Базилова А.А.

Компьютерлік қылмыстардың алдын алу шаралары

Автор мақалада компьютерлік қылмыстарды жасауға ықпал еткен негізгі себептерді қарастырады. Және олардың алдын алу шаралары мен әдістерін айқындай түскен. Сонымен қатар мақалада автор шет мемлекеттердің компьютерлік қылмыстардың алдын алу шараларын салыстырған. Сонымен қатар алдын алу шараларының тиімді жолдарына тоқталған.

Түйін сөздер: компьютер, антивирус, қылмыс, компьютерлік техника.

Bazilova A.A.

Prevention computing crime

The author of this article examines the main reasons for committing computer crimes. In addition, the way these crime prevention. Also, computer-crime prevention measures. In addition, the author of this article examined the experience of foreign countries for the prevention of computer crime. In addition, they were examined the most appropriate ways to prevent crime.

Key words: Computer antivirus, crime, computer equipment.

Базилова А.А.

Профилактика компьютерных преступлений

В данной статье рассматриваются основные причины совершения компьютерных преступлений и пути профилактики данных преступлений. Также меры предупреждения компьтерных преступлений. Автором был проанализирован опыт зарубежных стран по предупреждению компьютерных преступлений и были предложены наиболее оптимальные пути профилактики преступлений.

Ключевые слова: Компьютер, антивирус, преступления, компьютерная техника.

ӘОЖ 10.77.51

Базилова А.А.

Әл-Фараби атындағы Қазақ ұлттық университеті,
Қазақстан Республикасы, Алматы қ.
E-mail: bazilovaa@mail.ru

КОМПЬЮТЕРЛІК ҚЫЛМЫСТАРДЫҢ АЛДЫН АЛУ ШАРАЛАРЫ

Әлемдік тәжірибе көрсеткендей, осы мәселелерді шешу үшін құқыққорғау органдары түрлі алдын алу шараларын қолдануы тиіс. Бұл жағдайда алдын алу шараларын қылмысты ашуға, олардың тудыру себебін жою, қылмысты жасауға ықпал ететін жағдайларды анықтауға бағытталған қызмет деп түсіну керек. Біздің еліміз де компьютерлік қылмыстардың алдын алу әдістері мен құралдарын әзірлеумен криминалистика ғылымы айналысады. Қылмыстарды жасау және оларды ашу кезіндегі қылмыстық-релеванттық ақпараттар және осыларға негізделген қылмыстарды ашу, тексеру және алдын алу әдістерінің заңды қозғалысы туралы ғылым. Анықтамадан көрініп тұрғандай, қылмысты ескерту криминалистика әдістемесінің ең маңызды құрамдас бөлігі болып табылады.

– Құқық қорғау объектісі ретінде ақпараттық технологиялардың негізгі компоненттерінің заңды анықтамасын береді.

– Осы объектілерге меншік иесінің құқықтары мен міндеттерін орнықтырады және бекітеді.

– Ақпараттық технологиялар құралдарының қызметінің құқықтық режимін анықтайды.

– Нақты субъектілердің ақпараттық нақты бір түріне қол жету категорияларын анықтайды.

– Мәліметтер мен ақпараттардың құпиялылық категориясын орнықтырады.

– «Құпия ақпарат» терминін анықтау және оның жағынан қолдану шегарасын береді.

Осындай заңдар батыс елдерінде 20 жылдан аса уақыт бар. Бұл заңнаманың осы сала бойынша шешуші аккорды деп компьютерлік қылмысқа қылмыстық жауапкершілікті орнықтыратын 1996 жылы тамызында қабылданған РФ қылмыстық кодексін санауға болады. Мұндағы ақпарат-қылмыстық істер – құқықтық органдар нысаны. Компьютерлік қылмыстарды ескертудің ұйымдастыру-техникалық шаралары. Батыс елдеріне қолданылатын шаралар мәліметін қарастырамын. Менің көзқарасым бойынша, дамыған шетелдерде қолданылатын компьютерлік қылмыстарды ескертудің ұйымдастыру-техникалық шараларының ішіндегі дұрыстарын жекелей қарастырамын.

Қазіргі кезде компьютерлік қылмысты ескерту шараларының 3 негізгі тобын көрсете отырып, бірден мағынасын да

аша кетемін. Компьютерлік қылмысты ескертудің бұл тобына бәрінен бұрын компьютерлік саладағы заңға қарсы әрекеттерге қылмыстық жауапкершілік орнықтыратын заң нормалары жатады. Егер тарихқа жүгінсек, осындай типті бірінші нормативтік-құқықтық акт американ штаттары Флорида мен Аризонда 1978 жылы қабылданғанын көреміз. Бұл заң «Computer crime act of 1978» деп аталды. Сонан кейін Американың барлық штаттарында осындай заң қабылданды. Бұл құқықтық актар заңның ары қарай компьютерлік қылмысты ескерту шараларын жүзеге асырудағы түбегейлі негізі болды.

Біздің көршілес мемлекетіміз – Ресейге келсек, онда бұл бағыттағы алғашқы қадам деп «ЭЕМ және мәліметтер базасы программасын құқықтық қорғау туралы» 1992 жылдың 23 қыркүйегінде қабылданған Федералдық заңын санауға болады. Осындай заң шетелде 5-10 жыл бұрын қабылданған. 20 және 25 қаңтар күні 1995 ж. Федералды жиналыс 2 заңды сәйкес қабылдады: «байланыс туралы» және «Ақпараттар туралы ақпараттарды информатикалау және қорғау туралы». Бұл құқықтық акт бұл бағыттағы алға басу қадамы болды, олар:

Бұл елдердегі компьютерлік қылмыстардың алдын алуға жетекшілік жасау қазір келесі бағыттар бойынша:

1) басқару процедураларының компьютерлік қауіпсіздік талабына сай келуі;

2) компьютерлік залдар мен компьютерлік жабдықтарды техникалық қорғау мәселелерін әзірлеу;

3) мәліметтерді өңдеу стандарттары компьютерлік қауіпсіздік стандарттарын әзірлеу;

Компьютерлік қауіпсіздік стандарттарын қамтамасыз ету мақсатында кадр саясатын жүзеге асыру. Мысалы, АҚШ ұлттық стандарттар бюросы компьютерлік желілерге қойылатын базалық қауіпсіздік талабын әзірледі. Оның ішінде:

– жарамдылық-санкцияланған қол жеткізуді қамтамасыз ету үшін желі жарамды екендігіне кепілдік береді;

– бақыланатын қол жеткізу – желі тек санкциясы бар міндеттерді шешу үшін санкциясы бар пайдаланушыға қол жеткізуді қамтамасыз ететініне кепілдік береді;

– қорғалғандық-санкцияланбаған өзгерістер мен жоюдан мәліметтерді сақтау;

– құпиялылық-санкцияланбаған ашудан мәліметтерді сақтау;

– идентификациясын, берілген мәліметтер сапасы, мәліметтердің берілу уақыты мен ұзақтығы қамтамасыз етілетіне кепілдік береді.

Осы берілген талаптардың негізінде төмендегі критерийлердің жауап беретін сәйкес техникалық бақылау механизмдері жасалды:

1) тұтастық-механизм дұрыс жұмыс істеуіне кепілдік беретін базалық сенімділік;

2) тексеру мүмкіндігі – компьютерлік техника құралдарына қол сұғу және жүйелердің қауіпсіздігі мәселесіне қатысты басқа да жағдайлары әрекеттерін ашу және тексеру ісінде маңызы бар ақпараттарды жазу мүмкіндігі.

Осы шараларды іс жүзіне асыру нәтижесінде төмендегілерге мүмкіндік ашылды:

– компьютерлік техника құралдарына (КТҚ) физикалық қол жеткізуді бақылау;

– аппараттық КТҚ электрлік магниттік сәулеленуін бақылау;

– КТҚ-ға мүмкін болатын қауіпті бақылап, әрбір әрекет-талпыныстарды жазып алу (мониторинг әдісімен).

Жоғарыда келтірілгендерге қарай отырып, шетелде ақпаратты қорғаудың мақсаттары мен негізгі ережелері ресейліктердің базалық позициясының қатарына сәйкес келеді:

а) ақпараттың шығып кетуі, ұрлануы, жоғалуы, бүлінуі және өзгертілуін болдырмау;

б) жеке тұлғаға, қоғам мен мемлекетке түсер қауіпті болдырмау;

в) ақпаратты санкциясыз жою, модификациялау, бұлдіру, көшіру, блоктау әрекеттерін болдырмау, ақпараттық ресурстар мен жүйелерге заңсыз килігудің басқа да қалыптарын болдырмау;

г) құжатталған ақпараттардың меншік нысаны ретіндегі қызметінің құқықтық режимін қамтамасыз ету;

д) мемлекеттік құпияны және құжатталған ақпарат құпиялылығын сақтау;

е) ақпараттық процестер мен оларды әзірлеу кезінде ақпараттық жүйені өндіру мен қолдануда, ақпараттық технология және соларды қамтамасыз ету құралдарын қолдануда субьектінің құқығын қамтамасыз ету.

Отандық қылмыстық істердің материалдарын талдау ісі компьютерлік қылмыстарды жасауға ықпал еткен негізгі себептер мен жағдайлар көп ретте былай болғанын көрсетеді:

1) қаржы операцияларын жүзеге асыру процесінде бастапқы бухгалтерлік құжаттардың қашықтықтан беруі үшін автоматтандырылған желілерді автономды немесе жұмысшы

стансасы сапасында қолданатын компьютерді басқару (клавиатура) пультіне қызметкерлердің бақылаусыз қол жеткізуі;

2) қызмет көрсетуші персонал әрекетін бақыламау, ол қылмыскердің 1 п. көрсетілгендей қылмыс жасау құралы ретінде ЭЕМ-ді еркін қолданушы мүмкіндік береді;

3) кіргізілетін ақпараттың сәйкестігі мен дұрыстығын тексеруді қамтамасыз ететін, бақылаушы қорғанысы жоқ программалық қамтамасыз етудің төменгі деңгейі;

4) пайдаланушының дұрыс идентификациясының жеке биометрикалық параметрлер бойынша қамтамасыз етпейтін жұмысшы стансасы мен оның программаларының санкциясыз қол жеткізуден қорғаудың парольдық жүйесінің жеткіліксіздігі;

5) коммерциялық ақпараттардың құпиялылығы, құпия режиміне және компьютерлік техника құралдарына санкциясыз қол жеткізуден қорғау жағынан оның қауіпсіздігіне жауап беретін қызметтегі адамның болмауы;

6) машиналық ақпарат түрінде болатын қатаң қаржы есептері құжаттарына қызметкерлердің категриясына қарай қол жеткізу жағдайының болмауы;

7) коммерциялық және қызметтік құпияны жария етпеу, дербес мәліметтер мен басқа да құпиялы ақпараттарды таратпау жайында қызметкерлермен келесімшарттың болмауы.

Көрсетілген тұлғалардың қызметтің міндеттеріне берілген, бұрын КТҚ қауіпсіздігін қамтамасыз ету шараларын жүзеге асырудың келесі позициялары кіруі тиіс:

1) КТҚ қорғаудың талаптарын нақты ұйымдастыруда басшылық тарапынан қолдау көрсетуді қамтамасыз ету;

2) ақпараттарды қорғаудың кешенді жоспарын әзерлеу;

3) ұйымның қызметінің спецификасына сәйкес ақпаратты қорғаудың негізгі бағыттарын анықтау;

4) қорғау шараларын қаржыландыру шығындарының жалпы сметасын әзерленген жоспарға сәйкес құрастыру және оны ұйымның басшысына жоспардың қосымшасы ретінде бекітуге ұсыну;

5) қызметкерлер мен әкімшілік арасындағы сәйкес келісімшарттарды орнықтырылған өз құдыреті шамасында жасау арқылы ақпарат қауіпсіздігіне ұйымдардың қызметкерлерінің жауапкершіліктерін анықтау.

Мұнда, тәжірибе көрсеткендей, КТҚ қауіпсіздігінің шараларының тиімділігін арттырудың ең сенімді құралдары нақты ұйымдарда қолданылатын қорғаудың нақты ұйымдастыру – техникалық шараларымен жұмыс істеуші персоналын таныстыру және оған оқыту, үйрету.

Техникалық шаралар арнаулы мақсаттағы түрлі қондырғыларды қолдану деген сөз.

– тоқтаусыз қуат алу көзі;

– аппараттардың экрандық құрылғыларын, өткізгіш байланыс линиялары және компьютерлік техника орналасқан бөлме;

– телефониялық кешенді қорғау құрылғылары;

– өрттен сақтандыру құрылғысы;

– компьютер порттарын қорғау құралдары.

Қол жеткізу былайша анықталу керек:

– жалпы (әрбір пайдалануға сөзсіз ұсынылатын);

– бас тарту (сөзсіз бас тарту, мысалы ақпараттың бір бөлігін алып тастауға рұқсат сұрау);

– жағдайға қарай тәуелді, пайдаланушының сұранысын блоктауды қарастырады, мысалы, нақты бір терминалдан компьютерлік жүйеге сұраныс жасау кезінде немесе белгілі бір уақыт интервалында;

– мәліметтердің мазмұнына тәуелді (бұл жағдайда қол жеткізу туралы шешім мәліметтердің ағымдағы мәніне негізделеді, мысалы кейбір пайдаланушыға қайсыбір мәліметті оқуға тыйым салады);

– күйге тәуелді (компьютерлік жүйенің динамикалық жағдайы) программалар мен қорғау жүйесінің басқаратын компьютерлік жүйелердің ағымдағы күйіне байланысты жүзеге асырылады.

Компьютерлік қауіпсіздік саласында әзірлемелерге көп нәрсе байланысты екенін айтқым келеді. Соңғы нәтижесінде ол компьютерлік қауіпсіздігі құралдарын индустриялауға алып келуі тиісті.

Әдебиеттер

1 Девянин В. и др. Теоритические основы компьютерной безопасности. – М.: Радио и связь, 2000.

2 Битиев Ш.Б. Защита информаций и информационная безопасность. – Алматы: Асем-Систем, 2005.

3 Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2005.
4 Партыка Т.Л., Папов И.И. Информационная безопасность. – М.: Форум-Инфра, 2004.
5 Рябко Б.Я. Криптографические методы защиты информации. – М.: Горячая линия-телеком, 2005.
6 Левин М. Криптография без секретов. Руководство пользователя. – М.: Новый издательский дом, 2005.

References

1 Devjanin V. i dr. Teoriticheskie osnovy komp'juternoj bezopasnosti. – M.: Radio i svjaz', 2000.
2 Bitiev Sh.B. Zashhita informacij i informacionnaja bezopasnost'. – Almaty: Asem-Sistem, 2005.
3 Horev P.B. Metody i sredstva zashhity informacii v komp'juternyh sis-temah. – M.: Akademija, 2005.
4 Partyka T.L., Papov I.I. Informacionnaja bezopasnost'. – M.: Forum-Infra, 2004.
5 Rjabko B.Ja. Kriptograficheskie metody zashhity informacii. – M.: Gorjachaja linija-telekom, 2005.
6 Levin M. Kriptografija bez sekretov. Rukovodstvo pol'zovatelja. – M.: No-vyj izdatel'skij dom, 2005.