жүргізу барысында Электрондық ақпарат тасығышта қамтылған ақпаратты көшіруді жүзеге асыруға құқылы. Тергеу әрекетінің хаттамасында ақпаратты көшіруді жүзеге асыру кезінде қолданылған техникалық құралдар, оларды қолдану тәртібі, осы құралдар қолданылған электрондық ақпарат тасығыштар және алынған нәтижелер көрсетілуі тиіс. Хаттамаға тергеу әрекетін жүргізу барысында басқа электрондық ақпарат тасығыштардан көшірілген ақпаратты қамтитын электрондық ақпарат тасығыштар қоса беріледі. Бұл дәлелді мәні бар ақпараттың көшірмесінің пайда болу фактісін іс жүргізу куәлігін алуға мүмкіндік береді.

Тергеу әрекеті процесінде ақпаратты көшіру рәсімі мәліметтердің дұрыстығы мен өзгермейтіндігін қамтамасыз ету міндеттерін шешуге мүмкіндік беруі тиіс. Яғни, ақпаратты көшіру кезінде оны жоғалту немесе өзгерту мүмкіндігін болдырмайтын жағдайлар қамтамасыз етілуі тиіс. Көшіру әдісін таңдаудағы қателіктер, осы салада арнайы білімі жоқ адам көшіретін ақпарат көлемі алынған деректерді дәлел ретінде пайдалану мүмкіндігін мүлдем жоққа шығаруы немесе оларды әрі қарай сараптамалық зерттеу мүмкіндігін төмендетуі мүмкін. Сондықтан электронды медианы көшіру және басқа компьютерлік ақпаратты бекіту әдетте маманмен жүзеге асырылады.

Кейбір жағдайларда із жасау механизмінің заңдылықтарын ескере отырып тасымалдаушыларды алу дәлелді ақпаратты бекіту мақсатында қолайсыз болып табылады. Атап айтқанда, серверлердің қатты дискілерінің массивтерінде сақталған мәліметтерді осы дискілерді алып тастау арқылы бекіту өте қиын. Деректердің үлкен массивтерін сақтаудың және өңдеудің заманауи технологиялары компьютерлік технологияның жеке құралдары ретінде серверлер жиынтығының архитектурасын білдіреді, оның ішінде бір-бірінен үлкен қашықтықта орналасқан, олар ақпараттың бірыңғай қоймасы

ретінде жұмыс істейді. Жеке құрылғыларды немесе олардың қандай да бір жиынтығын физикалық алып қою қызығушылық тудыратын деректерді қалпына келтіру мүмкін кстігіне әкелуі мүмкін.

Қалыптасқан криминалистикалық практикаға сәйкес, егер із ақпаратын тасымалдаушыны заттай алып қою мүмкін болмаса, одан маңызды белгілерді көрсететін көшірме алынады. Іс жүзінде бұлтты қоймаларда немесе медиа-контентті (YouTube, Вконтакте және т. б.) хостинг және орналастыру қызметтерін ұсынатын компаниялардың серверлерінде орналастырылған деректерге қатысты дәлелді ақпаратты тіркеудің жалғыз қолайлы тәсілі оны көшіру болып табылады. Деректерді беру және сақтау серверлерінен ақпаратты алу кезінде барлық диск массиві емес, тек қажетті ақпарат алынады, бұл ретте мүмкіндігінше электрондық тасымалдағыштар мен компьютерлік техниканы алып қоймай ақпаратты тіркеу (көшіру) жүргізіледі.

Компьютерлік техниканы тексеру, электрондық ақпарат тасығыштарды алу және олардан ақпаратты көшіру кезінде маман ҚР ҚІЖК-нің тиісті рәсімдерге жоғарыда баяндалған талаптарын ұстанады:

– СВТ-ны, ақпарат тасығыштарды тексеру, оларды алып қою және ақпаратты көшіруді тәуелсіз маман екі куәгердің қатысуымен жүргізеді (әдетте, ұйым қызметкерлері тартылады, олар ұйым өкілдері ретінде де әрекет етеді);

– маман қабылдаған барлық іс-әрекеттер хаттамаланады, сонымен қатар, әдетте, фотосурет / бейне түсіру арқылы жазылады;

– алынатын ақпарат тасығыштар мөрленеді және олардағы ақпараттың бүлінуін және оған қол жеткізуді болдырмау үшін сенімді жерде (мысалы, сейфте) сақталады;

– барлық қатысушы тараптар куәландырған ақпаратты көшіру, деректерді түсіру/ алу, ақпарат тасығыштарды алып қою, оларды мөрлеу, материалдарды зерттеуге беру туралы актілер жасалады.

Көрсетілген актілерде объектілердің және олардың көздерінің толық тізімдемесі болуға тиіс. Яғни, объектіні бірегей сәйкестендіруге мүмкіндік беретін деректемелер көрсетілуі керек (мысалы, қатты магниттік дискілердегі жұмыс станциялары мен дискілердің сериялық нөмірлері, сондай-ақ олардың түрі). Мөрленген ақпарат тасығыштар тиісті актімен бірге оларды зерттеуге (сараптамаға) немесе Құқық қорғау органдарына бергенге дейін сақталады.

Оқиға орнын тексеру, компьютерлік техника құралдары мен ақпарат тасығыштарды алу және тексеру нәтижесінде дәлелдер мен дәлелдемелерді анықтауға көмектесетін маңызды деректер алынды. Бұл рәсімдерді тиімді жүргізу қылмыстық істерді ойдағыдай шешу үшін өте маңызды, өйткені ол қажетті дәлелдемелерді жинауға және қылмыстың мән-жайларын анықтауға мүмкіндік береді. Заманауи технологиялар мен әдістерді қолдана отырып, тексеру мен қазуды жүзеге асыру жұмысты тезірек және дәл жүргізуге мүмкіндік береді. Бұл процедуралардың дұрыс орындалуы қылмыстарды тергеудің негізгі элементі болып табылады және қылмыстық істердің әділ және әділ қаралуын қамтамасыз етеді.

Өзін-өзі бақылау мәселелері:

1. Оқиға орнын тексеру қандай кезеңдерді қамтиды?
2. Қазу кезінде қандай әдістер мен әдістер қолданылады?
3. Компьютерлік техника құралдарын қарау кезінде құқық қорғау органдарының қызметкерлері қандай өкілеттіктерге ие?
4. Компьютерлік техника мен ақпарат тасығыштарды тығыздау және алып қою қалай жүргізіледі?
5. Цифрлық дәлелдемелерді бекіту және сақтау қалай жүзеге асырылады?
6. Компьютерлік техниканы тексеру кезінде компьютерлік сараптама мамандарының рөлі қандай?
7. Деректердің тұтастығын сақтау тұрғысынан компьютерлік техниканы тексеру және алу кезінде қандай ережелерді сақтау керек?
8. Алынған компьютерлік техника мен ақпарат тасығыштарды талдау қалай жүзеге асырылады?
9. Компьютерлік медиадан жойылған деректерді қалпына келтіру үшін қандай әдістерді қолдануға болады?
10. Компьютерлік техниканы тексеру және алу нәтижесінде жиналған дәлелдемелерді пайдалану кезінде қандай шектеулер мен талаптар бар?

Өзін-өзі бақылауға арналған тест тапсырмалары:

1. Оқиға орнын тексерудің негізгі кезеңдері қандай?

a) оқиға орнын бекіту;

b) дәлелдемелер жинау;

c) алынған ақпаратты бағалау;

d) жоғарыда айтылғандардың барлығы;

e) тек a) және b).

2. Компьютерлік техниканы алудың негізгі мақсаты қандай?

a) компьютерлер мен ноутбуктерді алу;

b) қылмысқа байланысты цифрлық құрылғылар мен ақпарат тасығыштарды іздеу және алып қою;

c) компьютерлік техниканың техникалық жай-күйін бағалау;

d) жоғарыда айтылғандардың барлығы;

e) тек b) және c).

3. Ақпарат құралдарын тексерудің әдеттегі процедурасы қалай көрінеді?

a) компьютерге қосылу;

b) медианы пішімдеу;

c) деректерді көшіру;

d) мамандандырылған бағдарламалық қамтамасыз етуді пайдалана отырып талдау;

e) мазмұнды іріктеп тексеру.

4. Аталған іс шаралардың қайсысы оқиға болған жерді тексеру процесіне енгізіледі?

a) фотофиксация;

b) үлгілерді таңдау;

c) заттарды алып қою;

d) сараптамалық қорытынды;

e) жоғарыда айтылғандардың барлығы.

5. Компьютерлік техникаға қатысты оқиға орнын тексеру кезінде қандай әрекеттер жасалуы мүмкін?

a) куәгерлерге сұрақтар қою;

b) қатты дискінің көшірмесін жасаңыз;

c) операциялық жүйенің тізілімін талдау;

d) желілік белсенділікті талдау;

e) жоғарыда айтылғандардың барлығы.

6. Сот сараптамасының бөлігі ретінде қатты дискіден қандай деректерді табуға болады?

a) жергілікті файлдар;

b) кірген веб-сайттардың тарихы;

c) электрондық пошта мұрағаты;

d) жоғарыда айтылғандардың барлығы;

e) тек b) және c).

7. Сандық құрылғыларды алу кезінде әдетте қандай әдістер қолданылады?

a) классикалық тәсіл;
b) форензиялық талдау;
c) облыстар бойынша бөлу әдісі;
d) тәуелсіз сараптама;
e) жоғарыда айтылғандардың барлығы.

8. Оқиға орнын тексеру кезінде сандық құрылғыларды талдаудың мақсаты қандай?

a) жойылған файлдарды қалпына келтіру;
b) қылмыстық әрекеттің іздерін іздеу;
c) жасырын ақпаратты анықтау;
d) жоғарыда айтылғандардың барлығы;
e) тек b) және c).

9. Оқиға болған жерді тексеру кезінде қандай техникалық құралдар пайдаланылуы мүмкін?

a) мамандандырылған бағдарламалық қамтамасыз ету;
b) тазалау құралдары;
c) анализатор компьютерлері;
d) тіркеушілер;
e) жоғарыда айтылғандардың барлығы.

10. Оқиға орнын тексерудің негізгі принциптері қандай?

a) дәлелдемелердің сақталуын қамтамасыз ету;
b) дәлелдемелер тізбегін сақтау;
c) тексеру хаттамасын жүргізу;
d) жоғарыда айтылғандардың барлығы;
e) тек a) және b).

§5. Электрондық құжаттарды қарау

Ұзақ уақыттың жалғасында қоғамның қарқынды цифрлануы байқалады, оның қорытындысы, басқалармен қатар, электрондық құжаттарды белсенді енгізу болып табылады. Электрондық құжаттардың дәстүрлі құжаттармен салыстырғанда артықшылықтары даусыз. Электрондық құжаттарды сақтау, беру оңайырақ (өйткені оларда бір материалдық құралға сілтеме жоқ), сонымен қатар өңдеу. Алайда, мұндай артықшылықтарды құжат айналымының адал субъектілері ғана емес, сонымен бірге қылмыстық қоғамдастық өкілдері де пайдалана алады. Сонымен қатар, қылмыс жасау кезінде электронды құжаттарға жүгінетін қылмыскерлер көбінесе қылмыстарды жасыру дағдыларын дамытады, бұл қылмыстарды тергеу процесін қиындатуы мүмкін. Электрондық құжаттар пайда болатын қылмыстарды тергеуге қарсы тұруды жеңу үшін қызметкерлер электрондық құжаттарды қарау тактикасы туралы жақсы білуі керек.

Электрондық құжаттардың заңды анықтамасы электрондық құжаттарға не жатқызу керек деген мәселені ашпайды. Бұл жағдайда зерттеушілердің пікірлері осы тұрғыдан ерекшеленеді.

Алайда, «электрондық құжат» ұғымының заңды анықтамасы «ресми», «заңды маңызды» және т.б. тұжырымдамаларды қамтымайтынын атап өтуге болмайды. осыған байланысты мен қылмыстық іс жүргізу құқығы аясында Ресми құжаттар ғана емес, сонымен қатар ақпарат электрондық құжаттар бола алады деген пікір білдіргім келеді, заңды маңызды емес, бірақ соған қарамастан дәлелді мәнге ие.

Бұдан басқа, құқық қолдану практикасы Интернет желісіндегі хат-хабарларды, әлеуметтік желілердің скриншоттарын, бейнекамералардың деректерін және т. б. сот дәлелді маңызы бар құжаттар ретінде тани алатынын айғақтайды.

Электрондық құжаттарды жасау және пайдалану барысында қалатын цифрлық іздерге ерекше назар аударған жөн. Сот Электронды құжат ретінде қарастыруы мүмкін әртүрлі деректерді жасау кезінде қылмыскер бір уақытта Цифрлық іздерді жасауға ықпал етеді деп айтуға болады.

Осылайша, электрондық құжаттарды жасау, пайдалану және беру барысы цифрлық іздерді қалыптастырумен қатар жүреді, соның негізінде тергеу органдары қылмысты тергеудің одан әрі жолдарын анықтай алады немесе адамның қылмыс жасауға қатысы бар екенін мәлімдей алады.

Электрондық құжаттарды қарауға қатысты тактикалық қадамдарды нақтыламас бұрын тексеруді тергеу әрекеті ретінде қысқаша сипаттағым келеді.

Тексеру қылмыстардың барлық дерлік санаттарын тергеу кезінде жүргізіледі, соның арқасында тергеуші іс бойынша айтарлықтай ақпарат ала алады. Белгіленген тергеу әрекетінің мәні қылмыс оқиғаларын, сондай-ақ оған қатысы бар адамдарды анықтауға болатын дәлелдерді іздеуге байланысты деп айтуға болады.

Мысал ретінде электрондық құжаттардың келесі жіктелуін келтіруге болады:

1. Тіршілік формасына негізделген: виртуалды және материалдық. Материалдық құжаттардың қатарына электрондық тасымалдағыштарда тіркелген, семантикалық мазмұнға ие және тек электрондық ортада болатын ақпаратты тасымалдайтын объектілер жатады. Виртуалды құжат-бұл пайдаланушының ақпараттық жүйемен өзара әрекеттесуі нәтижесінде пайда болған ақпараттық объектілердің жиынтығы.

2. Мазмұны негізінде: мазмұнында мәтіндік ақпарат, графика, бейнежазба және т. б. бар құжаттар.

3. Қауіпсіздік дәрежесіне негізделген: жабық және ашық.

4. Материалдық тасығыштың типі негізінде: компьютерлік ақпараттың физикалық тасығыштарында орналастырылған құжаттар (сыртқы жад құрылғылары, мысалы, қатты дискілер, флэш-дискілер және т.б.); электрондық есептеу машинасының жедел есте сақтау құрылғысында (бұдан әрі – ЖЖҚ) орналастырылған құжаттар; перифериялық құрылғылардың ЖЖҚ-да орналастырылған құжаттар; құжаттар, компьютерлік байланыс құрылғылары мен желілік құрылғылардың жедел жадында орналастырылған.

Жоғарыда айтылғандар электрондық құжаттарды қарау тактикасы екі жақты сипатта болады деген қорытынды жасауға мүмкіндік береді. Бір жағынан, осы немесе басқа электрондық құжат орналасқан материалдық тасымалдаушының нысаны маңызды. Екінші жағынан, электрондық құжаттың өзінде орналастырылған ақпарат маңызды дәлелді рөлге ие.

Электрондық құжаттарды қарау тактикасын анықтай отырып, тергеудің бастапқы кезеңінде құжаттардың қайсысының дәлелді мәні бар екендігі белгісіз болатынын көрсетеміз. Осыған байланысты қызметкерлер дәлелдер болуы мүмкін электрондық құжаттардың барлық көлемін тексеруі керек.

Электрондық құжаттарды алу көзделген жерге келгеннен кейін алынатын объектілер туралы ақпарат алу қажет, мысалы, парольдер, логиндер, желілік өзара іс-қимыл құрылымы, ақпаратты көшіру мүмкіндігі және т.б. Мұндай ақпаратты жинауды заңды тұлғадан тиісті тасығышты алып қою кезінде электрондық ақпараттық тасығыштың иесіне не штаттық маманға жүгіну арқылы жүзеге асыруға болады.

Ақпаратты алу барысында маман әрбір нақты жағдай шеңберінде алудың ең тиімді тәсіліне сүйенуі тиіс: ақпаратты электрондық тасымалдаушымен (сервермен) алып қою немесе ақпаратты көшіру. Бұл ретте сервермен бірлесіп электрондық жеткізгіштерде орналасқан Электрондық ақпаратты алып қоюды ұсынуға болады.

Күшейтілген білікті электрондық қолтаңбамен (бұдан әрі – БЭК) куәландырылған электрондық құжаттарды қарау тактикасы мәселесі ерекше назар аударуды талап етеді. Мұндай құжаттарды қарау барысында тергеушілер БЭК-тің болу мәселелерін мұқият зерделеуі тиіс. Бұл тексеру арнайы бағдарламалық жасақтаманың көмегімен жүзеге асырылуы керек дегенді білдіреді, соның арқасында БЭК сенімділігі анықталады.

Электрондық құжаттарды қарау кезінде олардың жеке мазмұнының өзгеру белгілері анықталған жағдайлар бар. Бұл жағдайда тергеуші кейбір тармақтарға назар аударуы керек.

Электрондық құжаттарды бұрмалау фактілері анықталған жағдайда тергеуші тексеру барысында мыналарға назар аударуы тиіс:

1. Осы электрондық құжатты жасау уақытына.

2. Құжатқа өзгерістер енгізілген күн мен уақытқа, өзгерістер санына.

3. Енгізілген өзгерістердің мазмұнына (зерттелетін құжатты оның бұрынғы нұсқаларымен, жойылған ақпаратты қалпына келтіру әдісімен және т. б. салыстыру арқылы анықтауға болады.

4. Мұрағат қалталарында, «себетте» және т.б. орналасуы мүмкін құжаттың бұрынғы нұсқалары үшін.

5. Құжаттың резервтік көшірмелерінің болуына.

6. Электрондық құжаттың мәтінін басып шығарылған құжаттармен, қолда бар үлгілермен салыстыру.

Жалпы, электрондық құжаттарды қараудың келесі жалпы тактикалық ерекшеліктерін бөліп көрсетуге болады:

1. Тергеудің бастапқы кезеңінде электронды құжаттардың едәуір көлемі тексерілуге тиіс, өйткені көбінесе қандай құжатта дәлелді маңызы бар ақпарат болуы мүмкін екендігі белгісіз.

2. Тексеруге электрондық құжаттарды тиімді іздестіруді жүзеге асыруға, оларды алып қоюға, сондай – ақ (жекелеген жағдайларда) қылмыскердің құжаттарды алып тастағаннан кейін қалпына келтіруге қабілетті мамандарды тарту қажет.

3. Тексеру құжаттың электрондық жеткізгішінің өзіне де, электрондық құжаттың мәтінінде тікелей қамтылған ақпаратқа да қатысты жүргізілуі тиіс.

4. Электрондық құжат жалғандықтың ықтимал белгілеріне сәйкестігі тексерілуі керек.

Құжатты электронды тасымалдағышта тексеруді әдетте тергеуші немесе анықтаушы пән маманының қатысуымен жүргізеді. Мұндай тексерудің мақсаты құжаттың сыртқы белгілері мен деректемелерін анықтау және талдау, оның мазмұнын талдау, оны қолдан жасаудың (бұрмалаудың) мүмкін белгілерін анықтау болып табылады.

Its-те қамтылған құжаттарды, атап айтқанда интернетті қарау кезінде тексеру жанама түрде (its арқылы) жүзеге асырылады. Тексеру осы желіге қосылған және алдын ала тергеу органының бөлімшесінде орналасқан жұмыс жабдығының (компьютердің) көмегімен жүргізілуі мүмкін.

Сонымен қатар, автоматты ауысуды қамтитын ресурстарға сілтемелер техникалық тұрғыдан ресурстың өзіне ұқсас (әлеуметтік медиа ресурстарында, мысалы, бейненің өзі емес, экстремистік бағыттағы бейнелерге сілтемелер орналасуы мүмкін).

Интернет-ресурсты тексеру хаттамасы оның сыртқы түрін және тергеушінің амалдық жүйе мен шолғышты жүктеуден бастап сілтемелер мен мәзір элементтеріне дәйекті өтуге дейінгі барлық әрекеттерін сипаттайды. Желіде орналастырылған ақпарат статикалық емес болғандықтан, оны кейіннен өзгертуге немесе жоюға болатындықтан, тексеру уақытын көрсету керек, яғни ақпаратты тіркеудің әр әрекеті міндетті түрде уақытқа байланысты болуы керек. UTC уақыт белдеуін немесе уақытын Бүкіләлемдік Үйлестірілген уақытты (UTC), сондай-ақ сайттың әр көшірілген бетінің

мекен-жайын жазып, хаттамада көрсету керек. Сайт беттерінің мазмұнын браузердің стандартты құралдарының көмегімен де, сайттың барлық мазмұнын көшіруге арналған мамандандырылған бағдарламалық жасақтаманың көмегімен де көшіруге болады. Кейбір жағдайларда парақтың скриншотын алу жеткілікті. Youtube-тен бейнелерді көшіру үшін Интернетте еркін таратылатын арнайы бағдарламалар қолданылуы мүмкін.

Көшірілген файлдар жазылмайтын сақтау құралына (CD, DVD) сақталады, бұл оларды одан әрі Өзгертуді болдырмайды. Тексеру хаттамасында файлдарды қарау және көшіру кезінде қолданылған техникалық құралдар (компьютер) және бағдарламалық қамтамасыз ету көрсетіледі, файлдардың өзі тексеру хаттамасына қосымша ретінде ресімделеді.

Егер желіде орналастырылған ақпаратты тіркеуді ұйымның өкілі немесе жеке тұлға жүргізсе, онда веб-беттердің мазмұнын нотариалды куәландыру пайдаланылады.

Қорытындылай келе, электрондық құжаттарды қарау тактикасы іс жүзінде электрондық құжаттардың материалдық тасымалдаушыларын да, құжаттардың мазмұнын да тексеруді қамтиды деген қорытынды жасауға болады. Әрине, электрондық құжаттарды қарау ерекшелігі тергеуге жататын нақты қылмысқа, ол бастапқы тергеу жағдайына байланысты. Дегенмен, электрондық құжаттарды қараудың жалпы тактикалық ережелері бар, оларды сақтау міндетті болып табылады. Сонымен қатар, электрондық құжаттарды қарау кезінде ағасы оны жоғалту ықтималдығына байланысты қауіп-қатерді есептеу үшін қажет. Мұндай қауіптердің алдын алу үшін арнайы білімі бар маманның көмегі қажет болуы мүмкін.

Өзін-өзі бақылау мәселелері:

1. Электрондық құжаттарды қараудың негізгі мақсаттары қандай?
2. Электрондық құжаттардың қандай түрлері тексерілуі мүмкін?
3. Электрондық құжаттарды қарау үшін қандай әдістер қолданылады?
4. Электрондық құжаттарды тексеру барысында олардың аутентификациясы қалай жүзеге асырылады?
5. Электрондық құжаттарды қарау кезінде қандай қауіптер туындауы мүмкін?
6. Электрондық құжаттарды қарау кезінде метадеректерге талдау қалай жүргізіледі?
7. Электрондық құжаттарды қарау кезінде қандай стандарттар мен ережелерді сақтау керек?
8. Электрондық құжаттарды қарау кезінде құпия ақпаратты қорғау қалай жүзеге асырылады?
9. Электрондық құжаттарды қарау рәсімінің негізгі кезеңдері қандай?
10. Электрондық құжаттарды қарау үшін қандай нақты дағдылар мен білім қажет?

Өзін-өзі бақылауға арналған тест тапсырмалары:

1. Электрондық құжаттарды қарау үшін қандай әдістерді қолдануға болады?

a) таңертең оқу;
b) метадеректерді талдау;
c) фотоэлектрондық микроскоптарды қарау;
d) оқу;
e) дыбыс құрылымын талдау.

2. Электрондық құжаттың метадеректері дегеніміз не?

a) құжаттың мазмұны;
b) құжат туралы ақпарат;
c) материалдық тасымалдаушы;
d) метадеректер дегеніміз не;
e) бағдарламалық жасақтаманың сипаттамасы.

3. Электрондық құжаттардың қандай түрлері тексерілуі мүмкін?

a) тек суреттер;
b) тек мәтіндік файлдар;
c) кез келген сандық құжаттар;
d) тек Excel файлдары;
e) тек MP3 файлдары.

4. Электрондық құжаттарды тексеру кезінде олардың аутентификациясы қалай жүзеге асырылады?

a) мөртабан бойынша;
b) иісі бойынша;
c) дәміне қарай;
d) түсі бойынша;
e) кіріктірілген қолтаңба бойынша.

5. Электрондық құжаттарды қарау кезінде құпия ақпаратты қорғау қалай жүзеге асырылады?

a) қағазда;
b) шифрлау арқылы;
c) көпшілікке жариялау арқылы;
d) фильмде;
e) термиялық басып шығару арқылы.

6. Қағаз құжаттарды қараумен салыстырғанда электрондық құжаттарды қараудың қандай артықшылықтары бар?

a) құжаттамамен жұмыс процесін жеделдету;
b) сақтау орнын үнемдеу;
c) жоғары деректер қауіпсіздігі;
d) ақпаратты жылдам іздеу мүмкіндігі;
e) әдет және ыңғайлылық.

7. Электрондық құжаттарды қарау үшін қандай бағдарламалар мен қосымшаларды қолдануға болады?

a) MS Word;
б) Adobe Acrobat Reader бағдарламасы;

c) Google Docs;
d) Foxit Reader;
e) LibreOffice (Кітапхана кеңсесі).

8. Электрондық құжаттарды қарау процесі қандай?

a) тиісті бағдарламаны пайдаланып файлды ашу;
b) құжаттың мазмұнын оқу;
c) түсініктемелер мен белгілерді қосу мүмкіндігі;
d) құжатты қағазға басып шығару;
e) құжатты басқа форматқа түрлендіру (мысалы, PDF).

9. Қандай файл пішімдерін тексеруге болады?

a) docx (Microsoft Word);
b) .pdf (Portable Document Format);
c) xlsx (Microsoft Excel);
d) pptx (Microsoft PowerPoint);
e) jpg (сурет).

10. Электрондық құжаттарға қол жеткізуді бақылау қалай жүргізіледі?

a) құпия сөзді қорғау;
b) белгілі бір пайдаланушылар үшін шектеулі қол жетімділікті орнату;
c) деректерді шифрлау;
d) негізгі аутентификация;
e) пароль арқылы қол жетімді желілік протоколдарды пайдалану.

§6. Компьютерлік сараптаманың мақсаты

Компьютерлік сараптама-бұл құқықтық, техникалық немесе қауіпсіздік мәселелерін шешу үшін компьютерлік жүйелерді, деректерді және электрондық құрылғыларды талдау және зерттеу процесі. Компьютерлік сараптаманың мақсаты ақпараттық технологиялар мен нақты жағдайға байланысты деректерді объективті және кәсіби бағалауды қамтамасыз ету болып табылады.

Компьютерлік сараптаманың негізгі мақсаттарының бірі қылмыстық, азаматтық немесе әкімшілік істер шеңберінде дәлелдемелерді қамтамасыз ету болып табылады. Информатика мамандары қылмыстық әрекеттің жасалғанын анықтау, кінәлі тараптарды анықтау, сондай-ақ компьютерлік жүйелерде табылған мәліметтер негізінде оқиғалар тарихын қалпына келтіру үшін тәуелсіз зерттеулер жүргізеді.

Сонымен қатар, компьютерлік сараптама корпоративтік тергеу шеңберінде, соның ішінде ақпараттық қауіпсіздіктің бұзылуын, деректерге рұқсатсыз қол жеткізуді немесе құпия ақпараттың ағып кетуін анықтау үшін пайдаланылуы мүмкін. Компьютерлік сараптама сарапшылары осалдықтарды анықтау және оларды жою бойынша ұсыныстар беру үшін компанияның ақпараттық жүйелеріне аудит жүргізе алады.

Сондай-ақ, компьютерлік сараптама киберқауіпсіздік саласында маңызды рөл атқара алады. Осы саладағы сарапшылар хакерлік шабуылдарды зерттей алады, ақпараттық қауіпсіздіктің ықтимал қауіптерін талдай алады және олардың алдын алу және анықтау шараларын жасай алады.

Сонымен, компьютерлік сараптама сот практикасында зияткерлік меншікке, авторлық құқыққа немесе патенттерге қатысты дауларды шешу үшін пайдалы болуы мүмкін. Компьютерлік құқық сарапшылары заң бұзушылықтар жағдайларын зерттей алады және компьютерлік мәліметтер негізінде сараптамалық қорытынды бере алады.

Жалпы, компьютерлік сараптаманы тағайындау қауіпсіздікті қамтамасыз етуді, қылмыстық әрекеттерді анықтауды, дәлелдемелерді жинауды, дауларды шешуді және ақпараттық жүйелер мен деректерге қатысты мәселелер бойынша сараптамалық пікір беруді қамтиды. Бұл сала қазіргі әлемде маңызды компонент болып табылады, мұнда ақпараттық технологиялар үлкен рөл атқарады.

Арнайы білімнің көмегімен компьютерлік құралдарды зерттеу қылмыстық іс қозғалғанға дейін де, одан кейін де жүзеге асырылуы мүмкін. Мамандар бірқатар жағдайларда (мысалы, қылмыстық іс қозғалғанға дейін тексеру жүргізу кезінде) зерттеулер жүргізеді, бірақ бұл зерттеулер алдын-ала деп аталады және алынған нәтижелер дәлелді мәнге ие емес. Бұл әлі күнге дейін заттай дәлелдемелер мәртебесі жоқ, бірақ белгілі бір процессуалдық жағдайлар туындаған кезде болуы мүмкін компьютерлік құралдарды зерттеудің процессуалдық емес түрі туралы.

Міндеттер, мазмұн және әдістеме тұрғысынан алдын-ала зерттеу Сот-компьютерлік техникалық сараптамадан түбегейлі ерекшеленбейді, алайда мұндай зерттеудің нәтижелері сот дәлелдерінің көзі бола алмайды.

Белгілі бір процедуралық процедураны жүзеге асыру арқылы дәлелді мәнге ие бола алатын жедел ақпараттың кейбір түрлерінен айырмашылығы (мысалы, жедел қызметкердің есебінде ұсынылған объектілерді заттай дәлелдемелермен тану), алдын-ала зерттеу нәтижелері тікелей де, жанама түрде де сот дәлелдемелеріне айнала алмайды деп саналады.

Компьютерлік технологияларды қолдана отырып, қылмыстық және азаматтық істерді тергеу және сот арқылы қарау кезінде арнайы білімді қолданудың негізгі процедуралық формасы сот-компьютерлік сараптама болып табылады.

Сараптамалық зерттеу объектілері сараптама нәтижелері негізінде дәлелдемелер мәртебесіне ие болады және сараптама нәтижесінде алынған дәлелдемелік ақпарат көбінесе басқа көздерден пайда бола алмайды.

Сот-компьютерлік сараптама-инженерлік-техникалық сыныпқа жататын сот сараптамаларының дербес түрі. ЕЭК: объектінің компьютерлік құрал ретіндегі мәртебесін айқындау, оның тергеліп жатқан қылмыстағы рөлін анықтау және зерделеу, сондай-ақ кейіннен оны жан-жақты зерттеумен деректер тасымалдағыштардағы ақпаратқа қол жеткізу мақсатында жүргізіледі.

Сот сараптамасы теориясында, әдетте, «компьютерлік-техникалық сараптама» термині қолданылады және оның келесі түрлері бөлінеді: аппараттық-Компьютерлік, бағдарламалық-компьютерлік, ақпараттық-компьютерлік (деректерді сараптау) және компьютерлік-желілік.

Сараптама-криминалистикалық бөлімшелерге сараптама тағайындау кезінде «компьютерлік сараптама» термині пайдаланылады, ал тиісті зерттеулердің мазмұны "компьютерлік ақпаратты зерттеу"ретінде айқындалады. Тиісті сарапшылардың құзыретіне тек электрондық құрылғылардың ақпарат тасығыштарында бар БҚ және деректерге қатысты мәселелерді шешу кіреді. Компьютерлік жабдықты (аппаратураны) зерттеу мүмкіндігі туралы айтылмайды.

Осылайша, компьютерлік-техникалық сараптама мәселелеріне аталған мәселелерден басқа компьютерлік және желілік аппаратураны зерттеу мәселелерін де жатқызуға болады.

Компьютерлік сараптаманың шешіміне нақты сұрақ (сұрақтар) қойылады, мысалы, белгілі бір тапсырманы орындау үшін ақпарат тасымалдаушыларда бағдарламалық құралдар бар ма? Бұл ретте сарапшының алдына құқық емес, факт мәселелері қойылуы тиіс, өйткені соңғысы тергеушінің немесе соттың құзыретіне жатады. Мысалы, сарапшы Бағдарламаның бұл данасы контрафактілік екенін анықтай алмайды, ол тек контрафактілік белгілерді көрсетеді, мысалы, рұқсатсыз көшіруден қорғауды алып тастау, әзірлеуші жасамайтын бағдарламадағы өзгерістер, бағдарламалар пакетінің құрамы мен лицензияланған арасындағы айырмашылық (қосымша файлдардың болуы немесе болмауы) және т.б.

Компьютерлік саладағы құқық бұзушылықтар бойынша тергеу шеңберінде сараптамаға ұсынылатын объектілер әр түрлі:

– компьютерлік ақпарат (мәтіндік, графикалық, аудио және бейне файлдар, электрондық құжаттар, дерекқорлар, Журнал файлдары);

– бағдарламалық қамтамасыз ету;

– электрондық ақпарат құралдары (HDD, SDD, оптикалық дискілер, пластикалық карталар);

– компьютерлік техника (компьютерлер, ноутбуктер, смартфондар, электрондық дәптерлер, серверлік жабдықтар);

– перифериялық құрылғылар;

– баспа құрылғылары, көбейту техникасы және оларды қолдана отырып жасалған құжаттар;

– Its және байланыс желілері;

– телекоммуникациялық құрылғылар (ұялы байланыс аппаратурасы, деректерді берудің сымсыз цифрлық құрылғылары, желілік жабдықтар, маршрутизаторлар);

– өзге де СВТ (сандық фото-және бейнекамералар, цифрлық аудио-және бейнеаппаратура, бақылау-кассалық аппараттар, банкоматтар, Ойын автоматтары, арнайы техника құралдары);

– ақпаратпен, СВТ, ақпараттық және телекоммуникациялық жабдықтармен жұмыс жөніндегі құжаттама.

Ақпараттық объектілерді (деректерді)компьютерлік сараптаудың үлгілік мәселелері:

1. Зерттеуге ұсынылған ақпараттық объектілердің қасиеттері, сипаттамалары мен параметрлері (көлемі, жасалған күні-өзгерістері, атрибуттары және т.б.) қандай?

2. Ақпараттық объектінің нақты күйі стандартты күйге сәйкес келе ме?

3. Ақпараттық объектінің нақты күйі мен оның стандартты күйі арасында қандай сәйкессіздіктер бар?

4. Тасымалдағыштағы деректердің бастапқы күйі қандай (белгілі бір деректер жойылғанға немесе өзгертілгенге дейін қандай формада, қандай мазмұнда және қандай сипаттамаларда, атрибуттарда болған)?

5. Зерттеуге ұсынылған ақпараттық объектімен қандай операциялар жүргізілді?

Бағдарламалық құралдарды компьютерлік-техникалық сараптаудың үлгілік мәселелері:

1. Зерттеуге ұсынылған бағдарламалық жасақтаманың жалпы сипаттамалары (атауы, түрі, нұсқасы, жағдайы және т. б.) қандай?

2. Зерттеу үшін берілген функциялар қандай?

3. Белгілі бір функционалды тапсырманы орындау үшін осы бағдарламалық жасақтаманы пайдалану мүмкін бе?

4. Белгіленген параметрлерден ауытқулар бар ма?

5. Қандай қорғаныс мүмкіндіктері бар және олар қалай жүзеге асырылады?

6. Зерттеу үшін ұсынылған өзгерістермен қандай өзгерістер болды?

7. Енгізілген өзгерістер бағдарламалық құралға оны қорғауды жеңуге бағытталған ба?

8. Бағдарламалық жасақтаманы орнатқаннан бері оны пайдалану хронологиясы қандай?

9. Бағдарламалық жасақтамада ақпаратты жоюға, бұғаттауға, өзгертуге немесе көшіруге, компьютерлік жүйенің жұмысын бұзуға әкелетін дұшпандық функциялар бар ма?

Аппараттық құралдарды компьютерлік-техникалық сараптаудың үлгілік мәселелері:

1. Зерттеуге ұсынылған объект компьютерлік құрал ма?

2. Зерттелетін компьютерлік құралдың техникалық сипаттамалары (түрі, моделі, маркасы, көлемі, қуаты, деректерге қол жеткізудің орташа уақыты, деректерді беру жылдамдығы және т. б.) қандай?

3. Бұл компьютерлік құрал қандай функцияларды орындайды?

4. Ұсынылған аппараттық құралдың нақты күйі (ақаулы, ақаулы) қандай?

5. Онда типтік (қалыпты) параметрлерден ауытқулар, соның ішінде физикалық ақаулар бар ма?

6. Бұл аппараттық құралда қандай пайдалану режимдері орнатылған?

7. Компьютерде бар ақаулардың пайда болуы және оларды жою мүмкін бе?

Компьютерлік-желілік сараптаманың үлгілік мәселелері:

1. Бұл компьютерлік құралдың Интернет желісінде жұмыс істеу белгілері бар ма?

2. Интернетке қосылу үшін қандай аппараттық құралдар қолданылды?

3. Интернет желісінің түйінімен теңшелген байланыстар бар ма және олардың қасиеттері қандай (провайдердің телефон нөмірлері, пайдаланушының пар мен парольдері, жасалған күндері)?

4. Желіге қашықтан қол жеткізу бағдарламасының қондырғылары мен қосылу хаттамаларының мазмұны қандай?

5. Осы компьютерлік құралдан қандай Интернет мекенжайларға қол жеткізілді?

6. Электрондық төлемдерді жүргізу және несие картасының кодтарын пайдалану туралы ақпарат бар ма?

7. Электрондық пошта арқылы алынған (сондай-ақ жіберілген) пошта хабарламалары бар ма?

8. Интернет арқылы дербес байланыс бағдарламаларын пайдалану арқылы алынған (жіберілген) хабарламалар бар ма және олардың мазмұны қандай?

Компьютерлік-техникалық сараптаманың құзыретіне мәселелер жатпайды:

– зерттелетін тасымалдағыштарда жазылған бағдарламалар даналарының лицензиялануы/ контрафактілігі (құқықтық бағалауды талап етеді);

– зерттелетін объектілерді пайдалана отырып жүргізілген іс-әрекеттердің заңдылығы (құқықтық бағалауды талап етеді);

– бағдарламаларға арналған компьютерлердің, тасымалдаушылардың, лицензиялардың құны (Бағалау сараптамасы шеңберінде белгіленеді);

– табылған мәтіндерді, бағдарлама интерфейстерін, корреспонденцияларды және т. б. аудару.

Сарапшының қолында бар арнайы білімге негізделген зерттеу нәтижесі сарапшының қорытындысы болып табылады. Егер сарапшы қойылған сұрақтардың бір бөлігіне ғана жауап бере алса, ол осы сұрақтар бойынша қорытындылармен және қалған сұрақтарға жауап бере алмау себептерін негіздей отырып қорытынды дайындайды.

Егер ұсынылған материалдар сот сараптамасын жүргізу үшін жеткіліксіз болса немесе оны жүргізу үшін жеткілікті білімі жоқ деп есептесе, сарапшы сараптама жүргізуге арналған қаулыны орындаусыз қайтаруға құқылы.

Егер сот сараптамасын жүргізу кезінде сарапшы қылмыстық іс үшін маңызы бар, бірақ оған қатысты сұрақтар қойылмаған мән-жайларды анықтаса, онда ол оларды өз қорытындысында көрсетуге құқылы.

Қорытындыларды тұжырымдау кезінде сарапшы объективті және субъективті себептерден туындаған қателіктер жіберуі мүмкін. Сондықтан, кез-келген дәлел сияқты, сарапшының қорытындысы оның салыстырмалылығы, рұқсат етілуі (зерттеу материалдарын алудан бастап барлық кезеңдерде қылмыстық іс жүргізу заңының талаптарына қатаң сәйкестігі) және сенімділігі тұрғысынан бағаланады.

Компьютерлік қылмыстарға қатысты ең үлкен қиындықтар сарапшының қорытындысының дұрыстығын тексеру болып табылады, әсіресе ғылыми негізділік және сараптамалық зерттеу әдістерін қолдануға рұқсат беру бөлігінде. Ақпараттық технологиялардың серпінділігі, жоғары даму жылдамдығы және өзгеруі, бағдарламалық және аппараттық құралдардың алуан түрлілігі бірқатар жағдайларда компьютерлік сараптаманың стандартты, қалыптасқан, сыналған әдістерін әзірлеу мүмкін приводитстігіне әкеледі. Сарапшының қорытындысын бағалау процесінде тергеуші, анықтаушы, сот мынадай шешім қабылдауы тиіс:

– зерттеуге ұсынылған объектілерге рұқсат етіледі;

– сарапшыға ұсынылған бастапқы деректер дұрыс;

– сараптама жүргізу үшін сарапшыға ұсынылған материалдар жеткілікті;

– сарапшы жүргізген зерттеу толық;

– сарапшының қорытындысы дұрыс;

– сарапшының қорытындылары ол жүргізген зерттеулермен расталды;

– сарапшының қорытындысы дұрыс;

– сарапшының қорытындысы дәлелді күшке ие.

Тек осы жағдайда ғана сарапшының қорытындысы қылмыстық іс бойынша дәлел ретінде пайдаланылуы мүмкін.

Қорытындылай келе, компьютерлік сараптама қазіргі цифрлық дәуірде маңызды рөл атқаратынын атап өткім келеді. Оның мақсаты-компьютерлік жүйелер мен электрондық құрылғыларға қатысты дәлелдемелерді анықтау, талдау және жинау. Компьютерлік сараптама қылмыстық сот төрелігі, іскерлік сала, киберқауіпсіздік, ақпаратты қорғау және т. б. сияқты әртүрлі салаларда қажет.

Әр түрлі әдіснамалар мен құралдарға сүйене отырып, компьютерлік сарапшылар сандық дәлелдерге терең талдау жасай алады, жойылған немесе жасырын деректерді қалпына келтіре алады, қылмыстың немесе заңсыз әрекеттің іздерін анықтай алады. Компьютерлік сараптама нәтижелері бойынша жасалған сараптамалық есеп сот процестеріндегі маңызды дәлел болып табылады және құқық пен әділеттілік туралы шешім қабылдауға қызмет етеді.

Компьютерлік сараптаманың негізгі мақсаты заңды сенімділікті қамтамасыз ету және азаматтардың жеке өмірі мен құқықтарын қорғау болып табылады. Компьютерлік сараптама жүргізу компьютерлік технологиялар саласындағы қылмыстарды анықтауға және алдын алуға, сондай-ақ компаниялар мен мекемелердің мүдделерін зиянкестердің қауіп-қатерлерінен қорғауға көмектеседі.

Жалпы, компьютерлік сараптаманың мақсаты цифрлық әлемде құқықтық қорғау мен әділеттілікті қамтамасыз ету болып табылады. Бұл қазіргі заманғы құқықтық жүйенің ажырамас бөлігі және қылмыстармен күресу және азаматтар мен ұйымдардың мүдделерін қорғау үшін өте қажет.

Өзін-өзі бақылау мәселелері:

1. Компьютерлік сараптама дегеніміз не және оның мақсаты қандай?
2. Компьютерлік сараптама жүргізуді талап ететін қылмыстар мен оқиғалардың қандай түрлері бар?
3. Компьютерлік сараптама киберқылмыстарды тергеуге қалай көмектесе алады?
4. Компьютерлік сараптама арқылы қандай ақпаратты алуға болады?
5. Ақпаратты қорғау және деректердің ағып кетуіне жол бермеу үшін компьютерлік сараптаманың рөлі қандай?
6. Деректерді талдау және алу үшін компьютерлік сарапшылар қандай әдістер мен құралдарды пайдаланады?
7. Компьютерлік сараптама жүргізудің негізгі кезеңдері қандай?
8. Компьютерлік сараптама мамандарына қандай дағдылар мен біліктілік қажет?
9. Компьютерлік сараптаманы сот процедураларында қалай қолдануға болады?
10. Компьютерлік сараптама жүргізу кезінде қандай проблемалар мен қиындықтар туындауы мүмкін?

Өзін-өзі бақылауға арналған тест тапсырмалары:

1. Компьютерлік сараптама-бұл:

a) компьютердің жұмысын бағалау;

b) қылмыстық қызметті анықтау мақсатында компьютерлік жүйелер мен деректердің жай-күйін зерттеу;

c) компьютерлерге арналған бағдарламалық қамтамасыз етуді әзірлеу;

d) алгоритмдер мен деректер құрылымдарын зерттеу және талдау;

e) Компьютердің техникалық сипаттамаларын анықтау.

2. Компьютерлік сараптама нені қамтиды?

a) компьютердің жұмысын тексеру;

b) жойылған деректерді іздеу және шығару;

c) бағдарлама кодын талдау;

d) операциялық жүйенің түрін анықтау;

e) антивирустық бағдарламалық жасақтаманы орнату.

3. Компьютерлік сараптама сарапшысына қандай техникалық дағдылар қажет?

a) бағдарламалау тілдерін білу;

b) компьютерлік желілердің жұмыс принциптерін түсіну;

c) мәліметтер базасымен жұмыс істей білу;

d) құпия сөзді бұзу тәжірибесі;

e) кескінді өңдеу дағдылары.

4. Компьютерлік сараптаманы қандай құралдармен жүргізуге болады?

a) файлдық жүйені талдауға арналған бағдарламалар;

b) жойылған деректерді қалпына келтіру құралдары;

c) желілік сканерлер және трафик анализаторлары;

d) сот-медициналық бағдарламалық қамтамасыз ету;

e) мәтіндік құжаттарды құруға және өңдеуге арналған қосымшалар.

5. Бизнес саласындағы компьютерлік сараптаманың мақсаты:

a) компьютерлік желінің ақауларының себептерін анықтау;

b) деректерге рұқсатсыз қол жеткізу фактілерін анықтау;

c) бағдарламалық жасақтаманы пайдалану тиімділігін талдау;

d) құпия ақпараттың ағып кету себептерін анықтау;

e) жаңа бағдарламалық өнімдерді әзірлеу.

6. Компьютерлік сараптаманың қандай түрлері бар?

a) сот-компьютерлік сараптама;

b) медициналық компьютерлік сараптама;

c) қаржылық компьютерлік сараптама;

d) архитектуралық компьютерлік сараптама;

e) психологиялық компьютерлік сараптама.

7. Компьютерлік сараптама бойынша сарапшы қандай принциптерді ұстануы керек?

a) тәуелсіздік және объективтілік;

b) құпиялылық және құпиялылық;

c) заңнаманы толық білу;

d) командада жұмыс істеу қабілеті;

e) жоғары білім мен құзыреттілік.

8. Компьютерлік сараптама процесінің негізгі кезеңдері қандай?

a) деректерді жинау және талдау;

b) жойылған файлдарды қалпына келтіру;

c) бағдарламалық қамтамасыз етуді әзірлеу;

d) желілік трафикті бақылау;

e) табылған фактілерді анықтау және құжаттау.

9. Компьютерлік сараптаманың негізгі міндеті неде?

а) жойылған файлдарды қалпына келтіру;

б) компьютердің жұмысын жақсарту;

в) компьютерлік қылмыстарға байланысты дәлелдемелерді талдау және жинау;

г) жаңа бағдарламалық өнімдерді әзірлеу;

д) жасанды интеллект алгоритмдерін әзірлеу.

10. Компьютерлік сараптаманың қандай аспектілері желілік қауіпсіздік саласына жатады?

а) бағдарламалық жасақтаманың әртүрлі түрлерін зерттеу;

б) жүйенің желі бойынша тәуекелдер мен қауіптерге дайындығын айқындау;

в) компьютердің аппараттық бөлігін зерттеу;

г) жаңа операциялық жүйелерді әзірлеу;

д) желілік протоколдарды талдау және осалдықтарды іздеу.

§7. Ақпараттық қауіпсіздік инциденттерін анықтау құралдары

Ақпараттық қауіпсіздік біздің заманымыздағы ұйымдардың маңызды міндеттерінің біріне айналды. Интернет-технологиялар мен бизнес-процестерді цифрландырудың өсуімен инциденттердің осалдығы мен пайда болу қаупі артты. Нәтижесінде ақпараттық қауіпсіздік инциденттерін анықтаудың тиімді құралдарын әзірлеу және қолдану басым бағытқа айналды.

Ақпараттық қауіпсіздік оқиғасы-ақпараттық жүйелерге, ресурстарға немесе деректерге зиян келтіруі мүмкін кез келген қажетсіз, күтпеген немесе күтпеген оқиға. Оқиғалар деректердің құпиялылығын, тұтастығын немесе қолжетімділігін бұзуы мүмкін және ұйымның беделіне теріс әсер етуі мүмкін.

Инциденттерді анықтау құралдары ақпараттық жүйелердің қауіпсіздігін қамтамасыз етуде шешуші рөл атқарады. Олар рұқсатсыз кіруді, ішкі және сыртқы қауіптерді анықтауға және оларды жүзеге асырмас бұрын ықтимал оқиғалардың алдын алуға көмектеседі. Анықтау құралдарының арқасында ұйым туындаған қауіптерге жедел әрекет ете алады және ықтимал шығындарды азайтады.

Ақпараттық қауіпсіздік инциденттерін анықтау құралдарының негізгі түрлері:

a) бақылау және тіркеу жүйелері-желідегі белсенділікті бақылауға, оқиғалар журналдарын талдауға және ауытқуларды анықтауға мүмкіндік береді;

b) интражурналды анықтау жүйелері-рұқсатсыз кіру немесе ішкі шабуылдар сияқты ішкі қауіптерді анықтауға арналған;

c) интрузияны анықтау жүйелері-сыртқы шабуылдаушылардың желіге немесе ақпараттық жүйеге ену әрекеттерін анықтайды;

d) аналитикалық құралдар-ауытқуларды немесе күдікті әрекеттерді анықтау үшін деректерді өңдеу және талдау үшін қолданылады;

e) инцидентті басқару жүйелері-анықталған инциденттерге жауап беру процесін тиімді басқаруға, олардың шешілуін бақылауға және қайталанған жағдайлардың алдын алуға мүмкіндік береді.

Ақпараттық қауіпсіздік инциденттерін анықтау құралдары ұйымның ақпараттық жүйелері мен деректерін қорғау үшін өте маңызды. Олар қауіптерді тез анықтауға және оларға жауап беруге, сондай-ақ ықтимал оқиғалардың алдын алуға көмектеседі. Инциденттерді анықтау құралдарын дұрыс таңдау және дұрыс пайдалану ақпараттық қауіпсіздік стратегиясының ажырамас бөлігі болып табылады.

Ықтимал оқиғаларды дәл анықтау өте қиын болуы мүмкін:

– оқиғаларды әртүрлі тәсілдермен, егжей-тегжейлі және дәлдік деңгейлерімен анықтауға болады, сонымен қатар автоматтандырылған анықтау жүйелерінің жалған позитивтері болуы мүмкін;

– кейбір оқиғаларда оңай анықталатын айқын белгілер бар (мысалы, веб-парақтың дефейсі), ал басқа да көптеген оқиғаларды анықтау мүмкін емес, өйткені оларда мұндай айқын белгілер жоқ;

– АҚ оқиғаларының белгілері болуы мүмкін АҚ оқиғаларының көлемі, әдетте, өте үлкен, мысалы, ұйым күніне мыңдаған, тіпті миллиондаған интрузияны анықтау датчиктерінен ескертулер ала алады, бірақ олардың барлығы бірдей болған АҚ оқиғаларын көрсете алмайды (мысалы, сервердің істен шығуы немесе маңызды файлдардың өзгеруі мүмкін). АҚ оқиғасынан басқа себептерге, соның ішінде адамның қателігіне);

– оқиғалар тобын АҚ оқиғасы ретінде дұрыс анықтау үшін терең арнайы техникалық білім мен мол тәжірибе қажет болуы мүмкін, оқиға туралы ақпаратты әртүрлі жүйелерден (брандмауэр, IDPS Және қолданбалар) алуға және бірнеше түрлі журналдарда жазуға болады, олардың әрқайсысы оқиға туралы деректердің белгілі бір бөлігін көрсете алады (мысалы, брандмауэр журналында сұрау көзінің IP мекенжайы болуы мүмкін, ал қолданба журналында пайдаланушы аты болуы мүмкін).

Осылайша, қауіпсіздік оқиғаларын бағалау және оқиғаны анықтау кезінде не болғанын анықтау үшін екіұшты, қарама-қайшы және толық емес белгілерден бастау керек.

АҚ инциденттерінің белгілерін анықтаудың техникалық құралдары деңгейлерде жұмыс істейді:

– желілік және хост периметрі (брандмауэрлер, маршрутизаторлар, IDS кіруді анықтау жүйелері);

– хост (антивирустық қорғаныс құралдары, файлдардың тұтастығын бақылау бағдарламалары, іске қосуды басқару);

– қолданбалар (қолданба журналдары);

– қолданбалар (қолданба журналдары).

Брандмауэрлер кіріс желілік трафикті сүзеді, Протокол стегінің әртүрлі деңгейлерінде әрекет ете алады және желілік шабуылдарды анықтауға және бұғаттауға қабілетті. Байланыстарды бақылау маршрутизаторда жүзеге асырылуы мүмкін, бұл арна деңгейіндегі шабуылдарды тойтаруға мүмкіндік береді. Хост периметрі деңгейінде жеке брандмауэр жұмыс істейді, атап айтқанда, Windows операциялық жүйелеріне (ОЖ) ұқсас бағдарламалық жасақтама орнатылған, сонымен қатар үшінші тарап шешімдері орнатылуы мүмкін (мысалы, Comodo Firewall, Outpost Firewall, Trend Micro Internet Security, Avast Internet Security және т.б.). Хост деңгейіндегі брандмауэрлер көптеген серверлік ОЖ (Linux, Windows, BSD, Mac OS X Server) бөлігі ретінде қол жетімді.

Интрузияны анықтау/ алдын алу жүйелері (IDS/IPS, Intrusion Detection/ Prevention System) күдікті оқиғаларды анықтайды және олар туралы тиісті деректерді, соның ішінде шабуылды анықтау уақытын, шабуыл түрін, бастапқы және тағайындалған IP мекенжайларын және пайдаланушы атын (бар болса және белгілі болса)жазады. Желілік (NIDS, network based IDS), хост (HIDS, host based IDS) және таратылған (dids, distributed ids) арасында айырмашылық бар. Соңғысы ақпаратты АЖ түйіндеріне орнатылған бірнеше датчиктерден (бағдарламалық жасақтама немесе аппараттық құрал) алады. Әдетте, қолтаңбаны талдаумен қатар, IDS проактивті бақылауды жүзеге асыра отырып, аномалиялық талдауды қолданады.

Қазіргі заманғы антивирустық құралдар зиянды және қажетсіз бағдарламалардың әртүрлі түрлерін анықтауға, сондай-ақ қолтаңба, мінез-құлық және эвристикалық талдау әдістерін қолдану арқылы бағдарламалардың күдікті белсенділігін анықтауға мүмкіндік береді. IDS сияқты, антивирустық жүйелер жалған позитивтерге жол береді немесе жаңа немесе ерекше шабуыл таба алмауы мүмкін.

Көптеген шабуыл сценарийлері жүйелік файлдарға немесе Бағдарламалық жасақтамаға өзгертулер енгізуді немесе өзгертуді, іске қосуға рұқсат етілмеген компоненттерді қосуды қамтиды. Файлдардың тұтастығын бақылау бағдарламалары оқиғалар кезінде маңызды файлдарға енгізілген өзгерістерді анықтай алады. Тексеру құралдарының жұмысы әрбір тағайындалған файл үшін бақылау сомасын (әдетте хэш функциясының мәні) есептеуге негізделген. Егер бақылау сомасын қайта есептеу кезінде оның мәні алдыңғыдан өзгеше болса, онда файл өзгертілді. Windows жүйелік компоненттерінің тұтастығын тексеру және оларды қалпына келтіру кіріктірілген SFC утилитасы арқылы жүзеге асырылуы мүмкін. Windows ОЖ іске қосу компоненттерін тізілімде теңшеуге болады, сондықтан sysinternals Suite жиынтығынан autoruns сияқты арнайы утилиталарды пайдалану мағынасы бар.

Ішкі бұзушылар мен қауіптерді бақылау үшін ақпараттың ағып кетуінен қорғау жүйелері (DLP, data Leak Prevention) пайдаланылады, бұл ретте ағып кетуден қорғауды қажет ететін ақпаратты табу және санаттарға бөлу қолданбалы деңгейде (хабарламалар/ құжаттар мазмұны) жүргізіледі. Пайдаланушының әрекеттерін бақылау және бақылау хостта да, желілік шлюзде де жүзеге асырылуы мүмкін. Жүйелердің DLP талдау деректерін пайдалану белгілі бір заңды тіркеуді қажет етеді, себебі ол қызметкерлердің жеке ақпаратына әсер етуі мүмкін.

Брандмауэрлер мен маршрутизаторлар сияқты желілік құрылғылардың журналдары әдетте оқиғалар туралы ақпараттың негізгі көзі болып табылмайды. Бұл құрылғылар әдетте рұқсат етілмеген қосылымдар мен кіріс трафигін блоктау үшін конфигурацияланғанымен, олар "шикі" деректер деңгейінде (raw data) жұмыс істейді және рұқсат етілмеген әрекеттің сипаты туралы аз ақпарат береді. Дегенмен, мұндай деректер басқа техникалық құралдармен анықталған оқиғаларды салыстыру кезінде құнды болуы мүмкін.

АҚ инциденциясын талдау үшін ОЖ, қызметтер мен қосымшалардың журналдары үлкен маңызға ие, олар, мысалы, қандай есептік жазбаларға қол жеткізілгені және қандай әрекеттер жасалғаны туралы ақпаратты қамтуы мүмкін. Оқиғаларды журналдау және аудит саясаты АҚ инциденттерін басқару циклінің дайындық кезеңінде енгізілуі және конфигурациялануы керек. Көптеген ОЖ аутентификация әрекеттері және қауіпсіздік саясатын өзгерту сияқты оқиғалардың белгілі бір түрлерін тексеруге және жазуға конфигурациялануы мүмкін. Аудиторлық жазбалар құнды ақпарат бере алады, соның ішінде оқиға болған уақыт және оның шығу тегі (көзі).

Журнал файлдарында жасалған деректердің үлкен көлемі оларды өңдеуді, сақтауды және оқиғаларды анықтау үшін құнды ақпаратты алуды

қиындатады. Splunk және SUMO Logic сияқты үлкен деректерді, машиналық деректерді талдау және журналды басқару шешімдері, сондай-ақ деректерді біріктіруге және әртүрлі іздеу түрлерін біріктіруге мүмкіндік беретін Elasticsearch ашық бастапқы құралы бар.

Көбінесе журнал деректері оқиғаның мәнмәтіні туралы қосымша ақпарат алу үшін реактивті түрде қолданылады (яғни оқиғадан кейін). Осыны ескере отырып, журнал файлдарының қорғалуы және оларды жасаған жүйеден бөлек жүйеде сақталуы өте маңызды.

Егер АЖ өмірлік цикліне келесі іс-шаралар алдын ала енгізілсе, көптеген оқиғаларды тиімдірек және тиімдірек өңдеуге болады:

– жүйелердің тұрақты сақтық көшірмесін жасау және белгілі бір уақыт аралығында алдыңғы сақтық көшірмелерді сақтау;

– жұмыс станцияларында, серверлерде және желілік құрылғыларда аудитті қосу;

– орталықтандырылған журнал серверлерін қорғау үшін аудит жазбаларын қайта жіберу;

– барлық аутентификация әрекеттерін жазуды қоса, аудитті орындау үшін маңызды қолданбаларды орнату;

– жалпы ОЖ және қосымшалар файлдары үшін хэш мәндерінің дерекқорын жүргізу және ерекше маңызды ресурстардағы файлдардың тұтастығын бақылау;

– желі және жүйе конфигурациясының жазбаларын (мысалы, негізгі көрсеткіштер) жүргізу;

– жүйе мен желілік белсенділікке Тарихи тексерулер жүргізуді қолдайтын деректерді сақтау саясатын құру.

Белгілі бір оқиғаның орын алғанын бағалау үшін әртүрлі көздерде көрсетілген қауіпсіздік оқиғаларының корреляциясын анықтау қажет. Мысалы, NIDS белгілі бір хостқа қарсы шабуылдың басталуын анықтай алады, бірақ шабуылдың сәтті болғанын анықтау үшін аталған хосттың журналдарын зерттеу қажет болуы мүмкін.

АҚ инциденттерін анықтауды автоматтандырудың ең үлкен дәрежесін қамтамасыз ететін Siem жүйелері (Security Information and Event Management) қамтамасыз етеді:

– деректерді әртүрлі көздерден (желілік құрылғылар, қосымшалар, ОЖ, брандмауэр, IDS, антивирустық құралдар, DLP)шоғырландыру және сүзу;

– оқиғалар журналдарын бірыңғай форматта орталықтандырылған сақтау және оқиғаларды жетіспейтін ақпаратпен байыту;

– оқиғалардың корреляциясын анықтау (қатынастар мен заңдылықтарды іздеу) және оларды ережелер бойынша өңдеу, бұл ауытқуларды, ықтимал қауіптерді, АТ инфрақұрылымының бұзылуын, рұқсатсыз кіру әрекеттерін, сыртқы шабуылдарды жоғары ықтималдықпен анықтауға мүмкіндік береді;

– АҚ инциденттері туралы автоматты түрде хабарлау, инциденттер дерекқорын жүргізу және есептер шығару;

– оқиғаларды талдау және оқиғаларды талдау құралдарын ұсыну;

– сотта дәлел бола алатын құжатталған куәліктерді ұсыну.

SIEM тіркелген қауіпсіздік оқиғаларының массасынан нақты орын алған қауіпсіздік оқиғаларын анықтауға және тек маңызды және шынымен маңызды қауіптерге назар аударуға мүмкіндік береді. Дегенмен, бұл жүйелер өте қымбат және орнату қиын, орналастыру үшін де, одан әрі қолдау үшін де жоғары білікті қызметкерлерді қажет етеді.

Техникалық жүйелер жасаған мәліметтер ең жақсы дәлелдер болып табылады. Бұл «бірінші саты» деп аталатын дәлелдер, олар зерттеушінің қатысуынсыз жасалады (пайда болады). Қол жеткізуді бақылау жүйесінің Аудит журналы, ОЖ жүйелік журналдары, IDS журналдары, SIEM жүйелері және т. б. мысалдар болып табылады, олар бұл жағдайда электрондық құжаттар болып саналады.

Қауіпсіздік оқиғаларын анықтаудың техникалық құралдары өте тиімді, бірақ басқа ақпарат көздерін, мысалы, пайдаланушылардың немесе техникалық қызметкерлердің сәтсіздіктер немесе оқиғалардың басқа белгілері туралы хабарламаларын есте сақтау қажет. Оқиғаны дұрыс анықтау және түсіну үшін жаңа осалдықтарды, эксплуатацияларды және компаға келу көрсеткіштерін (инциденттердің белгілерін)қадағалау маңызды рөл атқарады. Бұл ақпарат CERT топтары мен Threat Intelligence компаниялары (feeds – жаңалықтар арналары), серіктестер мен аппараттық және бағдарламалық қамтамасыз ету провайдерлері туралы ақпарат, басқа оқиғаларға жауап беру топтарының тәжірибесі сияқты ашық көздерде қол жетімді болуы мүмкін. Ақпарат көзі ақылы жазылымдар мен Threat Intelligence қызметтері болуы мүмкін.

Threat Intelligence жедел деректері жаңа қауіп векторларының, «шабуыл тізбектерінің» (kill chain) пайда болуын, ақпараттық процестерді бұзу тәсілдерін және зиянкестердің құралдары мен тактикасындағы басқа да өзгерістерді бақылау арқылы оқиғаларға алдын ала дайындалуға мүмкіндік береді.

Өзін-өзі бақылау мәселелері:

1. Ақпараттық қауіпсіздік оқиғаларын анықтаудың негізгі құралдары қандай?
2. Ақпараттық қауіпсіздік инциденттерін анықтау құралдары қандай функцияларды орындайды?
3. Қауіпсіздік құралдары қандай қауіптер мен шабуылдарды анықтай алады?
4. Ақпараттық қауіпсіздік оқиғаларын анықтау үшін қандай әдістер мен алгоритмдер қолданылады?
5. Салыстыру және таңдау үшін анықтау құралының қандай сипаттамаларын қолдануға болады?
6. Ақпараттық қауіпсіздік оқиғаларын анықтаудың әрбір құралы қандай артықшылықтар мен кемшіліктерге ие болуы мүмкін?
7. Ақпараттық қауіпсіздікті анықтау құралдарының тиімділігіне қандай факторлар әсер етуі мүмкін?
8. Ақпараттық қауіпсіздік оқиғаларын анықтаудың тиімді жүйесін құруға қандай тәжірибелер мен стратегиялар көмектесе алады?
9. Ақпараттық қауіпсіздік инциденттерін анықтау құралын таңдау кезінде қандай талаптар ескерілуі керек?
10. Ұйымның ақпараттық жүйелерінің қауіпсіздігін қамтамасыз етуде ақпараттық қауіпсіздікті анықтау құралдарының рөлі қандай?

Өзін-өзі бақылауға арналған тест тапсырмалары:

1. Ақпараттық қауіпсіздік инциденттерін анықтау құралының (SOIB) қандай түрі инициализацияны алдын ала орнатуды қажет етпейді?

a) интрузивті анықтау жүйесі (IDS);
b) интрузиялық алдын алу жүйесі (IPS);
c) деректердің бұзылуын анықтау жүйесі (DLP);
d)антивирустық бағдарламалық жасақтама (APO);
e) оқиғаларды басқару және ақпараттық қауіпсіздік жүйесі (SIEM).

2. Желілік ресурстарға рұқсатсыз қол жеткізу әрекетін қандай ақпараттық қауіпсіздік инциденттерін анықтау құралы (SOIB) анықтай алады?

a) интрузивті анықтау жүйесі (IDS);
b) интрузиялық алдын алу жүйесі (IPS);
c) деректердің бұзылуын анықтау жүйесі (DLP);
d) антивирустық бағдарламалық жасақтама (APO);
e) оқиғаларды басқару және ақпараттық қауіпсіздік жүйесі (SIEM).

3. Төмендегілердің қайсысы SOIB бағдарлама кодының осалдығына негізделген қолданбаларға шабуылдарды анықтай алады және алдын алады?

a) Интрузивті анықтау жүйесі (IDS);
b) интрузиялық алдын алу жүйесі (IPS);
c) деректердің бұзылуын анықтау жүйесі (DLP);
d) антивирустық бағдарламалық жасақтама (APO);
e) анықтау және алдын алу Веб-қосымшалары (WAF).

4. Белгісіз қауіптерді іздеу және әдеттен тыс әрекеттерді анықтау үшін қандай SOIB технологиясы кеңінен қолданылады?

a) мінез-құлықты талдау;
b) қолтаңбаны талдау;
c) статистикалық талдау;
d) хэштеу;
e) шифрлау.

5. Құпия деректердің желі арқылы ағып кетуін анықтау және болдырмау үшін төмендегілердің қайсысы қолданылады?

a) интрузивті анықтау жүйесі (IDS);
b) интрузиялық алдын алу жүйесі (IPS);
c) деректердің бұзылуын анықтау жүйесі (DLP);
d) антивирустық бағдарламалық жасақтама (APO);
e) оқиғаларды басқару және ақпараттық қауіпсіздік жүйесі (SIEM).

6. Қауіпсіздік оқиғаларын бақылау және талдау үшін СОИБ қандай технологияны қолданады?

a) интрузивті анықтау жүйесі (IDS);
b) интрузиялық алдын алу жүйесі (IPS);
c) деректердің бұзылуын анықтау жүйесі (DLP);
d) антивирустық бағдарламалық жасақтама (APO);

e) оқиғаларды басқару және ақпараттық қауіпсіздік жүйесі (SIEM).

7. Ақпараттық қауіпсіздік инциденттерін анықтаудың аталған құралдарының қайсысы бағдарламалық жасақтама болып табылады?

a) биометриялық саусақ ізі сканері;

b) қауіпсіздік мониторингінің интеграцияланған жүйесі;

c) сервер бөлмесіндегі физикалық құлып;

d) брендтелген USB флэш-дискісі;

e) желілік трафикке арналған шифрлау құрылғысы.

8. Төменде келтірілген ақпараттық қауіпсіздік инциденттерін анықтау құралдарының қайсысы зиянды бағдарламалық жасақтаманы қолдана отырып шабуылды анықтауда тиімді?

a) интрузияны анықтау құрылғысы;

b) брандмауэр;

c) антивирустық бағдарламалық қамтамасыз ету;

d) желілік трафиктегі ауытқуларды анықтау жүйесі;

e) қауіпсіздік журналдарын талдау әдістері.

9. Ақпараттық қауіпсіздік инциденттерін анықтаудың қайсысы желілік трафиктегі ауытқуларға жауап беру әдісін қолданады?

a) интрузияны анықтау жүйесі;

b) физикалық биометриялық сканер;

c) желілік трафикке арналған шифрлау құрылғысы;

d) қауіпсіздікті бақылаудың интеграцияланған жүйесі;

e) антивирустық бағдарламалық жасақтама.

10. Ақпараттық қауіпсіздік инциденттерін анықтаудың төменде келтірілген құралдарының қайсысында ақпараттық жүйелерге шабуылдардың алдын алу және жолын кесудің қосымша функциясы бар?

a) брандмауэр;

b) интрузияны анықтау құрылғысы;

c) bitcoin әмиян;

d) желілік трафиктегі ауытқуларды анықтау жүйесі;

e) антивирустық бағдарламалық жасақтама.

ҚОРЫТЫНДЫ

Ақпараттық қауіпсіздік қазіргі цифрлық әлемнің негізгі аспектілерінің бірі болып табылады. Ақпараттық қауіпсіздік оқиғаларын тергеу деректерді қорғауды қамтамасыз етуде және ықтимал қауіптердің алдын алуда маңызды рөл атқарады.

Ақпараттық қауіпсіздік оқиғалары ұйымдар мен жеке адамдар үшін ауыр зардаптарға әкелуі мүмкін. Мұндай оқиғалар құпия ақпараттың ағып кетуіне, деректердің жойылуына немесе тіпті жүйенің дұрыс жұмыс істемеуіне әкелуі мүмкін. Зерттеу нәтижелері мұндай оқиғаларды тиімді тергеу үшін шаралар қабылдау қажеттілігін растайды.

Негізгі проблемалардың бірі-ақпараттық қауіпсіздік инциденттерін тергеу саласындағы білікті мамандардың жетіспеушілігі. Осыған байланысты мамандандырылған бағдарламалар мен білім беру курстарын әзірлеу және қолдау қажетті міндетке айналуда. Сондай-ақ, ақпараттық қауіпсіздік инциденттерін тергеуге көмектесетін жаңа әдістер мен құралдарды әзірлеу және енгізу қажет.

Ұйымдар арасындағы ынтымақтастық пен ақпарат алмасу ақпараттық қауіпсіздік оқиғаларын сәтті тергеудің ажырамас бөлігі болып табылатындығын атап өту маңызды. Әр түрлі құрылымдардың өзара әрекеттесуі және тәжірибе алмасу арқылы ғана қауіптің жаңа түрлерімен тиімді күресуге және олардың болашақта пайда болуына жол бермеуге болады.

Зерттеу нәтижелеріне сүйене отырып, ақпараттық қауіпсіздік инциденттерін тергеуді жетілдіру және дамыту қажет деген қорытынды жасауға болады. Ол үшін мамандардың біліктілігін арттыру, жаңа әдістемелер мен құралдарды әзірлеу, сондай-ақ ұйымдар арасындағы ынтымақтастыққа жәрдемдесу қажет. Тек осылай ғана ақпараттың сенімді қорғалуын қамтамасыз етуге және ықтимал қауіптердің алдын алуға болады.

ШУЛЬГИН *ЕВГЕНИЙ ПЕТРОВИЧ,*
САПАРҒАЛИЕВ *ЖАНДОС НУРБЕКОВИЧ,*
ДОСЫМБЕТОВ *ЕСЕН ОРАЗБЕКОВИЧ,*
ТАФИНЦЕВ *ПАВЕЛ АНАТОЛЬЕВИЧ*

АҚПАРАТТЫҚ ҚАУІПСІЗДІККЕ ӘРЕКЕТ ЕТУДІ ҰЙЫМДАСТЫРУ

ОҚУ ҚҰРАЛЫ

Басуға қол қойылды 21.07.2023 ж. Пішімі 60х90/16
Есептік баспа табағы 4,1. Таралымы 50 дана. Тапсырыс 73.
«Гласир» ЖШС баспаханасы. Қарағанды, Ермеков к., 112/5.